ID: 679479
Sample Name: llcubnch6T
Cookbook: default.jbs
Time: 21:06:11
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

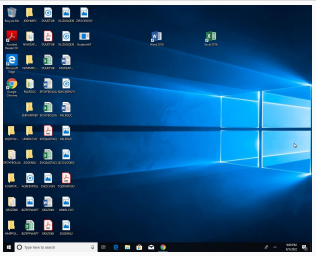
Windows Analysis Report

llcubnch6T

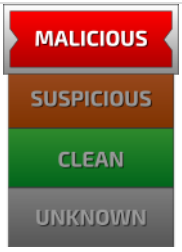
Overview

General Information

Sample Name:	llcubnch6T (renamed file extension from none to exe)
Analysis ID:	679479
MD5:	44e407b3de4a98.
SHA1:	6eb199e6837432.
SHA256:	da6abb6f3aae25..
Tags:	32 exe trojan
Infos:	



Detection



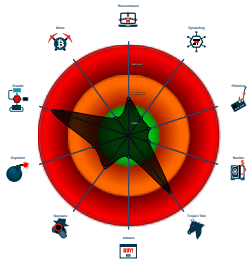
AsyncRAT

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AntiVM3
- Yara detected AsyncRAT
- Multi AV Scanner detection for drop…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader
- Machine Learning detection for drop…
- Adds a directory exclusion to Windo…

Classification



Process Tree

- **System is w10x64**
- llcubnch6T.exe (PID: 5324 cmdline: "C:\Users\user\Desktop\llcubnch6T.exe" MD5: 44E407B3DE4A9865AB747BDCA810B0B9)
  - powershell.exe (PID: 5040 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\RhFYnHFgJ.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6132 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\RhFYnHFgJ" /XML "C:\Users\user\AppData\Local\Temp\tmp95A0.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - llcubnch6T.exe (PID: 3720 cmdline: C:\Users\user\Desktop\llcubnch6T.exe MD5: 44E407B3DE4A9865AB747BDCA810B0B9)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT


```
{
  "Server": "91.193.75.135",
  "Ports": "3030",
  "Version": "0.5.7B",
  "Autorun": "false",
  "Install_Folder": "%AppData%"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.418726957.0000000003063000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.630822289.0000000003051000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x140ef:$x1: AsyncRAT • 0x1412d:$x1: AsyncRAT
00000009.00000000.410857927.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000009.00000000.410857927.0000000000402000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0xa0d9:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
00000009.00000002.635757563.00000000055A6000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x8743:$x1: AsyncRAT • 0x8781:$x1: AsyncRAT
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.llcubnch6T.exe.30fdb24.6.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.2.llcubnch6T.exe.30fdb24.6.unpack	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0x84d9:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
0.2.llcubnch6T.exe.310ae28.5.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.2.llcubnch6T.exe.310ae28.5.unpack	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0x84d9:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
0.2.llcubnch6T.exe.30fdb24.6.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 10 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected AsyncRAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Yara detected AsyncRAT

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion

Yara detected AntiVM3

Yara detected AsyncRAT

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings

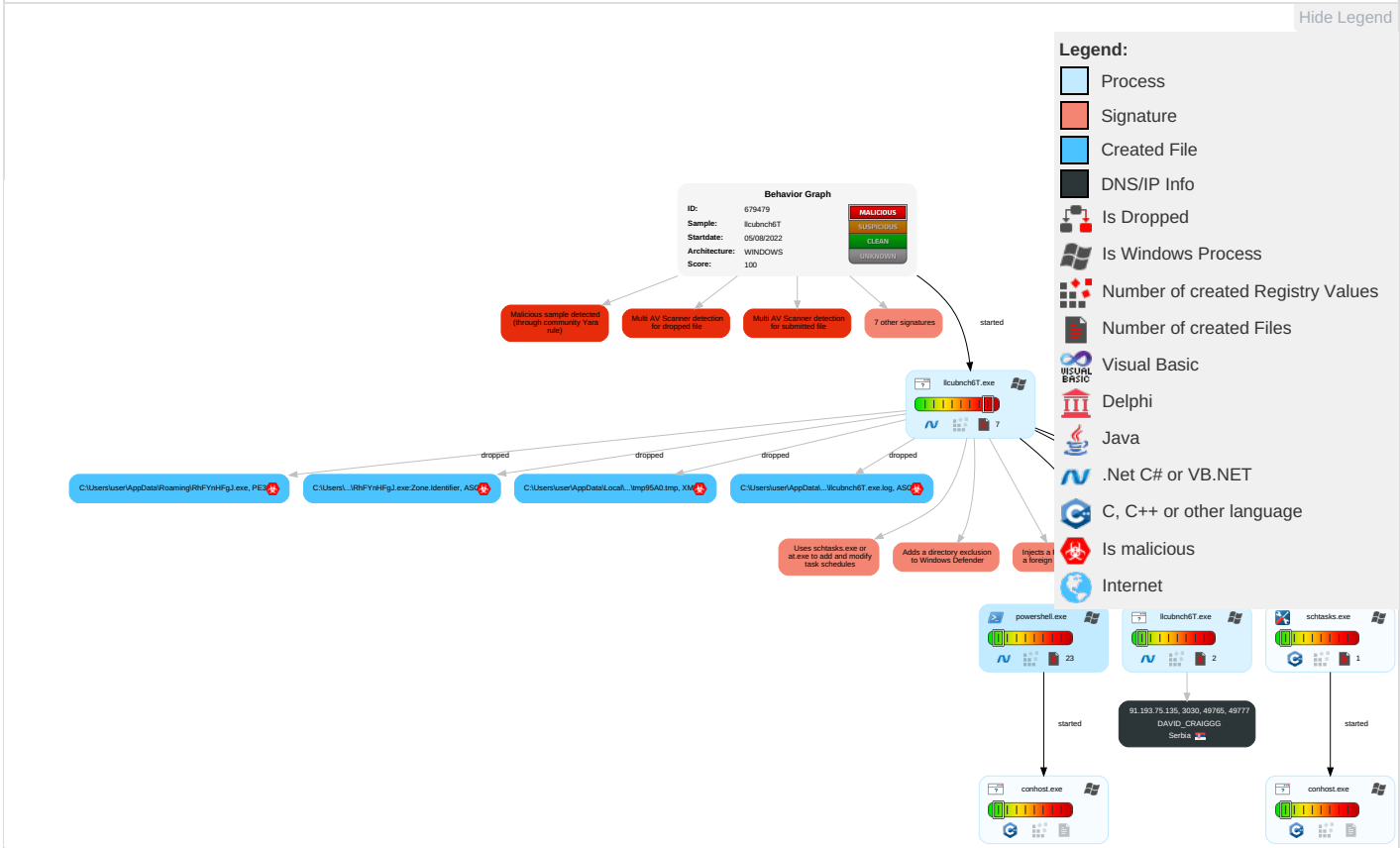
Yara detected AsyncRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Scheduled Task/Job	2 Scheduled Task/Job	1 1 1 Process Injection	1 Masqueradi ng	1 Input Capture	2 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communic ation	Remotely Track Device Without Authorizati on	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initializatio n Scripts	2 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati on	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualizatio n/Sandbox Evasion	Security Account Manager	2 1 Virtualizatio n/Sandbox Evasion	SMB/Wind ows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganogra phy	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonati on	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscat e/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic ation		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 2 Obfuscated Files or Information	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 2 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
llcubnch6T.exe	54%	Virustotal		Browse
llcubnch6T.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\RhFYnHFgJ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\RhFYnHFgJ.exe	54%	ReversingLabs	ByteCode-MSIL.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.llcubnch6T.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1202836		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/v;	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.fontbureau.comonydZ;	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comituFv;	0%	Avira URL Cloud	safe	
http://fontfabrik.comi;	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/E;	0%	Avira URL Cloud	safe	
http://www.fontbureau.comceta	0%	URL Reputation	safe	
http://www.sandoll.co.kront	0%	Avira URL Cloud	safe	
http://www.fontbureau.comepko	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/knl	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsiv9	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnarS/	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl-g	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0-sa;	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/lth;	0%	Avira URL Cloud	safe	
http://fontfabrik.comz	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cns	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0W	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.itcfonts.	0%	URL Reputation	safe	
http://www.urwpp.deFT	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comnc.Z;	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.sandoll.co.krtp	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comic	0%	URL Reputation	safe	
http://www.founder.com.cn/cnMic	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/ar	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueta	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/h;	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/aj#W	0%	Avira URL Cloud	safe	
http://www.carterandcone.comadD	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/u-hE;	0%	Avira URL Cloud	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comL.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/oi	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deC	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.sakkal.com0	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.goodfont.co.krtp	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma;	0%	Avira URL Cloud	safe	
http://www.urwpp.deo$	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comcetoS;	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.fontbureau.comav;	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/Z;	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.f	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/de-d	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/v;	llcubnch6T.exe, 00000000.00000003.376589985.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376392718.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376159863.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376304898.0000000005F71000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376048892.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376546388.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.375949766.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376099331.0000000005F71000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com2	llcubnch6T.exe, 00000000.00000003.367498032.0000000005F52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comonydZ;	llcubnch6T.exe, 00000000.00000003.379622921.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379851679.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380056944.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379770002.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379922349.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cn/bThe	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comituFv;	llcubnch6T.exe, 00000000.00000003.380490931.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380611387.0000000005F70000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380236923.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380325146.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380749411.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381516393.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380956167.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381059048.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381273773.0000000005F74000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://fontfabrik.comi;	llcubnch6T.exe, 00000000.00000003.369532282.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.369344253.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.369439345.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/E;	llcubnch6T.exe, 00000000.00000003.376766485.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376932034.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376589985.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376392718.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376159863.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376612294.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376304898.0000000005F71000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376546388.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376677530.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376099331.0000000005F71000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comceta	llcubnch6T.exe, 00000000.00000003.386884447.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.386656862.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.386539619.0000000005F74000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kront	llcubnch6T.exe, 00000000.00000003.371976372.0000000005F70000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comepko	llcubnch6T.exe, 00000000.00000003.379374870.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379548812.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379280133.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379140386.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	llcubnch6T.exe, 00000000.00000003.371976372.0000000005F70000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/knl	llcubnch6T.exe, 00000000.00000003.375863348.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.375712201.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.375949766.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comsiv9	llcubnch6T.exe, 00000000.00000003.380490931.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380611387.0000000005F70000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380325146.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	llcubnch6T.exe, 00000000.00000003.367498032.0000000005F52000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	llcubnch6T.exe, 00000000.00000003.382620508.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnarS/	llcubnch6T.exe, 00000000.00000003.373754624.0000000005F78000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	llcubnch6T.exe, 00000000.00000003.369532282.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.369672069.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.369439345.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.369755917.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.369565571.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnl-g	llcubnch6T.exe, 00000000.00000003.373045911.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372828062.0000000005F71000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.373098086.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372992295.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372713612.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.373141901.0000000005F78000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y0-sa;	llcubnch6T.exe, 00000000.00000003.376589985.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376392718.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376304898.0000000005F71000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376546388.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/lth;	llcubnch6T.exe, 00000000.00000003.376392718.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376159863.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376304898.0000000005F71000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376048892.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.375949766.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376099331.0000000005F71000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.comz	llcubnch6T.exe, 00000000.00000003.369532282.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.369672069.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.369755917.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.369565571.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cns	llcubnch6T.exe, 00000000.00000003.373045911.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372828062.0000000005F71000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.373098086.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372992295.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.373257248.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372713612.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.373141901.0000000005F78000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0W	llcubnch6T.exe, 00000000.00000003.376589985.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376392718.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376159863.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376612294.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376304898.0000000005F71000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376546388.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376099331.0000000005F71000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.html	llcubnch6T.exe, 00000000.00000003.376677530.0000000005F74000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.itcfonts.	llcubnch6T.exe, 00000000.00000003.377084125.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376932034.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.377017050.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deFT	llcubnch6T.exe, 00000000.00000003.380956167.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381059048.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	llcubnch6T.exe, 00000000.00000003.371976372.0000000005F70000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372078011.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372146838.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.371863268.0000000005F71000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comnc.Z;	llcubnch6T.exe, 00000000.00000003.378729506.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.deDPlease	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krtp	llcubnch6T.exe, 00000000.00000003.371976372.0000000005F70000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	llcubnch6T.exe, 00000000.00000003.378274559.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.378415798.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380956167.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381059048.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.378491515.0000000005F72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	llcubnch6T.exe, 00000000.00000003.373754624.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	llcubnch6T.exe, 00000000.00000002.418726957.0000000003063000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.come	llcubnch6T.exe, 00000000.00000003.367498032.0000000005F52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	llcubnch6T.exe, 00000000.00000003.377084125.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376766485.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376932034.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.377017050.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.377194158.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376677530.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comic	llcubnch6T.exe, 00000000.00000003.374008369.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.374159108.0000000005F79000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.374208532.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.373945445.0000000005F78000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	llcubnch6T.exe, 00000000.00000003.373444862.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.373397776.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.373494865.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	llcubnch6T.exe, 00000000.00000003.379280133.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381656755.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381059048.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.378729506.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381273773.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.386539619.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379770002.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379922349.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379140386.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.378822721.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnMic	llcubnch6T.exe, 00000000.00000003.373045911.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372828062.0000000005F71000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372992295.0000000005F78000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/	llcubnch6T.exe, 00000000.00000003.382515419.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.383198382.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.383615585.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.382620508.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.383062477.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.383441888.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.383716381.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.382877880.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.382700986.0000000005F74000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

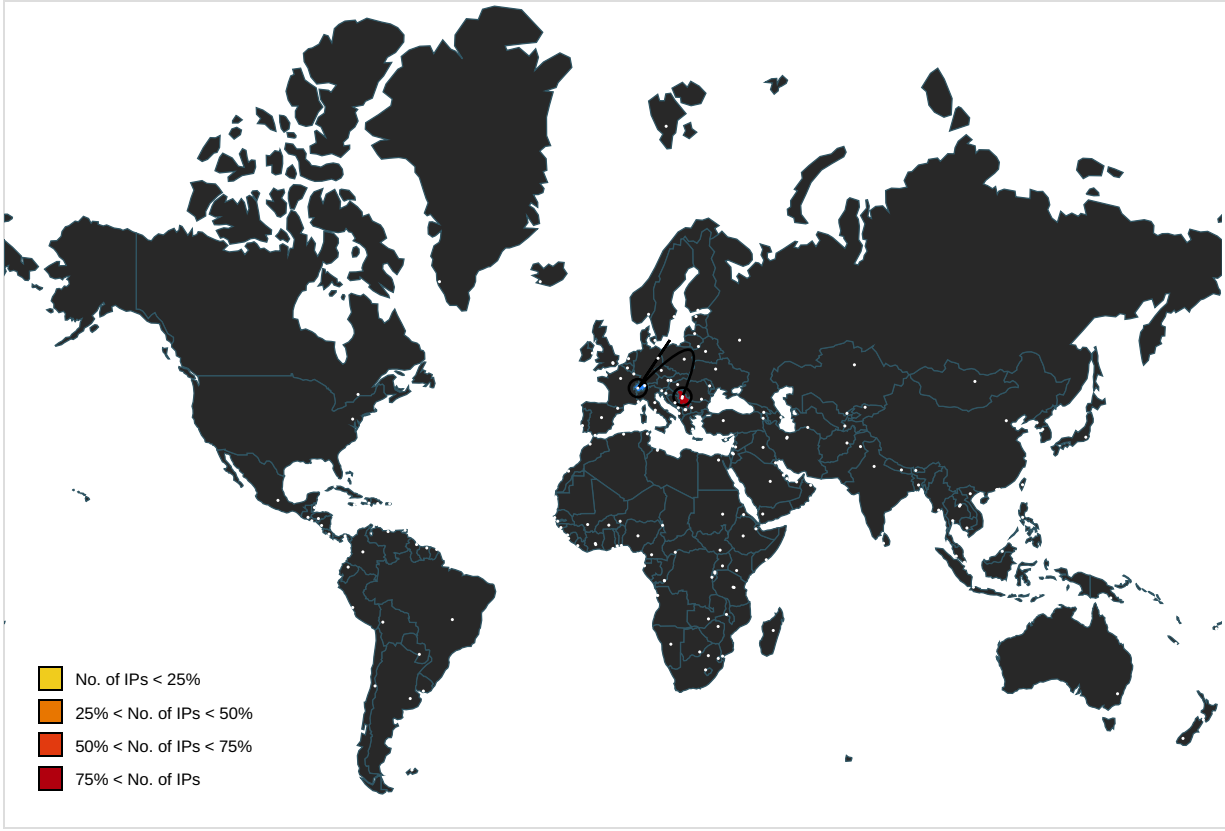
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	llcubnch6T.exe, 00000000.00000003.380490931.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380611387.0000000005F70000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380236923.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380325146.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380749411.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380956167.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381059048.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381273773.0000000005F74000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comslnt	llcubnch6T.exe, 00000000.00000003.374266055.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.374439978.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.374621756.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/ar	llcubnch6T.exe, 00000000.00000003.372828062.0000000005F71000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comueta	llcubnch6T.exe, 00000000.00000003.379851679.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380056944.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379770002.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379922349.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/h;	llcubnch6T.exe, 00000000.00000003.376766485.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376932034.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376589985.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376612294.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376546388.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376677530.0000000005F74000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/aj#W	llcubnch6T.exe, 00000000.00000003.372183289.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372085870.0000000005F78000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comadD	llcubnch6T.exe, 00000000.00000003.374008369.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.374159108.0000000005F79000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.374208532.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.373945445.0000000005F78000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/u-hE;	llcubnch6T.exe, 00000000.00000003.376048892.0000000005F72000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comion	llcubnch6T.exe, 00000000.00000003.379374870.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379280133.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comL.TTF	llcubnch6T.exe, 00000000.00000003.381774652.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380749411.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381516393.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.382095894.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380956167.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381656755.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381059048.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381273773.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381931622.0000000005F74000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/oi	llcubnch6T.exe, 00000000.00000003.376589985.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376392718.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376612294.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376304898.0000000005F71000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376546388.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	llcubnch6T.exe, 00000000.00000003.376099331.0000000005F71000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	llcubnch6T.exe, 00000000.00000003.379374870.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379622921.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379851679.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379548812.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379280133.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379770002.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379922349.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379140386.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.come.com	llcubnch6T.exe, 00000000.00000003.379374870.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379622921.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379851679.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379548812.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379280133.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379770002.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379922349.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379140386.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	llcubnch6T.exe, 00000000.00000003.370486654.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.370416567.0000000005F77000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deC	llcubnch6T.exe, 00000000.00000003.378274559.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.378415798.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.378491515.0000000005F72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	llcubnch6T.exe, 00000000.00000003.372828062.0000000005F71000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372078011.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com0	llcubnch6T.exe, 00000000.00000003.376677530.0000000005F74000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	llcubnch6T.exe, 00000000.00000003.372828062.0000000005F71000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372581826.0000000005F78000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372713612.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.372553600.0000000005F78000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.krtp	llcubnch6T.exe, 00000000.00000003.371976372.0000000005F70000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	llcubnch6T.exe, 00000000.00000003.379622921.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379851679.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380056944.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.379770002.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.coma;	llcubnch6T.exe, 00000000.00000003.380490931.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380325146.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.deo$	llcubnch6T.exe, 00000000.00000003.378274559.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.378415798.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.378491515.0000000005F72000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/	llcubnch6T.exe, 00000000.00000003.376677530.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.377578464.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.376099331.0000000005F71000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comcetoS;	llcubnch6T.exe, 00000000.00000003.386884447.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.386656862.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.413372395.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.386539619.0000000005F74000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.zhongyicts.com.cno.	llcubnch6T.exe, 00000000.00000003.373754624.0000000005F78000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	llcubnch6T.exe, 00000000.00000002.432126891.0000000007252000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comalic	llcubnch6T.exe, 00000000.00000003.380611387.0000000005F70000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380749411.0000000005F72000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381516393.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.380956167.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381059048.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.381273773.0000000005F74000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comav;	llcubnch6T.exe, 00000000.00000003.386884447.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.386656862.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.413372395.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.386539619.0000000005F74000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.galapagosdesign.com/Z;	llcubnch6T.exe, 00000000.00000003.382515419.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.382620508.0000000005F74000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.382700986.0000000005F74000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cno.f	llcubnch6T.exe, 00000000.00000003.373754624.0000000005F78000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/de-d	llcubnch6T.exe, 00000000.00000003.375863348.0000000005F73000.00000004.00000800.00020000.00000000.sdmp, llcubnch6T.exe, 00000000.00000003.375712201.0000000005F73000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.193.75.135	unknown	Serbia		209623	DAVID_CRAIGGG	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679479
Start date and time: 05/08/202221:06:11	2022-08-05 21:06:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	llcubnch6T (renamed file extension from none to exe)
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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/8@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Execution Graph export aborted for target llcubnch6T.exe, PID 3720 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- 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.

Simulations

Behavior and APIs

Time	Type	Description
21:07:33	API Interceptor	1x Sleep call for process: llcubnch6T.exe modified
21:07:40	API Interceptor	40x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\llcubnch6T.exe.log

Process:	C:\Users\user\Desktop\llcubnch6T.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1394
Entropy (8bit):	5.340883346054895
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84F0:MIHK5HKXE1qHbHKnYHKhQnoPtHoxHhAR

MD5:	B51A52A837298BCF7A6EB58551AEF99C
SHA1:	61EEFCC20AC255B8651769E5C48E27B2A983FC4A
SHA-256:	1D393FBB3CE754EA699462C2778587A7F2451EB23BE2BD5084C95A46B20BE8AF
SHA-512:	138544399787651C847837719606197E539857206CCB271E0F4A86E2017FBADABADF5A235B6F6F1DA8ADE7EF29DBA3115CD1996AD01F92CA30C57D0BF217C11
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e08

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22272
Entropy (8bit):	5.600170087985691
Encrypted:	false
SSDEEP:	384:ntCDDq0C6VKa/G/KBJYSB+sjultI+b7Y9g9SJ3xa1BMrm7Z1AV7Dw64I+iyYB:va/QOY4dClth79cBa4+M
MD5:	E6BC308E44F52713322480EE725334CB
SHA1:	57423595B636FC70CF53EB29D227CB6B9BC42F8E
SHA-256:	C581CF1C3C82F6B2DF7CD852361A0466AC85172BEC6E34D9655A6C18667BBEC7
SHA-512:	E4904783464A21408255C32364441F3741BF9544182F57CF7A14946E6AFC100F16D8CF3089F155AA4A08E4E65FF246F20517C7E1FE6DB962801CC6619ADBE19D
Malicious:	false
Reputation:	low
Preview:	@...e.....y.....>.y.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3wwz4tj5.5nu.psm1

Process:	C:\Windows\SysWOW64\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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_d1zr1t5y.vgy.ps1

Process:	C:\Windows\SysWOW64\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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp95A0.tmp

Process:	C:\Users\user\Desktop\llcubnch6T.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1608
Entropy (8bit):	5.124455319747427
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOilQRvh7hwrgXuNtLPaxvn:cgea6YrFdOFzOzN33ODOiDdKrsuTzuv
MD5:	0E2E547022BB8168544A3BD4F03B80DF
SHA1:	231F190A8B0CE5A7C8BE4346172F48D342B44234
SHA-256:	7B1A5B157DD8468BA308482C17F6451096304542DCAA29CF568026DCF494BC60
SHA-512:	2FE546649789F3022A8E3606F21199FCFCDBB0E493830556B87D9887A61717D65C2E3A763DF805216320D1A08A2408CCF00F714D212268E5B049940BE2A03BDF
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailab

C:\Users\user\AppData\Roaming\RhFYnHFgJ.exe

Process:	C:\Users\user\Desktop\llcubnch6T.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	621056
Entropy (8bit):	7.267556524859017
Encrypted:	false
SSDEEP:	12288:4H2iNSg6SKlpxxDAE7Mn3cs9OWvHoFiPEwjlk2Y/gbb:81SLlpxx8EEc85oFaj22p
MD5:	44E407B3DE4A9865AB747BDCA810B0B9
SHA1:	6EB199E6837432D8ACB98C03B22277F340726372
SHA-256:	DA6ABB6F3AAE250D50ED09B6EACC267C33E50895E3EBD7E6BA800AB018351EC5
SHA-512:	DB8E1652A6E8D90450114641F3573B9423BCE4C27C237AF49A59DC44ACF929580CDF59E5C216391EF87C27C52FC610653D19BCE2D1507E4D8F310B7D6DEE8AB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 54%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....s.b.....0..r.....b.... .....@.. .....@.....O..... ....H.....text...hq... ...r..... ..`.rsrc.....t.....@..@.reloc.....x.....@..B.....D.....H.....S.....B.....@.....^..}.....(.....(.....*.0..+.....,..{.....+.....{....o.....(....*..0.....(....s.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.....{....o.....{....o.....(.....{.....o .....{....o!....."...Bs"...o#...&.{....o!....."...Bs"...o#...&.{....o$....{.....o%.....{....o$....{.....o%.....{....o$....{.....o%.....{....o$....{.....o%.....{....o$...

C:\Users\user\AppData\Roaming\RhFYnHFgJ.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\llcubnch6T.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220805\PowerShell_transcript.724471.0b0YCxHN.20220805210738.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5815
Entropy (8bit):	5.37547468273822
Encrypted:	false
SSDEEP:	96:BZDTL5NKCqDo1ZSGZiTL5NKCqDo1ZE39PjZiTL5NKCqDo1ZEG//hZ+:7
MD5:	599FC2C562BB7B72B0592FCDFA20F17F
SHA1:	22D5820DE1296A150D38D950EFE7540DEF5672C1
SHA-256:	227A4D6538B52B6061A7960A5F9B9795AB1773C2752EEF201CFCD5B85E38E274
SHA-512:	C95070EF3920CCAC7689EB27A953C13DAE36173DF17D36194D0BBA930BC0FDFA470C559EE5713F53D2EF26D0D9F1107079E710A8DE326EA3E6AF045BAE1CB9D
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220805210740..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 724471 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\RhFYnHFgJ.exe..Process ID: 5040..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: 20220805210740..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\RhFYnHFgJ.exe..**********..Windows PowerShell transcript start..Start time: 20220805211241..Username: computer\user..RunAs User: DESKTOP

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.267556524859017
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	llcubnch6T.exe
File size:	621056
MD5:	44e407b3de4a9865ab747bdca810b0b9
SHA1:	6eb199e6837432d8acb98c03b22277f340726372
SHA256:	da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5
SHA512:	db8e1652a6e8d90450114641f3573b9423bce4c27c237af49a59dc44acf929580cdf59e5c216391ef87c27c52fc610653d19bce2d1507e4d8f310b7d6dee8a4b
SSDEEP:	12288:4H2iNSg6SKlpxxDAE7Mn3cs9OWvHoFiPEwjlk2Y/gbb:81SLlpxx8EEc85oFaj22p
TLSH:	52D4E082F2694F5BC0274BF9AC2594581727B39E503DD6096DFEB8EBA0727C34152E0B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....s.b.....0..r.....b.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x499162
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62E773E6 [Mon Aug 1 06:34:14 2022 UTC]
TLS Callbacks:	

CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
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
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
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
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
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
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
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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x99110	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9a000	0x3a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x97168	0x97200	False	0.7348273366418527	data	7.2738007120716635	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x9a000	0x3a8	0x400	False	0.38671875	data	2.9730132767456556	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9c000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x9a058	0x34c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

TCP Packets

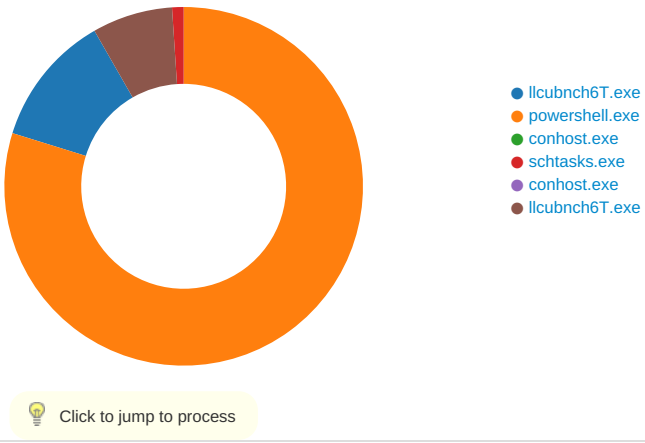
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 21:07:53.229300022 CEST	49765	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:07:53.269311905 CEST	3030	49765	91.193.75.135	192.168.2.6
Aug 5, 2022 21:07:53.830010891 CEST	49765	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:07:53.869882107 CEST	3030	49765	91.193.75.135	192.168.2.6
Aug 5, 2022 21:07:54.523250103 CEST	49765	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:07:54.563241959 CEST	3030	49765	91.193.75.135	192.168.2.6
Aug 5, 2022 21:07:59.581712961 CEST	49777	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:07:59.621660948 CEST	3030	49777	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:00.129159927 CEST	49777	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:00.169723034 CEST	3030	49777	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:00.674324989 CEST	49777	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:00.714421988 CEST	3030	49777	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:05.723584890 CEST	49779	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:05.763652086 CEST	3030	49779	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:06.268538952 CEST	49779	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:06.308541059 CEST	3030	49779	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:06.815474033 CEST	49779	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:06.858010054 CEST	3030	49779	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:11.866844893 CEST	49784	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:11.907004118 CEST	3030	49784	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:12.534842014 CEST	49784	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:12.575058937 CEST	3030	49784	91.193.75.135	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 21:08:13.222290993 CEST	49784	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:13.262275934 CEST	3030	49784	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:18.270786047 CEST	49787	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:18.311213017 CEST	3030	49787	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:18.832133055 CEST	49787	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:18.872239113 CEST	3030	49787	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:19.439817905 CEST	49787	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:19.479929924 CEST	3030	49787	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:24.489988089 CEST	49794	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:24.530139923 CEST	3030	49794	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:25.035784960 CEST	49794	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:25.075980902 CEST	3030	49794	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:25.582756996 CEST	49794	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:25.622864962 CEST	3030	49794	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:30.632461071 CEST	49797	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:30.672374010 CEST	3030	49797	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:31.223885059 CEST	49797	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:31.263833046 CEST	3030	49797	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:31.926997900 CEST	49797	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:31.967113018 CEST	3030	49797	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:36.977118015 CEST	49798	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:37.017225027 CEST	3030	49798	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:37.615282059 CEST	49798	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:37.655406952 CEST	3030	49798	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:38.161915064 CEST	49798	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:38.202013016 CEST	3030	49798	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:43.210587025 CEST	49800	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:43.250809908 CEST	3030	49800	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:43.756254911 CEST	49800	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:43.796329021 CEST	3030	49800	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:44.459325075 CEST	49800	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:44.499526024 CEST	3030	49800	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:49.509156942 CEST	49816	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:49.549237013 CEST	3030	49816	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:50.148332119 CEST	49816	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:50.188297033 CEST	3030	49816	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:50.750245094 CEST	49816	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:50.790303946 CEST	3030	49816	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:55.806442976 CEST	49845	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:55.846424103 CEST	3030	49845	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:56.360430002 CEST	49845	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:56.400496960 CEST	3030	49845	91.193.75.135	192.168.2.6
Aug 5, 2022 21:08:56.962353945 CEST	49845	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:08:57.002532959 CEST	3030	49845	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:02.585449934 CEST	49854	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:02.625430107 CEST	3030	49854	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:03.259737968 CEST	49854	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:03.299568892 CEST	3030	49854	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:03.947386980 CEST	49854	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:03.987705946 CEST	3030	49854	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:08.997055054 CEST	49859	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:09.038681984 CEST	3030	49859	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:09.541527033 CEST	49859	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:09.581378937 CEST	3030	49859	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:10.088469982 CEST	49859	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:10.128552914 CEST	3030	49859	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:15.136780977 CEST	49870	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:15.176758051 CEST	3030	49870	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:15.682686090 CEST	49870	3030	192.168.2.6	91.193.75.135

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 21:09:15.722548962 CEST	3030	49870	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:16.229609013 CEST	49870	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:16.269427061 CEST	3030	49870	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:21.278151035 CEST	49883	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:21.318515062 CEST	3030	49883	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:21.855076075 CEST	49883	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:21.895132065 CEST	3030	49883	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:22.558250904 CEST	49883	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:22.598500967 CEST	3030	49883	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:27.606158018 CEST	49885	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:27.646354914 CEST	3030	49885	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:28.152470112 CEST	49885	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:28.192559004 CEST	3030	49885	91.193.75.135	192.168.2.6
Aug 5, 2022 21:09:28.699387074 CEST	49885	3030	192.168.2.6	91.193.75.135
Aug 5, 2022 21:09:28.739516973 CEST	3030	49885	91.193.75.135	192.168.2.6

Statistics

Behavior



System Behavior

Analysis Process: llcubnch6T.exe PID: **5324**, Parent PID: **6100**

General

Target ID:	0
Start time:	21:07:20
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\llcubnch6T.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\llcubnch6T.exe"
Imagebase:	0xa30000
File size:	621056 bytes
MD5 hash:	44E407B3DE4A9865AB747BDCA810B0B9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.418726957.0000000003063000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.419146088.00000000030EE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000000.00000002.419146088.00000000030EE000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	low

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	6CC1CF06	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	6CC1CF06	unknown
C:\Users\user\AppData\Roaming\RhFYnHFgJ.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6BA6DD66	CopyFileW
C:\Users\user\AppData\Roaming\RhFYnHFgJ.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6BA6DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp95A0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BA67038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\llcubnch6T.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF2C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp95A0.tmp	success or wait	1	6BA66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RhFYnHFgJ.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 73 fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 72 09 00 00 06 00 00 00 00 00 00 62 fd 09 00 00 20 00 00 00 fd 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 09 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELsb0rb @ @	success or wait	3	6BA6DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RhFYnHFgJ.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6BA6DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp95A0.tmp	0	1608	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo	success or wait	1	6BA61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\llcubnch6T.exe.log	0	1394	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6CF2C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CB503DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BA61B4F	ReadFile

Analysis Process: powershell.exe PID: **5040**, Parent PID: **5324**

General

Target ID:	5
Start time:	21:07:36
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\RhFYnHFgJ.exe
Imagebase:	0xf10000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6CC1CF06	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	6CC1CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_d1zr1t5y.vgy.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BA61E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3wwz4tj5.5nu.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BA61E60	CreateFileW
C:\Users\user\Documents\20220805	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BA6BEFF	CreateDirectoryW
C:\Users\user\Documents\20220805\PowerShell_transcript.724471.0b0YCxHN.20220805210738.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BA61E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_d1zr1t5y.vgy.ps1	success or wait	1	6BA66A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3wwz4tj5.5nu.psm1	success or wait	1	6BA66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_d1zr1t5y.vgy.ps1	0	1	31	1	success or wait	1	6BA61B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3wwz4tj5.5nu.psm1	0	1	31	1	success or wait	1	6BA61B4F	WriteFile
C:\Users\user\Documents\20220805\PowerShell_transcript.724471.0b0YCxHN.20220805210738.txt	0	3	ff		success or wait	1	6BA61B4F	WriteFile
C:\Users\user\Documents\20220805\PowerShell_transcript.724471.0b0YCxHN.20220805210738.txt	3	685	2a 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 32 30 38 30 35 32 31 30 37 34 30 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 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 37 32 34 34 37 31 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	**********Windows PowerShell transcript startStart time: 20220805210740Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 724471 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	44	6BA61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 79 14 00 00 18 00 00 00 fd 0e fd 03 fd 0a fd 0a fd 0a 00 00 3e 01 79 00 0b 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ey>y@	success or wait	1	6CEE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6CEE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6CEE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6CEE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6CEE76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 16 3b 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 45 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 00 01 fd 44 00 01 6d 45 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;@;@;@<@<@<@W@M@E@;M@D@D@@M@<M@$M@8M@?M@BMDmE	success or wait	11	6CEE76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CB503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CBFCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CBFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CB503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	6CBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CBF5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6CC01F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22396	success or wait	1	6CC0203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CB503DE	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	6BA61B4F	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	6BA61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	110	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6BA61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CB503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6BA61B4F	ReadFile

Analysis Process: conhost.exe PID: **5308**, Parent PID: **5040**

General

Target ID:	6
Start time:	21:07:37
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: schtasks.exe PID: **6132**, Parent PID: **5324**

General

Target ID:	7
Start time:	21:07:37
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\RhFYnHFgJ" /XML "C:\Users\user\AppData\Local\Temp\tmp95A0.tmp
Imagebase:	0x290000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp95A0.tmp	unknown	2	success or wait	1	29AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp95A0.tmp	unknown	1609	success or wait	1	29ABD9	ReadFile

Analysis Process: conhost.exe PID: **1672**, Parent PID: **6132**

General

Target ID:	8

Start time:	21:07:39
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: llcubnch6T.exe PID: **3720**, Parent PID: **5324**

General

Target ID:	9
Start time:	21:07:42
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\llcubnch6T.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\llcubnch6T.exe
Imagebase:	0xce0000
File size:	621056 bytes
MD5 hash:	44E407B3DE4A9865AB747BDCA810B0B9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000009.00000002.630822289.0000000003051000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000009.00000000.410857927.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000009.00000000.410857927.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000009.00000002.635757563.00000000055A6000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	low

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	6CC1CF06	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	6CC1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBF5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BA61B4F	ReadFile

Disassembly

No disassembly