ID: 620365
Sample Name: g0dvHLi4bP
Cookbook: default.jbs
Time: 16:58:27
Date: 04/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report g0dvHLi4bP 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
System Summary 6
Data Obfuscation 6
Boot Survival 6
Hooking and other Techniques for Hiding and Protection 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 17
Public IPs 18
Private 18
General Information 18
Warnings 19
Simulations 19
Behavior and APIs 19
Joe Sandbox View / Context 19
IPs 19
Domains 19
ASNs 19
JA3 Fingerprints 19
Dropped Files 19
Created / dropped Files 20
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AheGmkp.exe.log 20
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\g0dvHLi4bP.exe.log 20
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 20
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jbaicfx1.xuw.psm1 21
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_up2wzwhf.0gz.ps1 21
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_v2bqczrd.h4q.psm1 21
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wlxjtc3d.5pt.ps1 22
C:\Users\user\AppData\Local\Temp\tmp972C.tmp 22
C:\Users\user\AppData\Local\Temp\tmpF6C5.tmp 22
C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe 23
C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe:Zone.Identifier 23
C:\Users\user\AppData\Roaming\lyfhOEwABQlG.exe 23
C:\Users\user\AppData\Roaming\lyfhOEwABQlG.exe:Zone.Identifier 24
C:\Users\user\Documents\20220504\PowerShell_transcript.302494.9BrDU9eF.20220504170044.txt 24
C:\Users\user\Documents\20220504\PowerShell_transcript.302494.Si+7UG0m.20220504170002.txt 24
Static File Info 25
General 25
File Icon 25
Static PE Info 25
General 25
Entrypoint Preview 25
Data Directories 27

Sections 27
Resources 28
Imports 28
Version Infos 28
Network Behavior 28
Network Port Distribution 28
TCP Packets 28
UDP Packets 30
DNS Queries 30
DNS Answers 30
SMTP Packets 30
Statistics 31
Behavior 31
System Behavior 31
Analysis Process: g0dvHLi4bP.exePID: 7044, Parent PID: 5212 31
General 31
File Activities 32
File Created 32
File Deleted 32
File Written 32
File Read 34
Analysis Process: powershell.exePID: 5868, Parent PID: 7044 34
General 34
File Activities 35
File Created 35
File Deleted 35
File Written 35
File Read 37
Analysis Process: conhost.exePID: 3064, Parent PID: 5868 40
General 40
Analysis Process: schtasks.exePID: 5864, Parent PID: 7044 40
General 40
File Activities 41
File Read 41
Analysis Process: conhost.exePID: 6388, Parent PID: 5864 41
General 41
Analysis Process: g0dvHLi4bP.exePID: 5432, Parent PID: 7044 41
General 41
File Activities 42
File Created 42
File Deleted 42
File Written 42
File Read 43
Registry Activities 43
Key Value Created 43
Analysis Process: AheGmkp.exePID: 6920, Parent PID: 684 44
General 44
File Activities 44
File Created 44
File Deleted 44
File Written 44
File Read 45
Analysis Process: AheGmkp.exePID: 6188, Parent PID: 684 45
General 45
Analysis Process: powershell.exePID: 7028, Parent PID: 6920 46
General 46
Analysis Process: conhost.exePID: 5324, Parent PID: 7028 46
General 46
Analysis Process: schtasks.exePID: 4952, Parent PID: 6920 46
General 46
Analysis Process: conhost.exePID: 6684, Parent PID: 4952 46
General 46
Analysis Process: AheGmkp.exePID: 6104, Parent PID: 6920 47
General 47
Analysis Process: AheGmkp.exePID: 5944, Parent PID: 6920 47
General 47
Analysis Process: AheGmkp.exePID: 7068, Parent PID: 6920 47
General 47
Disassembly 48

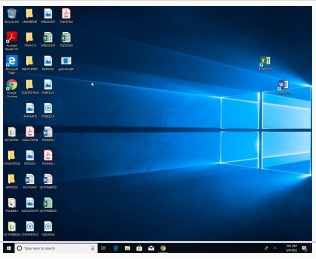
Windows Analysis Report

g0dvHLi4bP

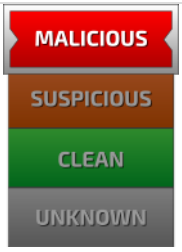
Overview

General Information

Sample Name:	g0dvHLi4bP (renamed file extension from none to exe)
Analysis ID:	620365
MD5:	4c414b473bccbb..
SHA1:	77bf848d5a1d4d..
SHA256:	7bb212946fdeb4..
Tags:	32 exe
Infos:	



Detection



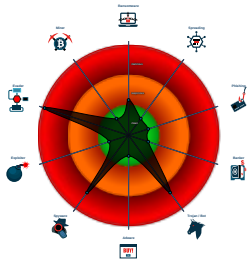
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- g0dvHLi4bP.exe (PID: 7044 cmdline: "C:\Users\user\Desktop\g0dvHLi4bP.exe" MD5: 4C414B473BCCBBCE2C7CDE00248EA1A1)
  - powershell.exe (PID: 5868 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lyfhOEwABQlG.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5864 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lyfhOEwABQlG" /XML "C:\Users\user\AppData\Local\Temp\tmpF6C5.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - g0dvHLi4bP.exe (PID: 5432 cmdline: C:\Users\user\Desktop\g0dvHLi4bP.exe MD5: 4C414B473BCCBBCE2C7CDE00248EA1A1)
- AheGmkp.exe (PID: 6920 cmdline: "C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe" MD5: 4C414B473BCCBBCE2C7CDE00248EA1A1)
  - powershell.exe (PID: 7028 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lyfhOEwABQlG.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4952 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lyfhOEwABQlG" /XML "C:\Users\user\AppData\Local\Temp\tmp972C.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AheGmkp.exe (PID: 6104 cmdline: C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe MD5: 4C414B473BCCBBCE2C7CDE00248EA1A1)
  - AheGmkp.exe (PID: 5944 cmdline: C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe MD5: 4C414B473BCCBBCE2C7CDE00248EA1A1)
  - AheGmkp.exe (PID: 7068 cmdline: C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe MD5: 4C414B473BCCBBCE2C7CDE00248EA1A1)
- AheGmkp.exe (PID: 6188 cmdline: "C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe" MD5: 4C414B473BCCBBCE2C7CDE00248EA1A1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "Az@gcmce.com",
  "Password": "   DANIEL3116",
  "Host": "us2.smtp.mailhostbox.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000000.596334236.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000018.00000000.596334236.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000018.00000000.595827903.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000018.00000000.595827903.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.501848453.00000000029C1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 37 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
24.0.AheGmkp.exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
24.0.AheGmkp.exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
24.0.AheGmkp.exe.400000.12.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32a97:$s10: logins • 0x324fe:$s11: credential • 0x2eb12:$g1: get_Clipboard • 0x2eb20:$g2: get_Keyboard • 0x2eb2d:$g3: get_Password • 0x2fe0c:$g4: get_CtrlKeyDown • 0x2fe1c:$g5: get_ShiftKeyDown • 0x2fe2d:$g6: get_AltKeyDown
0.2.g0dvHLi4bP.exe.3b7d998.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.g0dvHLi4bP.exe.3b7d998.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 69 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

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

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Yara detected AntiVM3

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

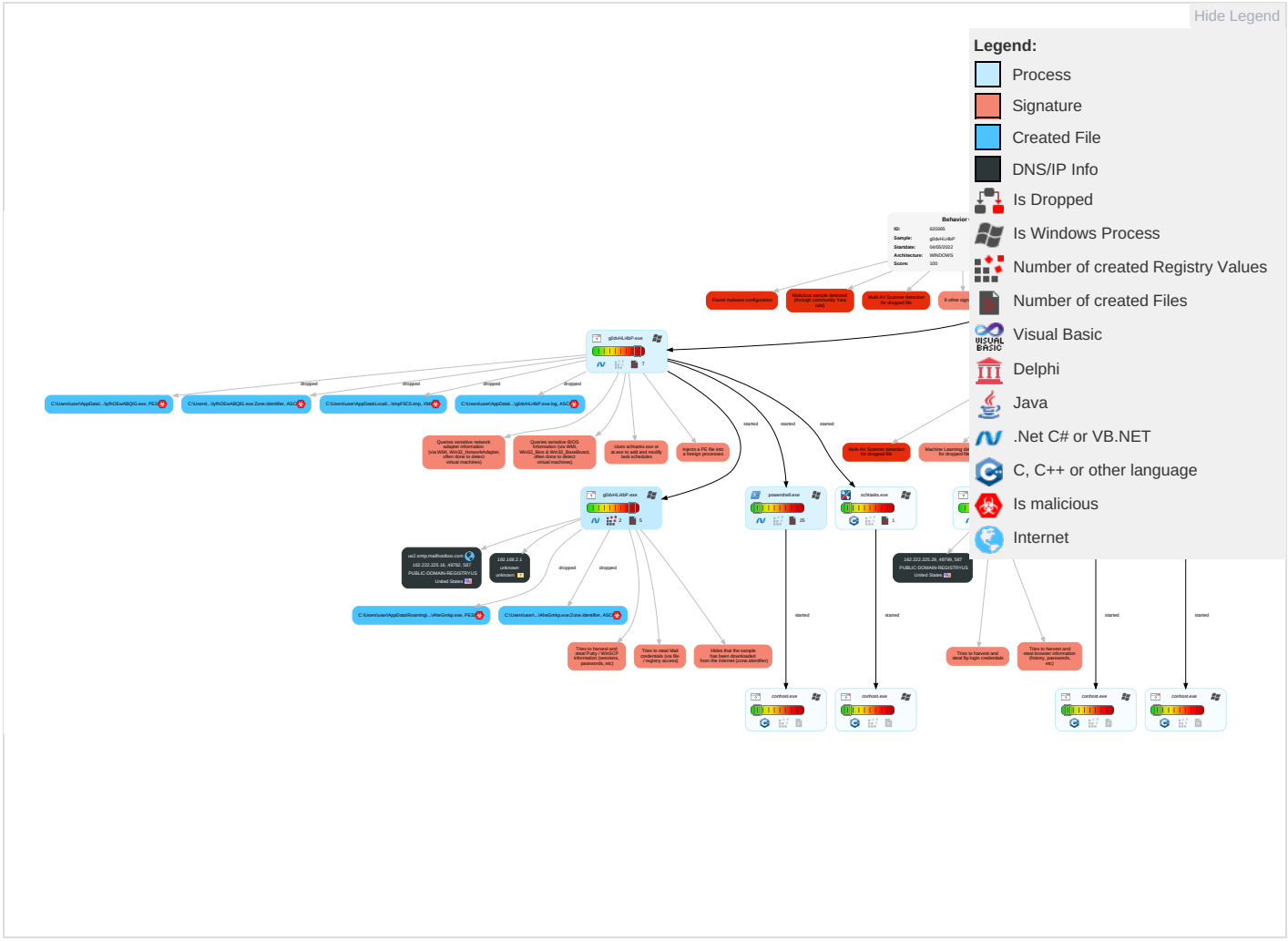
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 1 Process Injection	1 1 Disable or Modify Tools	2 OS Credential Dumping	1 Account Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 File and Directory Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	3 Obfuscated Files or Information	Security Account Manager	1 1 4 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 3 Software Packing	NTDS	1 Query Registry	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	3 1 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Process 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 3 1 Virtualization/Sandbox Evasion	DCSync	1 3 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 1 Process Injection	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

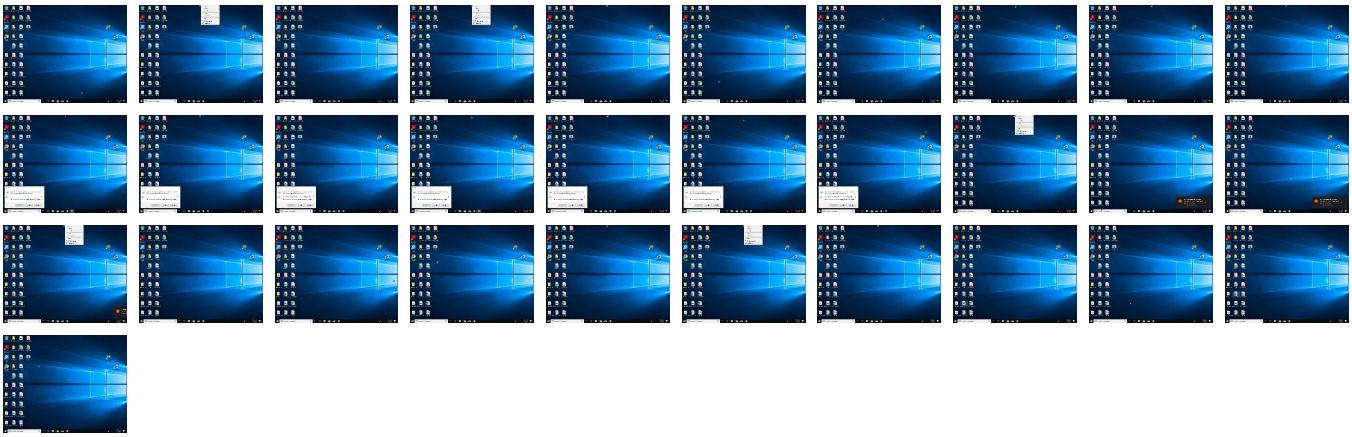
Behavior Graph



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
g0dvHLi4bP.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
g0dvHLi4bP.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\lyfhOEwABQlG.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\lyfhOEwABQlG.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.g0dvHLi4bP.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
24.0.AheGmkp.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
24.0.AheGmkp.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
24.0.AheGmkp.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
24.2.AheGmkp.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.g0dvHLi4bP.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
24.0.AheGmkp.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.g0dvHLi4bP.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.g0dvHLi4bP.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.g0dvHLi4bP.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
24.0.AheGmkp.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.2.g0dvHLi4bP.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://Iq79XHPURIYANir.org	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://crl.usertr	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comivd	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnese	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn;	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0r	0%	Avira URL Cloud	safe	
http://www.fontbureau.comTTF	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	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.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://en.wikipediaN	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/d	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.com5	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/V	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://www.fontbureau.comlicF	0%	URL Reputation	safe	
http://www.sajatypeworks.comk-s	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://api.ipify.org%appdata	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://KMYoUX.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/_	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	162.222.225.16	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lq79XHPURIYANir.org	AheGmkp.exe, 00000018.00000002.706330970.00000000033DC000.00000004.00000800.00020000.00000000.sdmp, AheGmkp.exe, 00000018.00000002.706504468.0000000003412000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	g0dvHLi4bP.exe, 00000008.00000002.704236786.0000000003021000.00000004.00000800.00020000.00000000.sdmp, AheGmkp.exe, 00000018.00000002.705211628.0000000003091000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	g0dvHLi4bP.exe, 00000008.00000002.705876237.000000000337A000.00000004.00000800.00020000.00000000.sdmp, AheGmkp.exe, 00000018.00000002.706376253.00000000033E6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.usertr	AheGmkp.exe, 00000018.00000003.646298713.0000000001425000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comivd	g0dvHLi4bP.exe, 00000000.00000003.434322634.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435735907.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434263544.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436481267.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434449814.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435975473.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.438134623.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436182054.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435045732.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434508936.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435924012.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435216005.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.439477892.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436845818.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.438504418.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434538231.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436004358.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.438993924.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434891771.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434977488.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.439167968.000000000599B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnese	g0dvHLi4bP.exe, 00000000.00000003.437207014.0000000005988000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn;	g0dvHLi4bP.exe, 00000000.00000003.437408108.0000000005987000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000002.507431111.0000000005980000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.492845361.0000000005980000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0r	g0dvHLi4bP.exe, 00000000.00000003.440198384.000000000598B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.440096725.000000000598B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comTTF	g0dvHLi4bP.exe, 00000000.00000003.447425136.0000000005988000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.446963602.0000000005987000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	g0dvHLi4bP.exe, 00000000.00000003.434322634.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435735907.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434263544.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436481267.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434449814.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435975473.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.438134623.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436182054.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435045732.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434508936.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435924012.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435216005.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.439477892.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436845818.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.438504418.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434538231.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436004358.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.438993924.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434891771.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434977488.000000000599B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/:	g0dvHLi4bP.exe, 00000000.00000003.440198384.000000000598B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.440096725.000000000598B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.wikipediaN	g0dvHLi4bP.exe, 00000000.00000003.433882247.00000000059A3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/d	g0dvHLi4bP.exe, 00000000.00000003.440198384.000000000598B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.440096725.000000000598B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	AheGmkp.exe, 00000018.00000002.705211628.0000000003091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

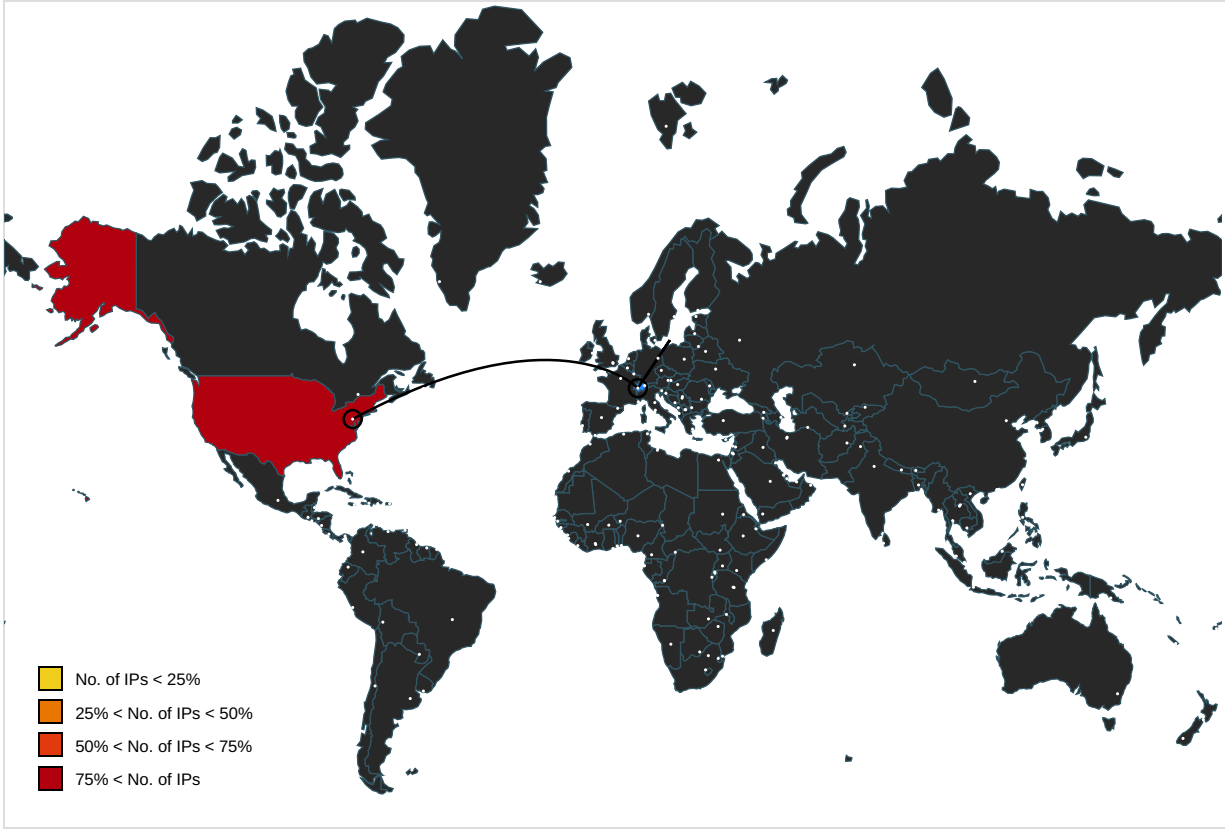
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comgrito	g0dvHLi4bP.exe, 00000000.00000003.458208870.000000000598A000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000002.507431111.0000000005980000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.492845361.0000000005980000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com5	g0dvHLi4bP.exe, 00000000.00000003.458208870.000000000598A000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000002.507431111.0000000005980000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.492845361.0000000005980000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/V	g0dvHLi4bP.exe, 00000000.00000003.440198384.000000000598B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.440096725.000000000598B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	g0dvHLi4bP.exe, 00000000.00000002.501848453.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000002.502149951.0000000002B5E000.00000004.00000800.00020000.00000000.sdmp, AheGmkp.exe, 0000000C.00000002.603631401.0000000002B91000.00000004.00000800.00020000.00000000.sdmp, AheGmkp.exe, 0000000C.00000002.604682206.0000000002D5C000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.come	g0dvHLi4bP.exe, 00000000.00000003.434322634.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435735907.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434263544.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436481267.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434449814.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435975473.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.438134623.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436182054.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435045732.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434508936.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435924012.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435216005.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.439477892.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436845818.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.438504418.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434538231.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436004358.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.438993924.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434891771.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434977488.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434167177.000000000599B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	g0dvHLi4bP.exe, 00000008.00000002.704236786.0000000003021000.00000004.00000800.00020000.00000000.sdmp, AheGmkp.exe, 00000018.00000002.705211628.0000000003091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	g0dvHLi4bP.exe, 00000008.00000002.705876237.000000000337A000.00000004.00000800.00020000.00000000.sdmp, AheGmkp.exe, 00000018.00000003.646298713.0000000001425000.00000004.00000020.00020000.00000000.sdmp, AheGmkp.exe, 00000018.00000002.706376253.00000000033E6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comlicF	g0dvHLi4bP.exe, 00000000.00000003.447425136.0000000005988000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.446963602.0000000005987000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comk-s	g0dvHLi4bP.exe, 00000000.00000003.434322634.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435735907.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434263544.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436481267.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434449814.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435975473.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.438134623.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436182054.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435045732.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434508936.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435924012.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.435216005.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.439477892.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436845818.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.438504418.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434538231.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436004358.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.438993924.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434891771.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.434977488.000000000599B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.439167968.000000000599B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	g0dvHLi4bP.exe, 00000000.00000003.447425136.0000000005988000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000002.507828493.0000000006C12000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.446963602.0000000005987000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comF	g0dvHLi4bP.exe, 00000000.00000003.446963602.0000000005987000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	g0dvHLi4bP.exe, 00000008.00000002.705876237.000000000337A000.00000004.00000800.00020000.00000000.sdmp, AheGmkp.exe, 00000018.00000003.646298713.0000000001425000.00000004.00000020.00020000.00000000.sdmp, AheGmkp.exe, 00000018.00000002.706376253.00000000033E6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%appdata	AheGmkp.exe, 00000018.00000002.705211628.0000000003091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	g0dvHLi4bP.exe, 00000008.00000002.704236786.0000000003021000.00000004.00000800.00020000.00000000.sdmp, AheGmkp.exe, 00000018.00000002.705211628.0000000003091000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/	g0dvHLi4bP.exe, 00000000.00000003.440096725.000000000598B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	g0dvHLi4bP.exe, 00000000.00000003.447425136.0000000005988000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.458208870.000000000598A000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.446963602.0000000005987000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.come.com	g0dvHLi4bP.exe, 00000000.00000003.458208870.000000000598A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	g0dvHLi4bP.exe, 00000000.00000003.434389436.0000000005986000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	g0dvHLi4bP.exe, 00000000.00000002.507828493.000000006C12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	g0dvHLi4bP.exe, 00000000.00000002.507828493.000000006C12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	g0dvHLi4bP.exe, 00000000.00000002.507828493.000000006C12000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.437408108.0000000005987000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.436963733.0000000005987000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.437207014.0000000005988000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	g0dvHLi4bP.exe, 00000000.00000002.507828493.000000006C12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://KMYoUX.com	AheGmkp.exe, 00000018.00000002.705211628.0000000003091000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comt	g0dvHLi4bP.exe, 00000000.00000003.447425136.0000000005988000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.446963602.0000000005987000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	g0dvHLi4bP.exe, 00000000.00000003.440096725.000000000598B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	g0dvHLi4bP.exe, 00000000.00000002.507828493.000000006C12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ocsp.sectigo.com0A	g0dvHLi4bP.exe, 00000008.00000002.705876237.000000000337A000.00000004.00000800.00020000.00000000.sdmp, AheGmkp.exe, 00000018.00000003.646298713.0000000001425000.00000004.00000020.00020000.00000000.sdmp, AheGmkp.exe, 00000018.00000002.706376253.00000000033E6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalic	g0dvHLi4bP.exe, 00000000.00000003.447425136.0000000005988000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.446963602.0000000005987000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/_	g0dvHLi4bP.exe, 00000000.00000003.440198384.000000000598B000.00000004.00000800.00020000.00000000.sdmp, g0dvHLi4bP.exe, 00000000.00000003.440096725.000000000598B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.222.225.29	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
162.222.225.16	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620365
Start date and time: 04/05/202216:58:27	2022-05-04 16:58:27 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	g0dvHLi4bP (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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@23/15@2/3
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.2%) • Quality average: 66.5% • Quality standard deviation: 39.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.152.110.14, 52.242.101.226, 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Execution Graph export aborted for target AheGmkp.exe, PID 6104 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: g0dvHLi4bP.exe

Simulations

Behavior and APIs

Time	Type	Description
16:59:56	API Interceptor	551x Sleep call for process: g0dvHLi4bP.exe modified
17:00:03	API Interceptor	54x Sleep call for process: powershell.exe modified
17:00:18	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run AheGmkp C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe
17:00:26	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run AheGmkp C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe
17:00:33	API Interceptor	263x Sleep call for process: AheGmkp.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\AheGmkp.exe.log

Process:	C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
Reputation:	unknown
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,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\g0dvHLi4bP.exe.log

Process:	C:\Users\user\Desktop\g0dvHLi4bP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE8:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHJ
MD5:	EA78C102145ED608EF0E407B978AF339
SHA1:	66C9179ED9675B9271A97AB1FC878077E09AB731
SHA-256:	8BF01E0C445BD07C0B4EDC7199B7E17DAF1CA55CA52D4A6EAC4EF211C2B1A73E
SHA-512:	8C04139A1FC3C3BDACB680EC443615A43EB18E73B5A0CFCA644CB4A5E71746B275B3E238DD1A5A205405313E457BB75F9BBB93277C67AFA5D78DCFA30E5DA02B
Malicious:	**true**
Reputation:	unknown
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,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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=b77a

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):	22136
Entropy (8bit):	5.597822703095696
Encrypted:	false
SSDEEP:	384:rtCDXq0+++NURn/Jvbc1S0ncjultIUMptQCvjg3hInUML+mfmAV7edMDS5ZQvnI2:Hen/F+TcCltn0K066fK6pk7+1
MD5:	B70ECAE7C579586D29CC3A2E7A951E8D
SHA1:	2E80B12AD6A3815720063BE0596D7E767BC5DC71

SHA-256:	D0057D879F3C464632DA27A3CF4052068A35D5CB2EC249C904850291C72E37F2
SHA-512:	9F8E625D2BB43EBC607F0CC460A6DC195DA0604A7A56D63788FD04BDB18EF36CCBADBB7B442F4C193FF5373FE5C40C185510101A07578DE64D6C6FE60297A278
Malicious:	false
Reputation:	unknown
Preview:	@...e.....W.....{.s.....n...&.\.....@.....H.....<@.^.L."My...:B..... .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_jbaicfx1.xuw.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:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_up2wzwhf.0gz.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_v2bqczrd.h4q.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:	unknown

Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wlxjtc3d.5pt.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp972C.tmp

Process:	C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1603
Entropy (8bit):	5.134080332336202
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtjxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTdv
MD5:	904679853A08670AB337ACD5326AE5EC
SHA1:	42D1F905EA56C74288A9B79BAE92980F032E52BF
SHA-256:	67CA6167D39906C125752E95BACF21D6173A4FEBF2242130733391BB51124B86
SHA-512:	274D3DF62321515C671D9C3C2F3F20E59ABB36042A423126890C8929F0096FB0E3EA037DDA57713B0E9BAC5511D0B2F9441A09F187B7B7F678D726638AA491D5
Malicious:	false
Reputation:	unknown
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</StartWhenAvailable>.

C:\Users\user\AppData\Local\Temp\tmpF6C5.tmp

Process:	C:\Users\user\Desktop\g0dvHLi4bP.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1603
Entropy (8bit):	5.134080332336202
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtjxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTdv
MD5:	904679853A08670AB337ACD5326AE5EC
SHA1:	42D1F905EA56C74288A9B79BAE92980F032E52BF
SHA-256:	67CA6167D39906C125752E95BACF21D6173A4FEBF2242130733391BB51124B86
SHA-512:	274D3DF62321515C671D9C3C2F3F20E59ABB36042A423126890C8929F0096FB0E3EA037DDA57713B0E9BAC5511D0B2F9441A09F187B7B7F678D726638AA491D5
Malicious:	**true**
Reputation:	unknown
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</StartWhenAvailable>.

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

Process:	C:\Users\user\Desktop\g0dvHLi4bP.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	536064
Entropy (8bit):	7.963464056116047
Encrypted:	false
SSDEEP:	12288:P2L2I3WfZbHLfAFrv3fjx5u45RXKmMPA6KAzVb9Dg+qyx2H:P25I17A1vtg43KpPA6Nb98+qyx2H
MD5:	4C414B473BCCBBCE2C7CDE00248EA1A1
SHA1:	77BF848D5A1D4D0FDC252AA170E7B8AF19BCC012
SHA-256:	7BB212946FDEB406C7AA8F691405D185065514D5DC1F269F8E409762FF9F6915
SHA-512:	0FA66C53045E9E74D294420D66DEADCAD7EE56D13E33DD90E73B0DE1E6958CD3B5C347E13E85797895BBAC5F23B3CC3926D6B9A75F242EF2379D93230C7B0 9B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....u.....0.."..... .Z@.. ...`....@.. ..... ..@.....@..O....`..<.....?..... .....H.....text...` ... ..."..... ..`.rsrc...<....`.....$.....@..@.rel oc.....@..B.....<@.....H.....<H...0.....x.. .....0.....}.....(.....(.....~....t2.....3...%.r...p.%.~.....%.r...p.%.~.....%.r...p.%.~..... %.r...p.(....o.....r...p.....%.....%.r)..p.%.rG..p.%.rY..p....(.....*...{....rg..p%.-...o..... .....*.0.....{....o.....0...(.....,..r{..p(....&....r...p..r...p(.....,..r...p(....&.v.r...p(.....,. .r...p(....&s.....o.....H.(....&...9...%..:.o.....1.....2...s.....o.....o

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

Process:	C:\Users\user\Desktop\g0dvHLi4bP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

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

Process:	C:\Users\user\Desktop\g0dvHLi4bP.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	536064
Entropy (8bit):	7.963464056116047
Encrypted:	false
SSDEEP:	12288:P2L2I3WfZbHLfAFrv3fjx5u45RXKmMPA6KAzVb9Dg+qyx2H:P25I17A1vtg43KpPA6Nb98+qyx2H
MD5:	4C414B473BCCBBCE2C7CDE00248EA1A1
SHA1:	77BF848D5A1D4D0FDC252AA170E7B8AF19BCC012
SHA-256:	7BB212946FDEB406C7AA8F691405D185065514D5DC1F269F8E409762FF9F6915
SHA-512:	0FA66C53045E9E74D294420D66DEADCAD7EE56D13E33DD90E73B0DE1E6958CD3B5C347E13E85797895BBAC5F23B3CC3926D6B9A75F242EF2379D93230C7B0 9B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....u.....0.."..... .Z@.. ...`....@.. ..... ..@.....@..O....`..<.....?..... .....H.....text...` ... ..."..... ..`.rsrc...<....`.....$.....@..@.rel oc.....@..B.....<@.....H.....<H...0.....x.. .....0.....}.....(.....(.....~....t2.....3...%.r...p.%.~.....%.r...p.%.~.....%.r...p.%.~..... %.r...p.(....o.....r...p.....%.....%.r)..p.%.rG..p.%.rY..p....(.....*...{....rg..p%.-...o..... .....*.0.....{....o.....0...(.....,..r{..p(....&....r...p..r...p(.....,..r...p(....&.v.r...p(.....,. .r...p(....&s.....o.....H.(....&...9...%..:.o.....1.....2...s.....o.....o

C:\Users\user\AppData\Roaming\lyfhOEwABQlG.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\g0dvHLi4bP.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**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220504\PowerShell_transcript.302494.9BrDU9eF.20220504170044.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):	5807
Entropy (8bit):	5.392757491075899
Encrypted:	false
SSDEEP:	96:BZp/AZNsqDo1ZSZ3/AZNsqDo1ZR5PhjZ4/AZNsqDo1ZacRRDZw:k
MD5:	32E8DB16DD68F89E485E50B09244EC15
SHA1:	9D9603BDC78658E9E4224DDFBE085827D4CA5A7E
SHA-256:	987995A1AB28758D3AF5782BEE36DA9657011669D31200ED43EC2B7FDC146757
SHA-512:	6DB9F4B1090662FF98CD6246F1E737F90C46FCFE5D0D0B4697792A661F7E6DF83F01A69DE738DBA7FEA5B183E509098A81B493554DB0179330C83A562DD0928A
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220504170046..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 302494 (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\lyfhOEwABQlG.exe..Process ID: 7028..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: 20220504170046..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\lyfhOEwABQlG.exe..**********..Windows PowerShell transcript start..Start time: 20220504170310..Username: computer\user..RunAs User: DESKTOP-716

C:\Users\user\Documents\20220504\PowerShell_transcript.302494.Si+7UG0m.20220504170002.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):	5807
Entropy (8bit):	5.3977275389029815
Encrypted:	false
SSDEEP:	96:BZS/AZNGqDo1Z3ZB/AZNGqDo1Zi5PhjZa/AZNGqDo1Z3cRRoZT:S
MD5:	6B817459B04BE9489F42E626B6DC8A60
SHA1:	92EB9952E3D42C49FF1617E2D30515F574E608C2
SHA-256:	52D51ABABD9EA021CB841743B99361348CE4FD47A25C17C2000CAC813F8F7789
SHA-512:	3A0E1748F60B6FA3A885B610CF803F5F9BD9B2DE6C86BFD42894B959FC0BE09DCFBAC166634F79109A67E6DD9A6A871FBD67E9F24640694BA2A6024ED92BA029
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220504170003..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 302494 (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\lyfhOEwABQlG.exe..Process ID: 5868..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: 20220504170003..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\lyfhOEwABQlG.exe..**********..Windows PowerShell transcript start..Start time: 20220504170356..Username: computer\user..RunAs User: DESKTOP-716

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.963464056116047
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:	g0dvHLi4bP.exe
File size:	536064
MD5:	4c414b473bccbbce2c7cde00248ea1a1
SHA1:	77bf848d5a1d4d0fdc252aa170e7b8af19bcc012
SHA256:	7bb212946fdeb406c7aa8f691405d185065514d5dc1f269f8e409762ff9f6915
SHA512:	0fa66c53045e9e74d294420d66deadcad7ee56d13e33dd90e73b0de1e6958cd3b5c347e13e85797895bbac5f23b3cc3926d6b9a75f242ef2379d93230c7b0f9b
SSDEEP:	12288:P2L2I3WfZbHLfAFrv3fjx5u45RXKmMPA6KAzVb9Dg+qyx2H:P25I17A1vtg43KpPA6Nb98+qyx2H
TLSH:	8CB4120462F38336FBB972F26A6453C123753A4DB026F6A82C9093EE9CC1B5B5554F53
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....u.....0.."..... Z@... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48405a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xD8BB75AE [Fri Mar 23 05:33:34 2085 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x84008	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x86000	0x63c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x83fec	0x1c	.text
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	0x82060	0x82200	False	0.956357693924	data	7.97222784974	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x63c	0x800	False	0.35009765625	data	3.50595023872	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x86090	0x3ac	data		
RT_MANIFEST	0x8644c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

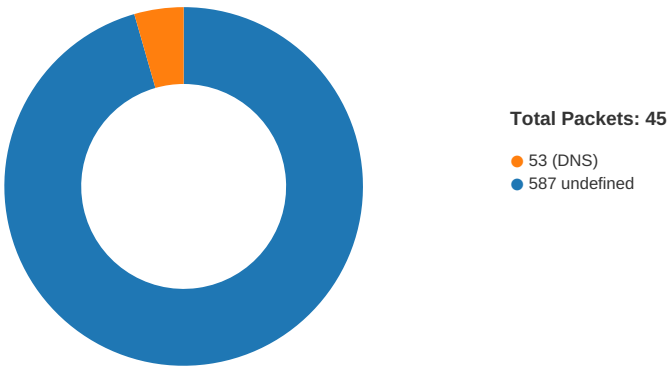
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020-2021 by David Xanatos (xanasoft.com)
Assembly Version	1.0.0.0
InternalName	PolicyExcept.exe
FileVersion	1.0.0.0
CompanyName	sandboxie-plus.com
LegalTrademarks	
Comments	
ProductName	Sandboxie
ProductVersion	1.0.0.0
FileDescription	Sandboxie Installer
OriginalFilename	PolicyExcept.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 17:00:25.724492073 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:25.921848059 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:25.921967983 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:27.126470089 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:27.126799107 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:27.324078083 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:27.324179888 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:27.324503899 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:27.522455931 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:27.581762075 CEST	49782	587	192.168.2.5	162.222.225.16

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 17:00:27.779381037 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:27.779432058 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:27.779459000 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:27.779479980 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:27.779582977 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:27.779632092 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:27.781455994 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:27.856467009 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:27.977020979 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:28.006202936 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:28.204210043 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:28.247243881 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:28.367575884 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:28.565136909 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:28.566299915 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:28.764785051 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:28.767256021 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:28.967353106 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:29.068176985 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:29.074171066 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:29.273842096 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:29.292809010 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:29.502237082 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:29.506899118 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:29.705562115 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:29.706659079 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:29.706773043 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:29.707461119 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:29.707537889 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:00:29.904197931 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:29.904995918 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:30.056780100 CEST	587	49782	162.222.225.16	192.168.2.5
May 4, 2022 17:00:30.247364998 CEST	49782	587	192.168.2.5	162.222.225.16
May 4, 2022 17:01:17.341106892 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:17.538479090 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:17.538868904 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:18.743863106 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:18.746946096 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:18.944420099 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:18.944461107 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:18.950834990 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:19.148854017 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:19.203214884 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:19.400837898 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:19.400871038 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:19.400893927 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:19.400909901 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:19.400974989 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:19.401024103 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:19.403031111 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:19.460330009 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:19.599139929 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:19.604698896 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:19.804348946 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:19.854656935 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:19.952203035 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:20.149756908 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:20.150518894 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:20.349066019 CEST	587	49799	162.222.225.29	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 17:01:20.349889994 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:20.550350904 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:20.550903082 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:20.750528097 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:20.751018047 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:20.965641022 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:20.966207027 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:21.164452076 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:21.165565968 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:21.165731907 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:21.165860891 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:21.165971041 CEST	49799	587	192.168.2.5	162.222.225.29
May 4, 2022 17:01:21.362831116 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:21.362926960 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:21.503638983 CEST	587	49799	162.222.225.29	192.168.2.5
May 4, 2022 17:01:21.663621902 CEST	49799	587	192.168.2.5	162.222.225.29

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 17:00:25.672841072 CEST	62466	53	192.168.2.5	8.8.8.8
May 4, 2022 17:00:25.694880962 CEST	53	62466	8.8.8.8	192.168.2.5
May 4, 2022 17:01:17.260657072 CEST	63241	53	192.168.2.5	8.8.8.8
May 4, 2022 17:01:17.281758070 CEST	53	63241	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2022 17:00:25.672841072 CEST	192.168.2.5	8.8.8.8	0xcc9c	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
May 4, 2022 17:01:17.260657072 CEST	192.168.2.5	8.8.8.8	0xe78b	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2022 17:00:25.694880962 CEST	8.8.8.8	192.168.2.5	0xcc9c	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 4, 2022 17:00:25.694880962 CEST	8.8.8.8	192.168.2.5	0xcc9c	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 4, 2022 17:00:25.694880962 CEST	8.8.8.8	192.168.2.5	0xcc9c	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 4, 2022 17:00:25.694880962 CEST	8.8.8.8	192.168.2.5	0xcc9c	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 4, 2022 17:01:17.281758070 CEST	8.8.8.8	192.168.2.5	0xe78b	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 4, 2022 17:01:17.281758070 CEST	8.8.8.8	192.168.2.5	0xe78b	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 4, 2022 17:01:17.281758070 CEST	8.8.8.8	192.168.2.5	0xe78b	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 4, 2022 17:01:17.281758070 CEST	8.8.8.8	192.168.2.5	0xe78b	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)

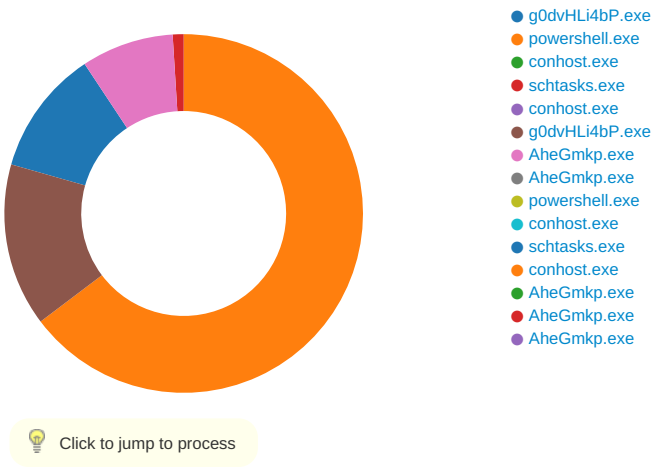
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2022 17:00:27.126470089 CEST	587	49782	162.222.225.16	192.168.2.5	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 4, 2022 17:00:27.126799107 CEST	49782	587	192.168.2.5	162.222.225.16	EHLO 302494

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2022 17:00:27.324179888 CEST	587	49782	162.222.225.16	192.168.2.5	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
May 4, 2022 17:00:27.324503899 CEST	49782	587	192.168.2.5	162.222.225.16	STARTTLS
May 4, 2022 17:00:27.522455931 CEST	587	49782	162.222.225.16	192.168.2.5	220 2.0.0 Ready to start TLS
May 4, 2022 17:01:18.743863106 CEST	587	49799	162.222.225.29	192.168.2.5	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 4, 2022 17:01:18.746946096 CEST	49799	587	192.168.2.5	162.222.225.29	EHLO 302494
May 4, 2022 17:01:18.944461107 CEST	587	49799	162.222.225.29	192.168.2.5	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
May 4, 2022 17:01:18.950834990 CEST	49799	587	192.168.2.5	162.222.225.29	STARTTLS
May 4, 2022 17:01:19.148854017 CEST	587	49799	162.222.225.29	192.168.2.5	220 2.0.0 Ready to start TLS

Statistics

Behavior



System Behavior

Analysis Process: g0dvHLi4bP.exe PID: **7044**, Parent PID: **5212**

General

Target ID:	0
Start time:	16:59:39
Start date:	04/05/2022
Path:	C:\Users\user\Desktop\g0dvHLi4bP.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\Desktop\g0dvHLi4bP.exe"
Imagebase:	0x620000
File size:	536064 bytes
MD5 hash:	4C414B473BCCBBCE2C7CDE00248EA1A1
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: 00000000.00000002.501848453.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.502149951.0000000002B5E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.504524116.0000000003B12000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.504524116.0000000003B12000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	6E42CF06	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	6E42CF06	unknown
C:\Users\user\AppData\Roaming\lyfhOEwABQlG.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	6D27DD66	CopyFileW
C:\Users\user\AppData\Roaming\lyfhOEwABQlG.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6D27DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF6C5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D277038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\g0dvHLi4bP.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E73C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF6C5.tmp	success or wait	1	6D276A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\lyfhOEwABQlG.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 75 fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 22 08 00 00 0a 00 00 00 00 00 00 5a 40 08 00 00 20 00 00 00 60 08 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 08 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.$PELu0"Z@ `@ @	success or wait	3	6D27DD66	CopyFileW
C:\Users\user\AppData\Roaming\lyfhOEwABQlG.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	6D27DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF6C5.tmp	0	1603	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 61 6c 66 6f 6e 73 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 3e 0a	<?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	6D271B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\g0dvHLi4bP.exe.log	0	1308	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	6E73C907	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	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E405705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E40CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D271B4F	ReadFile

Analysis Process: powershell.exe PID: **5868**, Parent PID: **7044**

General

Target ID:	4
Start time:	17:00:00
Start date:	04/05/2022
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\lyfhOEwABQlG.exe
Imagebase:	0x920000
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	6E42CF06	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	6E42CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wlxjtc3d.5pt.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D271E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_v2bqczrd.h4q.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D271E60	CreateFileW
C:\Users\user\Documents\20220504	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D27BEFF	CreateDirectoryW
C:\Users\user\Documents\20220504\PowerShell_transcript.302494.Si+7UG0m.20220504170002.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D271E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wlxjtc3d.5pt.ps1	success or wait	1	6D276A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_v2bqczrd.h4q.psm1	success or wait	1	6D276A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wlxjtc3d.5pt.ps1	0	1	31	1	success or wait	1	6D271B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_v2bqczrd.h4q.psm1	0	1	31	1	success or wait	1	6D271B4F	WriteFile
C:\Users\user\Documents\20220504\PowerShell_transcript.302494.Si+7UG0m.20220504170002.txt	0	3	ff		success or wait	1	6D271B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220504\PowerShell_transcript.302494.Si+7UG0m.20220504170002.txt	3	682	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 35 30 34 31 37 30 30 30 33 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 30 32 34 39 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********Windows PowerShell transcript startStart time: 20220504170003Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 302494 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\	success or wait	44	6D271B4F	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 57 14 00 00 18 00 00 00 7b 0c 73 05 07 07 fd 06 fd 06 00 00 6e 01 fd 00 26 00 5c 0c 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eW{sn&\@	success or wait	1	6E6F76FC	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 42 00 00 00 0e 00 20 00	H<@^L"My:B	success or wait	17	6E6F76FC	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	6E6F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6E6F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6E6F76FC	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 fd 01 40 00 55 00 40 00 47 00 40 00 54 01 40 00 fd 3e 40 01 fd 29 40 01 fd 3f 40 01 fd 6f 40 01 fd 6f 40 01 fd 6f 40 01 fd 3f 40 01 56 00 40 00 fd 01 40 00 fd 00 40 00 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 fd 67 40 01 fd 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 fd 00 40 00 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 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40	@U@G@T@>@)@? @o@o@o@? @V@@@@V@H@ X@g@@[@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@;M@D@D@@M @<M@	success or wait	11	6E6F76FC	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	6E405705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E405705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E40CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E40CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E40CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E405705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E405705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E405705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E405705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E3603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E405705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E411F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23104	success or wait	1	6E41203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3603DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6D271B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6D271B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E405705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E405705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D271B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E405705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E405705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	65	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	11	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6D271B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6D271B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6D271B4F	ReadFile

Analysis Process: conhost.exe PID: **3064**, Parent PID: **5868**

General

Target ID:	5
Start time:	17:00:01
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **5864**, Parent PID: **7044**

General

Target ID:	6
Start time:	17:00:01
Start date:	04/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lyfhOEwABQlG" /XML "C:\Users\user\AppData\Local\Temp\tmpF6C5.tmp
Imagebase:	0xe30000
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\tmpF6C5.tmp	unknown	2	success or wait	1	E3AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF6C5.tmp	unknown	1604	success or wait	1	E3ABD9	ReadFile

Analysis Process: conhost.exe PID: **6388**, Parent PID: **5864**

General

Target ID:	7
Start time:	17:00:02
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: g0dvHLi4bP.exe PID: **5432**, Parent PID: **7044**

General

Target ID:	8
Start time:	17:00:04
Start date:	04/05/2022
Path:	C:\Users\user\Desktop\g0dvHLi4bP.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\g0dvHLi4bP.exe
Imagebase:	0xbd0000
File size:	536064 bytes
MD5 hash:	4C414B473BCCBBCE2C7CDE00248EA1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.487111726.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.487111726.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.488270274.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.488270274.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.487666234.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.487666234.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.489038629.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.489038629.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.696067771.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.696067771.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.704236786.0000000003021000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.704236786.0000000003021000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	6E42CF06	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	6E42CF06	unknown
C:\Users\user\AppData\Roaming\AheGmkp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D27BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.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	6D27DD66	CopyFileW
C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6D27DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe:Zone.Identifier	success or wait	1	637682A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.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 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 75 fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 22 08 00 00 0a 00 00 00 00 00 00 5a 40 08 00 00 20 00 00 00 60 08 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 08 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.$PELu0"Z@ `@ @	success or wait	3	6D27DD66	CopyFileW
C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.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	6D27DD66	CopyFileW

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	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E405705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E40CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6D271B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c3d0bcad-59c3-41fa-89dd-89b9005799af	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6D271B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D271B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D271B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	AheGmkp	unicode	C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe	success or wait	1	6D27646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	AheGmkp	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6D27DE2E	RegSetValueExW

Analysis Process: AheGmkp.exe PID: **6920**, Parent PID: **684**

General

Target ID:	12
Start time:	17:00:26
Start date:	04/05/2022
Path:	C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe"
Imagebase:	0x780000
File size:	536064 bytes
MD5 hash:	4C414B473BCCBBCE2C7CDE00248EA1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.606786408.0000000003CE2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000002.606786408.0000000003CE2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000C.00000002.603631401.0000000002B91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000C.00000002.604682206.0000000002D5C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 31%, ReversingLabs
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	6E42CF06	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	6E42CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp972C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D277038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp972C.tmp	success or wait	1	6D276A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp972C.tmp	0	1603	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 6c 6f 6e 65 73 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 3e 0a	<?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	6D271B4F	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	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E405705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E40CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E405705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D271B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D271B4F	ReadFile

Analysis Process: AheGmkp.exe PID: **6188**, Parent PID: **684**

General

Target ID:	15
Start time:	17:00:35
Start date:	04/05/2022
Path:	C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe"
Imagebase:	0xc50000
File size:	536064 bytes
MD5 hash:	4C414B473BCCBBCE2C7CDE00248EA1A1
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: 0000000F.00000002.594985042.00000000031F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: powershell.exe PID: 7028, Parent PID: 6920

General	
Target ID:	17
Start time:	17:00:41
Start date:	04/05/2022
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\lyfhOEwABQlG.exe
Imagebase:	0x920000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 5324, Parent PID: 7028

General	
Target ID:	18
Start time:	17:00:42
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 4952, Parent PID: 6920

General	
Target ID:	19
Start time:	17:00:44
Start date:	04/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lyfhOEwABQlG" /XML "C:\Users\user\AppData\Local\Temp\tmp972C.tmp
Imagebase:	0xe30000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6684, Parent PID: 4952

General

Target ID:	21
Start time:	17:00:46
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AheGmkp.exe PID: **6104**, Parent PID: **6920**

General	
Target ID:	22
Start time:	17:00:52
Start date:	04/05/2022
Path:	C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe
Imagebase:	0x410000
File size:	536064 bytes
MD5 hash:	4C414B473BCCBBCE2C7CDE00248EA1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AheGmkp.exe PID: **5944**, Parent PID: **6920**

General	
Target ID:	23
Start time:	17:00:54
Start date:	04/05/2022
Path:	C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe
Imagebase:	0x340000
File size:	536064 bytes
MD5 hash:	4C414B473BCCBBCE2C7CDE00248EA1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AheGmkp.exe PID: **7068**, Parent PID: **6920**

General	
Target ID:	24
Start time:	17:00:55
Start date:	04/05/2022
Path:	C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\AheGmkp\AheGmkp.exe
Imagebase:	0xbf0000
File size:	536064 bytes

MD5 hash:	4C414B473BCCBBCE2C7CDE00248EA1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000000.596334236.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000018.00000000.596334236.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000000.595827903.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000018.00000000.595827903.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000000.596964511.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000018.00000000.596964511.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000002.705211628.0000000003091000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000018.00000002.705211628.0000000003091000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000002.696078477.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000018.00000002.696078477.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000000.595144687.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000018.00000000.595144687.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly