Research Incident response Microsoft Incident Response Ransomware

17 min read

# The five-day job: A BlackByte ransomware intrusion case study

By Microsoft Incident Response

July 6, 2023

Threat intelligence Microsoft 365 Defender Microsoft Defender more

As ransomware attacks continue to grow in number and sophistication, threat actors can quickly impact business operations if organizations are not well prepared. In a recent investigation by Microsoft Incident Response (previously known as Microsoft Detection and Response Team – DART) of an intrusion, we found that the threat actor progressed through the full attack chain, from initial access to impact, in less than five days, causing significant business disruption for the victim organization.

Our investigation found that within those five days, the threat actor employed a range of tools and techniques, culminating in the deployment of BlackByte 2.0 ransomware, to achieve their objectives. These techniques included:

- Exploitation of unpatched internet-exposed Microsoft Exchange Servers
- Web shell deployment facilitating remote access
- Use of living-off-the-land tools for persistence and reconnaissance
- Deployment of Cobalt Strike beacons for command and control (C2)
- Process hollowing and the use of vulnerable drivers for defense evasion
- Deployment of custom-developed backdoors to facilitate persistence
- Deployment of a custom-developed data collection and exfiltration tool

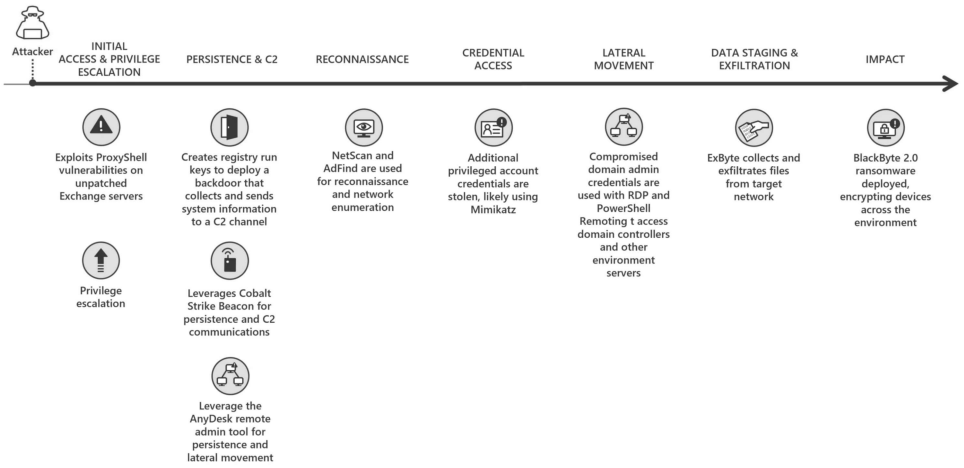


Figure 1. BlackByte 2.0 ransomware attack chain

In this blog, we share details of our investigation into the end-to-end attack chain, exposing security weaknesses that the threat actor exploited to advance their attack. As we learned from Microsoft's tracking of ransomware attacks and the cybercriminal economy that enables them, disrupting common attack patterns could stop many of the attacker activities that precede ransomware deployment. This case highlights that common security hygiene practices go a long way in preventing, identifying, and responding to malicious activity as early as possible to mitigate the impact of ransomware attacks. We encourage organizations to follow the outlined mitigation steps, including ensuring that internet-facing assets are up to date and configured securely. We also share indicators of compromise, detection details, and hunting guidance to help organizations identify and respond to these attacks in their environments.

# Forensic analysis

## Initial access and privilege escalation

To obtain initial access into the victim's environment, the threat actor was observed exploiting the ProxyShell vulnerabilities CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207 on unpatched Microsoft Exchange Servers. The exploitation of these vulnerabilities allowed the threat actor to:

- Attain system-level privileges on the compromised Exchange host
- Enumerate LegacyDN of users by sending Autodiscover requests, including SIDs of users
- Construct a valid authentication token and use it against the Exchange PowerShell backend
- Impersonate domain admin users and create a web shell by using the *New-MailboxExportRequest* cmdlet
- Create web shells to obtain remote control on affected servers

The threat actor was observed operating from the following IP to exploit ProxyShell and access the web shell:

- 185.225.73[.]244

## Persistence

**Backdoor**

After gaining access to a device, the threat actor created the following registry run keys to run a payload each time a user signs in:

| Registry key | Value name | Value data |
|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run | MsEdgeMsE | rundll32 C:\Users\user\Downloads\api-msvc.dll,Default |

| | | |
|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run | MsEdgeMsE | rundll32 C:\temp\api-msvc.dll,Default |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run | MsEdgeMsE | rundll32 C:\systemtest\api-system.png,Default |

The file *api-msvc.dll* (SHA-256: 4a066569113a569a6feb8f44257ac8764ee8f2011765009fdfd82fe3f4b92d3e) was determined to be a backdoor capable of collecting system information, such as the installed antivirus products, device name, and IP address. This information is then sent via HTTP POST request to the following C2 channel:

- *hxxps://myvisit[.]alteksecurity[.]org/t*

The organization was not using Microsoft Defender Antivirus, which detects this malware as Trojan:Win32/Kovter!MSR, as the primary antivirus solution, and the backdoor was allowed to run.

An additional file, *api-system.png*, was identified to have similarities to *api-msvc.dll*. This file behaved like a DLL, had the same default export function, and also leveraged run keys for persistence.

**Cobalt Strike Beacon**

The threat actor leveraged Cobalt Strike to achieve persistence. The file *sys.exe* (SHA-256: 5f37b85687780c089607670040dbb3da2749b91b8adc0aa411fd6280b5fa7103), detected by Microsoft Defender Antivirus as Trojan:Win64/CobaltStrike!MSR, was determined to be a Cobalt Strike Beacon and was downloaded directly from the file sharing service *temp[.]sh*:

- *hxxps://temp[.]sh/szAyn/sys.exe*

This beacon was configured to communicate with the following C2 channel:

- 109.206.243[.]59:443

**AnyDesk**

Threat actors leverage legitimate remote access tools during intrusions to blend into a victim network. In this case, the threat actor utilized the remote administration tool AnyDesk, to maintain persistence and move laterally within the network. AnyDesk was installed as a service and was run from the following paths:

- *C:\systemtest\anydesk\AnyDesk.exe*
- *C:\Program Files (x86)\AnyDesk\AnyDesk.exe*
- *C:\Scripts\AnyDesk.exe*

Successful connections were observed in the AnyDesk log file *ad_svc.trace* involving anonymizer service IP addresses linked to TOR and MULLVAD VPN, a common technique that threat actors employ to obscure their source IP ranges.

## Reconnaissance

We found the presence and execution of the network discovery tool NetScan being used by the threat actor to perform network enumeration using the following file names:

- *netscan.exe* (SHA-256:1b9badb1c646a19cdf101ac4f6fdd23bc61eaab8c9f925eb41848cea9fd0738e)
- *netapp.exe* (SHA-256:1b9badb1c646a19cdf101ac4f6fdd23bc61eaab8c9f925eb41848cea9fd0738e)

Additionally, execution of AdFind (SHA-256: f157090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455e), an Active Directory reconnaissance tool, was observed in the environment.

## Credential access

Evidence of likely usage of the credential theft tool Mimikatzwas also uncovered through the presence of a related log file *mimikatz.log*. Microsoft IR assesses that Mimikatz was likely used to attain credentials for privileged accounts.

## Lateral movement

Using compromised domain admin credentials, the threat actor used Remote Desktop Protocol (RDP) and PowerShell remoting to obtain access to other servers in the environment, including domain controllers.

## Data staging and exfiltration

In one server where Microsoft Defender Antivirus was installed, a suspicious file named *explorer.exe* was identified, detected as Trojan:Win64/WinGoObfusc.LK!MT, and quarantined. However, because tamper protection wasn't enabled on this server, the threat actor was able to disable the Microsoft Defender Antivirus service, enabling the threat actor to run the file using the following command:

explorer.exe P@$$w0rd

After reverse engineering *explorer.exe*, we determined it to be ExByte, a GoLang-based tool developed and commonly used in BlackByte ransomware attacks for collection and exfiltration of files from victim networks. This tool is capable of enumerating files of interest across the network and, upon execution, creates a log file containing a list of files and associated metadata. Multiple log files were uncovered during the investigation in the path:

- *C:\Exchange\MSExchLog.log*

Analysis of the binary revealed a list of file extensions that are targeted for enumeration.

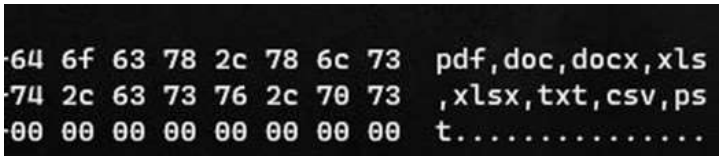


Figure 2. Binary analysis showing file extensions enumerated by *explorer.exe*

Forensic analysis identified a file named *data.txt* that was created and later deleted after ExByte execution. This file contained obfuscated credentials that ExByte leveraged to authenticate to the popular file sharing platform Mega NZ using the platform's API at:

- *hxxps://g.api.mega.co[.]nz*

```
char *__fastcall decodeMegaDomain(__int64 a1)
{
  __int64 v1; // r14
  void *v2; // rax
  __int64 v4; // [rsp-40h] [rbp-A8h]
  __int64 v5[4]; // [rsp+40h] [rbp-28h] BYREF

  if ( v5 <= *(v1 + 16) )
    runtime_morestack_noctxt(a1);
  v5[0] = 0x6BCB26650E75CCBi64;
  v5[1] = 0x482DFFCB3A84B973i64;
  v5[2] = 0x238600C953313797i64;
  v5[3] = 0xFE95A7C665DF2E3i64;
  runtime_growslice(v4);
  qmemcpy(v2, "https://g.api.mega.co.nz", 24);
  return runtime_slicebytetostring(24i64);
}
```

Figure 3. Binary analysis showing explorer.exe functionality for connecting to file sharing service MEGA NZ

We also determined that this version of Exbyte was crafted specifically for the victim, as it contained a hardcoded device name belonging to the victim and an internal IP address.

**ExByte execution flow**

Upon execution, ExByte decodes several strings and checks if the process is running with privileged access by reading \\.*PHYSICALDRIVE0*:

- If this check fails, *ShellExecuteW* is invoked with the *lpOperation* parameter *RunAs*, which runs *explorer.exe* with elevated privileges.

After this access check, *explorer.exe* attempts to read the *data.txt* file in the current location:

- If the text file doesn't exist, it invokes a command for self-deletion and exits from memory:

```
C:\Windows\system32\cmd.exe /c ping 1.1.1.1 -n 10 > nul & Del <PATH>\explorer.exe
```

- If *data.txt* exists, *explorer.exe* reads the file, passes the buffer to Base64 decode function, and then decrypts the data using the key provided in the command line. The decrypted data is then parsed as JSON below and fed for login function:

```
{
    "a":"us0",
    "user":"<CONTENT FROM data.txt>"
}
```

Finally, it forms a URL for sign-in to the API of the service MEGA NZ:

- *hxxps://g.api.mega.co[.]nz/cs?id=1674017543*

## Data encryption and destruction

On devices where files were successfully encrypted, we identified suspicious executables, detected by Microsoft Defender Antivirus as Trojan:Win64/BlackByte!MSR, with the following names:

- *wEFT.exe*
- *schillerized.exe*

The files were analyzed and determined to be BlackByte 2.0 binaries responsible for encryption across the environment. The binaries require an 8-digit key number to encrypt files.

Two modes of execution were identified:

- When the *-s* parameter is provided, the ransomware self-deletes and encrypts the machine it was executed on.
- When the *-a* parameter is provided, the ransomware conducts enumeration and uses an Ultimate Packer Executable (UPX) packed version of PsExec to deploy across the network. Several domain admin credentials were hardcoded in the binary, facilitating the deployment of the binary across the network.

Depending on the switch (*-s* or *-a*), execution may create the following files:

- *C:\SystemData\M8yl89s7.exe* (UPX-packed PsExec with a random name; SHA-256: ba3ec3f445683d0d0407157fda0c26fd669c0b8cc03f21770285a20b3133098f)
- *C:\SystemData\wEFT.exe* (Additional BlackByte binary)
- *C:\SystemData\MsExchangeLog1.log* (Log file)
- *C:\SystemData\rENEgOtiAtES* (A vulnerable (CVE-2019-16098) driver *RtCore64.sys* used to evade detection by installed antivirus software; SHA-256: 01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd)
- *C:\SystemData\iHu6c4.ico* (Random name – BlackBytes icon)
- *C:\SystemData\BB_Readme_file.txt* (BlackByte ReadMe file)
- *C:\SystemData\skip_bypass.txt* (Unknown)

**BlackByte 2.0 ransomware capabilities**

Some capabilities identified for the BlackByte 2.0 ransomware were:

- Antivirus bypass
  - The file *rENEgOtiAtES* created matches *RTCore64.sys*, a vulnerable driver (CVE-2049-16098) that allows any authenticated user to read or write to arbitrary memory
  - The BlackByte binary then creates and starts a service named *RABAsSaa* calling *rENEgOtiAtES*, and exploits this service to evade detection by installed antivirus software
- Process hollowing

    - Invokes *svchost.exe*, injects to it to complete device encryption, and self-deletes by executing the following command:
        - `cmd.exe /c ping 1.1.1.1 -n 10 > Nul & Del "PATH_TO_BLACKBYTE" /F /Q`
- Modification / disabling of Windows Firewall
    - The following commands are executed to either modify existing Windows Firewall rules, or to disable Windows Firewall entirely:
        - `cmd /c netsh advfirewall set allprofiles state off`
        - `cmd /c netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes`
        - `cmd /c netsh advfirewall firewall set rule group="Network Discovery" new enable=Yes`
- Modification of volume shadow copies
    - The following commands are executed to destroy volume shadow copies on the machine:
        - `cmd /c vssadmin Resize ShadowStorge /For=B:\ /On=B:\ /MaxSize=401MB`
        - `cmd /c vssadmin Resize ShadowStorage /For=B:\ /On=B:\ /MaxSize=UNBOUNDED`
- Modification of registry keys/values
    - The following commands are executed to modify the registry, facilitating elevated execution on the device:
        - `cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f`
        - `cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLinkedConnections /t REG_DWORD /d 1 /f`
        - `cmd /c reg add HKLM\\SYSTEM\\CurrentControlSet\\Control\\FileSystem /v LongPathsEnabled /t REG_DWORD /d 1 /f`
- Additional functionality
    - Ability to terminate running services and processes
    - Ability to enumerate and mount volumes and network shares for encryption
    - Perform anti-forensics technique timestomping (sets the file time of encrypted and ReadMe file to 2000-01-01 00:00:00)
    - Ability to perform anti-debugging techniques

## Recommendations

To guard against BlackByte ransomware attacks, Microsoft recommends the following:

- Ensure that you have a patch management process in place and that patching for internet-exposed devices is prioritized; Understand and assess your cyber exposure with advanced vulnerability and configuration assessment tools like Microsoft Defender Vulnerability Management
- Implement an endpoint detection and response (EDR) solution like Microsoft Defender for Endpoint to gain visibility into malicious activity in real time across your network
- Ensure antivirus protections are updated regularly by turning on cloud-based protection and that your antivirus solution is configured to block threats
- Enable tamper protection to prevent components of Microsoft Defender Antivirus from being disabled
- Block inbound traffic from IPs specified in the indicators of compromise section of this report
- Block inbound traffic from TOR exit nodes
- Block inbound access from unauthorized public VPN services
- Restrict administrative privileges to prevent authorized system changes

## Conclusion

BlackByte ransomware attacks target organizations that have infrastructure with unpatched vulnerabilities.  As outlined in the Microsoft Digital Defense Report, common security hygiene practices, including keeping systems up to date, could protect against 98% of attacks.

As new tools are being developed by threat actors, a modern threat protection solution like Microsoft 365 Defender is necessary to prevent and detect the multiple techniques used in the attack chain, especially where the threat actor attempts to evade or disable specific defense mechanisms. Hunting for malicious behavior should be performed regularly in order to detect potential attacks that could evade detections, as a complementary activity for continuous monitoring from security tools alerts and incidents.

To understand how Microsoft can help you secure your network and respond to network compromise, visit https://aka.ms/MicrosoftIR.

## Microsoft 365 Defender detections

**Microsoft Defender Antivirus**

Microsoft Defender Antivirus detects this threat as the following malware:

- Trojan:Win32/Kovter!MSR
- Trojan:Win64/WinGoObfusc.LK!MT
- Trojan:Win64/BlackByte!MSR
- HackTool:Win32/AdFind!MSR
- Trojan:Win64/CobaltStrike!MSR

**Microsoft Defender for Endpoint**

The following alerts might indicate threat activity related to this threat. Note, however, that these alerts can be also triggered by unrelated threat activity.

- 'CVE-2021-31207' exploit malware was detected
- An active 'NetShDisableFireWall' malware in a command line was prevented from executing.
- Suspicious registry modification.
- 'Rtcore64' hacktool was detected
- Possible ongoing hands-on-keyboard activity (Cobalt Strike)
- A file or network connection related to a ransomware-linked emerging threat activity group detected
- Suspicious sequence of exploration activities
- A process was injected with potentially malicious code
- Suspicious behavior by cmd.exe was observed
- 'Blackbyte' ransomware was detected

**Microsoft Defender Vulnerability Management**

Microsoft Defender Vulnerability Management surfaces devices that may be affected by the following vulnerabilities used in this threat:

- CVE-2021-34473
- CVE-2021-34523
- CVE-2021-31207
- CVE-2019-16098

## Hunting queries

**Microsoft 365 Defender**

Microsoft 365 Defender customers can run the following query to find related activity in their networks:

**ProxyShell web shell creation events**

```
DeviceProcessEvents
| where ProcessCommandLine has_any ("ExcludeDumpster","New-ExchangeCertificate")
```

**Suspicious vssadmin events**

```
DeviceProcessEvents
| where ProcessCommandLine has_any ("vssadmin","vssadmin.exe") and ProcessCommanc
```

**Detection for persistence creation using Registry Run keys**

```
DeviceRegistryEvents
| where ActionType == "RegistryValueSet"
| where (RegistryKey has @"Microsoft\Windows\CurrentVersion\RunOnce" and Registry
    or (RegistryKey has @"Microsoft\Windows\CurrentVersion\RunOnceEx" and Registr
    or (RegistryKey has @"Microsoft\Windows\CurrentVersion\Run" and RegistryValue
| where RegistryValueData startswith @"rundll32"
| where RegistryValueData endswith @".dll,Default"
| project Timestamp,DeviceId,DeviceName,ActionType,RegistryKey,RegistryValueName,
```

**Microsoft Sentinel**

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with 'TI map') to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace. More details on the Content Hub can be found here: https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy

Microsoft Sentinel also has a range of detection and threat hunting content that customers can use to detect the post exploitation activity detailed in this blog in addition to Microsoft 365 Defender detections list above.

- ProxyShell
- Web shell activity
- Suspicious file downloads on Exchange Servers
- Firewall rule changes
- Shadow copy deletion
- Anamolous RDP activity

## Indicators of compromise

The table below shows IOCs observed during our investigation. We encourage our customers to investigate these indicators in their environments and implement detections and protections to identify past related activity and prevent future attacks against their systems.

| Indicator | Type | Description |
|---|---|---|
| 4a066569113a569a6feb8f44257ac8764ee8f2011765009fdfd82fe3f4b92d3e | SHA-256 | api-msvc.dll (Backdoor installed through RunKeys) |
| 5f37b85687780c089607670040dbb3da2749b91b8adc0aa411fd6280b5fa7103 | SHA-256 | sys.exe (Cobalt Strike Beacon) |
| 01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd | SHA-256 | rENEgOtiAtES (Vulnerable driver RtCore64.sys created by BlackByte binary) |
| ba3ec3f445683d0d0407157fda0c26fd669c0b8cc03f21770285a20b3133098f | SHA-256 | [RANDOM_NAME].exe (UPX Packed PsExec created by BlackByte binary) |
| 1b9badb1c646a19cdf101ac4f6fdd23bc61eaab8c9f925eb41848cea9fd0738e | SHA-256 | "netscan.exe", "netapp.exe (Netscan network discovery tool) |

| | | |
|---|---|---|
| f157090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455e | SHA-256 | AdFind.exe (Active Directory information gathering tool) |
| hxxps://myvisit[.]alteksecurity[.]org/t | URL | C2 for backdoor api-msvc.dll |
| hxxps://temp[.]sh/szAyn/sys.exe | URL | Download URL for sys.exe |
| 109.206.243[.]59 | IP Address | C2 for Cobalt Strike Beacon sys.exe |
| 185.225.73[.]244 | IP Address | Originating IP address for ProxyShell exploitation and web shell interaction |

**NOTE:** These indicators should not be considered exhaustive for this observed activity.

## Appendix

File extensions targeted by BlackByte binary for encryption:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| .4dd | .4dl | .accdb | .accdc | .accde | .accdr | .accdt | .accft |
| .adb | .ade | .adf | .adp | .arc | .ora | .alf | .ask |
| .btr | .bdf | .cat | .cdb | .ckp | .cma | .cpd | .dacpac |
| .dad | .dadiagrams | .daschema | .db | .db-shm | .db-wal | .db3 | .dbc |
| .dbf | .dbs | .dbt | .dbv | . dbx | . dcb | . dct | . dcx |
| . ddl | . dlis | . dp1 | . dqy | . dsk | . dsn | . dtsx | . dxl |
| . eco | . ecx | . edb | . epim | . exb | . fcd | . fdb | . fic |
| . fmp | . fmp12 | . fmpsl | . fol | .fp3 | . fp4 | . fp5 | . fp7 |
| . fpt | . frm | . gdb | . grdb | . gwi | . hdb | . his | . ib |
| . idb | . ihx | . itdb | . itw | . jet | . jtx | . kdb | . kexi |
| . kexic | . kexis | . lgc | . lwx | . maf | . maq | . mar | . masmav |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| . mdb | . mpd | . mrg | . mud | . mwb | . myd | . ndf | . nnt |
| . nrmlib | . ns2 | . ns3 | . ns4 | . nsf | . nv | . nv2 | . nwdb |
| . nyf | . odb | . ogy | . orx | . owc | . p96 | . p97 | . pan |
| . pdb | . pdm | . pnz | . qry | . qvd | . rbf | . rctd | . rod |
| . rodx | . rpd | . rsd | . sas7bdat | . sbf | . scx | . sdb | . sdc |
| . sdf | . sis | . spg | . sql | . sqlite | . sqlite3 | . sqlitedb | . te |
| . temx | . tmd | . tps | . trc | . trm | . udb | . udl | . usr |
| . v12 | . vis | . vpd | . vvv | . wdb | . wmdb | . wrk | . xdb |
| . xld | . xmlff | . abcddb | . abs | . abx | . accdw | . and | . db2 |
| . fm5 | . hjt | . icg | . icr | . kdb | . lut | . maw | . mdn |
| . mdt | | | | | | | |

Shared folders targeted for encryption (Example: *[IP address]**Downloads*):

| | | | | |
|---|---|---|---|---|
| Users | Backup | Veeam | homes | home |
| media | common | Storage Server | Public | Web |
| Images | Downloads | BackupData | ActiveBackupForBusiness | Backups |
| NAS-DC | DCBACKUP | DirectorFiles | share | |

File extensions ignored:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| .ini | .url | .msilog | .log | .ldf | .lock | .theme | .msi |
| .sys | .wpx | .cpl | .adv | .msc | .scr | .key | .ico |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| .dll | .hta | .deskthemepack | .nomedia | .msu | .rtp | .msp | .idx |
| .ani | .386 | .diagcfg | .bin | .mod | .ics | .com | .hlp |
| .spl | .nls | .cab | .exe | .diagpkg | .icl | .ocx | .rom |
| .prf | .thempack | .msstyles | .icns | .mpa | .drv | .cur | .diagcab |
| .cmd | .shs | | | | | | |

Folders ignored:

| | | | | |
|---|---|---|---|---|
| windows | boot | program files (x86) | windows.old | programdata |
| intel | bitdefender | trend micro | windowsapps | appdata |
| application data | system volume information | perflogs | msocache | |

Files ignored:

| | | | |
|---|---|---|---|
| bootnxt | ntldr | bootmgr | thumbs.db |
| ntuser.dat | bootsect.bak | autoexec.bat | iconcache.db |
| bootfont.bin | | | |

Processes terminated:

| | | | | |
|---|---|---|---|---|
| teracopy | teamviewer | nsservice | nsctrl | uranium |
| processhacker | procmon | pestudio | procmon64 | x32dbg |
| x64dbg | cff explorer | procexp | pslist | tcpview |
| tcpvcon | dbgview | rammap | rammap64 | vmmap |
| ollydbg | autoruns | autorunssc | filemon | regmon |
| idaq | idaq64 | immunitydebugger | wireshark | dumpcap |

| | | | | |
|---|---|---|---|---|
| hookexplorer | importrec | petools | lordpe | sysinspector |
| proc_analyzer | sysanalyzer | sniff_hit | windbg | joeboxcontrol |
| joeboxserver | resourcehacker | fiddler | httpdebugger | dumpit |
| rammap | rammap64 | vmmap | agntsvc | cntaosmgr |
| dbeng50 | dbsnmp | encsvc | infopath | isqlplussvc |
| mbamtray | msaccess | msftesql | mspub | mydesktopqos |
| mydesktopservice | mysqld | mysqld-nt | mysqld-opt | Ntrtscan |
| ocautoupds | ocomm | ocssd | onenote | oracle |
| outlook | PccNTMon | powerpnt | sqbcoreservice | sql |
| sqlagent | sqlbrowser | sqlservr | sqlwriter | steam |
| synctime | tbirdconfig | thebat | thebat64 | thunderbird |
| tmlisten | visio | winword | wordpad | xfssvccon |
| zoolz | | | | |

Services terminated:

| | | | |
|---|---|---|---|
| CybereasonRansomFree | vnetd | bpcd | SamSs |
| msftesql | nsService | klvssbridge64 | vapiendpoint |
| Smcinst | SmcService | SntpService | svcGenericHost |
| TmCCSF | tmlisten | TrueKey | TrueKeyScheduler |
| WRSVC | McTaskManager | OracleClientCache80 | mfefire |
| mfemms | RESvc | mfevtp | sacsvr |
| SepMasterService | PDVFSService | ESHASRV | SDRSVC |

| | | | |
|---|---|---|---|
| KAVFS | KAVFS_KAVFSGT | kavfsslp | klnagent |
| masvc | MBAMService | MBEndpointAgent | McShield |
| Antivirus | AVP | DCAgent | bedbg |
| MMS | ekrn | EPSecurityService | EPUpdateService |
| EsgShKernel | msexchangeadtopology | AcrSch2Svc | MSOLAP$TPSAMA |
| msexchangeimap4 | ARSM | unistoresvc_1af40a | ReportServer$TPS |
| W3Svc | MSExchangeSRS | ReportServer$TPSAMA | Zoolz 2 Service |
| aphidmonitorservice | SstpSvc | MSExchangeMTA | ReportServer$SYS |
| UI0Detect | MSExchangeSA | MSExchangeIS | ReportServer |
| POP3Svc | MSExchangeMGMT | SMTPSvc | MsDtsServer |
| MSExchangeES | EraserSvc11710 | Enterprise Client Service | MsDtsServer100 |
| stc_raw_agent | VSNAPVSS | PDVFSService | AcrSch2Svc |
| CASAD2DWebSvc | CAARCUpdateSvc | McAfee | avpsus |
| mfewc | BMR Boot Service | DefWatch | ccEvtMgr |
| SavRoam | RTVsc screenconnect | ransom | sqltelemetry |
| vnc | teamviewer | msolap | veeam |
| sql | memtas | vss | sophos |
| mepocs | wuauserv | | |

Drivers that Blackbyte can bypass:

| | | | |
|---|---|---|---|
| 360avflt.sys | 360box.sys | 360fsflt.sys | 3 |

| | | | |
|---|---|---|---|
| a2acc.sys | a2acc64.sys | a2ertpx64.sys | a |
| a2gffx64.sys | a2gffx86.sys | aaf.sys | a |
| accessvalidator.sys | acdriver.sys | acdrv.sys | a |
| adcvcsnt.sys | adspiderdoc.sys | aefilter.sys | a |
| agseclock.sys | agsyslock.sys | ahkamflt.sys | a |
| ahnrghlh.sys | aictracedrv_am.sys | airship-filter.sys | a |
| alfaff.sys | altcbt.sys | amfd.sys | a |
| amm8660.sys | amsfilter.sys | amznmon.sys | a |
| anvfsm.sys | apexsqlfilterdriver.sys | appcheckd.sys | a |
| arfmonnt.sys | arta.sys | arwflt.sys | a |
| asiofms.sys | aswfsblk.sys | aswmonflt.sys | a |
| aszfltnt.sys | atamptnt.sys | atc.sys | a |
| aternityregistryhook.sys | atflt.sys | atrsdfw.sys | a |
| avapsfd.sys | avc3.sys | avckf.sys | a |
| avgmfrs.sys | avgmfx64.sys | avgmfx86.sys | a |
| avgtpx86.sys | avipbb.sys | avkmgr.sys | a |
| axfltdrv.sys | axfsysmon.sys | ayfilter.sys | b |
| bamfltr.sys | bapfecpt.sys | bbfilter.sys | b |
| bdfiledefend.sys | bdfilespy.sys | bdfm.sys | b |
| bdrdfolder.sys | bdsdkit.sys | bdsfilter.sys | b |
| bdsysmon.sys | bedaisy.sys | bemk.sys | b |

| | | | |
|---|---|---|---|
| bfmon.sys | bhdrvx64.sys | bhdrvx86.sys | b |
| bkavautoflt.sys | bkavsdflt.sys | blackbirdfsa.sys | b |
| bmregdrv.sys | boscmflt.sys | bosfsfltr.sys | b |
| brcow_x_x_x_x.sys | brfilter.sys | brnfilelock.sys | b |
| bsrfsflt.sys | bssaudit.sys | bsyaed.sys | b |
| bsyirmf.sys | bsyrtm.sys | bsysp.sys | b |
| bzsenspdrv.sys | bzsenth.sys | bzsenyaradrv.sys | c |
| cancelsafe.sys | carbonblackk.sys | catflt.sys | c |
| cbfilter20.sys | cbfltfs4.sys | cbfsfilter2017.sys | c |
| cdo.sys | cdrrsflt.sys | cdsgfsfilter.sys | c |
| cfsfdrv | cgwmf.sys | change.sys | c |
| ciscoampcefwdriver.sys | ciscoampheurdriver.sys | ciscosam.sys | c |
| cmdcwagt.sys | cmdguard.sys | cmdmnefs.sys | c |
| codex.sys | conduantfsfltr.sys | containermonitor.sys | c |
| cpepmon.sys | crexecprev.sys | crncache32.sys | c |
| cruncopy.sys | csaam.sys | csaav.sys | c |
| csagent.sys | csareg.sys | csascr.sys | c |
| csfirmwareanalysis.sys | csflt.sys | csmon.sys | c |
| ctifile.sys | ctinet.sys | ctrpamon.sys | c |
| cvofflineflt32.sys | cvofflineflt64.sys | cvsflt.sys | c |
| cybkerneltracker.sys | cylancedrv64.sys | cyoptics.sys | c |

| | | | |
|---|---|---|---|
| cytmon.sys | cyverak.sys | cyvrfsfd.sys | c |
| datanow_driver.sys | dattofsf.sys | da_ctl.sys | c |
| dcsnaprestore.sys | deepinsfs.sys | delete_flt.sys | c |
| dgedriver.sys | dgfilter.sys | dgsafe.sys | c |
| diskactmon.sys | dkdrv.sys | dkrtwrt.sys | c |
| docvmonk.sys | docvmonk64.sys | dpmfilter.sys | c |
| drsfile.sys | drvhookcsmf.sys | drvhookcsmf_amd64.sys | c |
| dsark.sys | dsdriver.sys | dsfemon.sys | c |
| dskmn.sys | dtdsel.sys | dtpl.sys | c |
| dwshield64.sys | eamonm.sys | easeflt.sys | e |
| ecatdriver.sys | edevmon.sys | ednemfsfilter.sys | e |
| edsigk.sys | eectrl.sys | eetd32.sys | e |
| eeyehv64.sys | egambit.sys | egfilterk.sys | e |
| ehdrv.sys | elock2fsctldriver.sys | emxdrv2.sys | e |
| epdrv.sys | epfw.sys | epfwwfp.sys | e |
| epp64.sys | epregflt.sys | eps.sys | e |
| eraser.sys | esensor.sys | esprobe.sys | e |
| estregmon.sys | estregp.sys | estrkmon.sys | e |
| evmf.sys | evscase.sys | excfs.sys | e |
| failmount.sys | fam.sys | fangcloud_autolock_driver.sys | f |
| farwflt.sys | fasdriver | fcnotify.sys | f |

| | | | |
|---|---|---|---|
| fekern.sys | fencry.sys | ffcfilt.sys | f |
| filefilter.sys | fileflt.sys | fileguard.sys | f |
| filemonitor.sys | filenamevalidator.sys | filescan.sys | f |
| filesystemcbt.sys | filetrace.sys | file_monitor.sys | f |
| filrdriver.sys | fim.sys | fiometer.sys | f |
| fjseparettifilterredirect.sys | flashaccelfs.sys | flightrecorder.sys | f |
| fmdrive.sys | fmkkc.sys | fmm.sys | f |
| fortirmon.sys | fortishield.sys | fpav_rtp.sys | f |
| fsatp.sys | fsfilter.sys | fsgk.sys | f |
| fsmonitor.sys | fsnk.sys | fsrfilter.sys | f |
| fsw31rj1.sys | gagsecurity.sys | gbpkm.sys | g |
| gefcmp.sys | gemma.sys | geprotection.sys | g |
| gkff.sys | gkff64.sys | gkpfcb.sys | g |
| gpminifilter.sys | groundling32.sys | groundling64.sys | g |
| gzflt.sys | hafsnk.sys | hbflt.sys | h |
| hdcorrelatefdrv.sys | hdfilemon.sys | hdransomoffdrv.sys | h |
| hexisfsmonitor.sys | hfileflt.sys | hiofs.sys | h |
| hooksys.sys | hpreg.sys | hsmltmon.sys | h |
| hvlminifilter.sys | ibr2fsk.sys | iccfileioad.sys | i |
| icfclientflt.sys | icrlmonitor.sys | iderafilterdriver.sys | i |
| ifs64.sys | ignis.sys | iguard.sys | i |

| | | | |
|---|---|---|---|
| im.sys | imffilter.sys | imfilter.sys | i |
| immunetprotect.sys | immunetselfprotect.sys | inisbdrv64.sys | i |
| intmfs.sys | inuse.sys | invprotectdrv.sys | i |
| iothorfs.sys | ipcomfltr.sys | ipfilter.sys | i |
| irongatefd.sys | isafekrnl.sys | isafekrnlmon.sys | i |
| isedrv.sys | isfpdrv.sys | isirmfmon.sys | i |
| issfltr.sys | issregistry.sys | it2drv.sys | i |
| iwdmfs.sys | iwhlp.sys | iwhlp2.sys | i |
| jdppwf.sys | jkppob.sys | jkppok.sys | j |
| k7sentry.sys | kavnsi.sys | kawachfsminifilter.sys | k |
| kernelagent32.sys | kewf.sys | kfac.sys | k |
| klam.sys | klbg.sys | klboot.sys | k |
| kldtool.sys | klfdefsf.sys | klflt.sys | k |
| klif.sys | klifaa.sys | klifks.sys | k |
| klsnsr.sys | klupd_klif_arkmon.sys | kmkuflt.sys | k |
| kmxfile.sys | kmxsbx.sys | ksfsflt.sys | k |
| kubwksp.sys | lafs.sys | lbd.sys | l |
| lcgfile.sys | lcgfilemon.sys | lcmadmon.sys | l |
| lcmprintmon.sys | ldsecdrv.sys | libwamf.sys | l |
| lmdriver.sys | lnvscenter.sys | locksmith.sys | l |
| magicbackupmonitor.sys | magicprotect.sys | majoradvapi.sys | r |

| | | | |
|---|---|---|---|
| maxproc64.sys | maxprotector.sys | mbae64.sys | r |
| mbamshuriken.sys | mbamswissarmy.sys | mbamwatchdog.sys | r |
| mcfilemon64.sys | mcstrg.sys | mearwfltdriver.sys | r |
| mfeaack.sys | mfeaskm.sys | mfeavfk.sys | r |
| mfefirek.sys | mfehidk.sys | mfencbdc.sys | r |
| mfencrk.sys | mfeplk.sys | mfewfpk.sys | r |
| minitrc.sys | mlsaff.sys | mmpsy32.sys | r |
| mozycorpfilter.sys | mozyenterprisefilter.sys | mozyentfilter.sys | r |
| mozyoemfilter.sys | mozyprofilter.sys | mpfilter.sys | r |
| mpxmon.sys | mracdrv.sys | mrxgoogle.sys | r |
| msixpackagingtoolmonitor.sys | msnfsflt.sys | mspy.sys | r |
| mumdi.sys | mwac.sys | mwatcher.sys | r |
| namechanger.sys | nanoavmf.sys | naswsp.sys | r |
| netaccctrl.sys | netaccctrl64.sys | netguard.sys | r |
| nlcbhelpi64.sys | nlcbhelpx64.sys | nlcbhelpx86.sys | r |
| nmpfilter.sys | nntinfo.sys | novashield.sys | r |
| nprosec.sys | npxgd.sys | npxgd64.sys | r |
| nrcomgrdki.sys | nregsec.sys | nrpmonka.sys | r |
| nsminflt64.sys | ntest.sys | ntfsf.sys | r |
| nullfilter.sys | nvcmflt.sys | nvmon.sys | r |
| nxrmflt.sys | oadevice.sys | oavfm.sys | c |

| | | | |
|---|---|---|---|
| odfsfimfilter.sys | odfstokenfilter.sys | offsm.sys | o |
| ospfile_mini.sys | ospmon.sys | parity.sys | p |
| pavdrv.sys | pcpifd.sys | pctcore.sys | p |
| pecfilter.sys | perfectworldanticheatsys.sys | pervac.sys | p |
| pgpfs.sys | pgpwdefs.sys | phantomd.sys | p |
| pkticpt.sys | plgfltr.sys | plpoffdrv.sys | p |
| pointguardvistar32.sys | pointguardvistar64.sys | procmon11.sys | p |
| pscff.sys | psgdflt.sys | psgfoctrl.sys | p |
| psisolator.sys | pwipf6.sys | pwprotect.sys | p |
| qfapflt.sys | qfilter.sys | qfimdvr.sys | q |
| qmon.sys | qqprotect.sys | qqprotectx64.sys | q |
| qutmdrv.sys | ranpodfs.sys | ransomdefensexxx.sys | r |
| redlight.sys | regguard.sys | reghook.sys | r |
| repmon.sys | revefltmgr.sys | reveprocprotection.sys | r |
| rgnt.sys | rmdiskmon.sys | rmphvmonitor.sys | r |
| rrmon64.sys | rsfdrv.sys | rsflt.sys | r |
| rswctrl.sys | rswmon.sys | rtologon.sys | r |
| rubrikfileaudit.sys | ruidiskfs.sys | ruieye.sys | r |
| ruiminispy.sys | rvsavd.sys | rvsmon.sys | r |
| ryfilter.sys | ryguard.sys | safe-agent.sys | s |
| sahara.sys | sakfile.sys | sakmfile.sys | s |

| | | | |
|---|---|---|---|
| sanddriver.sys | santa.sys | sascan.sys | s |
| scaegis.sys | scauthfsflt.sys | scauthiodrv.sys | s |
| scifsflt.sys | sciptflt.sys | sconnect.sys | s |
| sddrvldr.sys | sdvfilter.sys | se46filter.sys | s |
| secone_proc10.sys | secone_reg10.sys | secone_usb.sys | s |
| secure_os.sys | secure_os_mf.sys | securofsd_x64.sys | s |
| segiraflt.sys | segmd.sys | segmp.sys | s |
| serfs.sys | sfac.sys | sfavflt.sys | s |
| sgresflt.sys | shdlpmedia.sys | shdlpsf.sys | s |
| shldflt.sys | si32_file.sys | si64_file.sys | s |
| sisipsfilefilter | sk.sys | skyamdrv.sys | s |
| slb_guard.sys | sld.sys | smbresilfilter.sys | s |
| snexequota.sys | snilog.sys | snimg.sys | s |
| sodatpfl.sys | softfilterxxx.sys | soidriver.sys | s |
| sophosdt2.sys | sophosed.sys | sophosntplwf.sys | s |
| spellmon.sys | spider3g.sys | spiderg3.sys | s |
| sprtdrv.sys | sqlsafefilterdriver.sys | srminifilterdrv.sys | s |
| srtspit.sys | ssfmonm.sys | ssrfsf.sys | s |
| stegoprotect.sys | stest.sys | stflt.sys | s |
| strapvista.sys | strapvista64.sys | svcbt.sys | s |
| swfsfltrv2.sys | swin.sys | symafr.sys | s |

| | | | |
|---|---|---|---|
| symefasi.sys | symevent.sys | symevent64x86.sys | s |
| symhsm.sys | symrg.sys | sysdiag.sys | s |
| sysplant.sys | szardrv.sys | szdfmdrv.sys | s |
| szpcmdrv.sys | taniumrecorderdrv.sys | taobserveflt.sys | t |
| tbrdrv.sys | tdevflt.sys | tedrdrv.sys | t |
| tesxnginx.sys | tesxporter.sys | tffregnt.sys | t |
| thetta.sys | thfilter.sys | threatstackfim.sys | t |
| tkdacxp64.sys | tkfsavxp.sys | tkfsavxp64.sys | t |
| tkpcftcb.sys | tkpcftcb64.sys | tkpl2k.sys | t |
| tkspxp.sys | tkspxp64.sys | tmactmon.sys | t |
| tmevtmgr.sys | tmeyes.sys | tmfsdrv2.sys | t |
| tmpreflt.sys | tmumh.sys | tmums.sys | t |
| topdogfsfilt.sys | trace.sys | trfsfilter.sys | t |
| trufos.sys | trustededgeffd.sys | tsifilemon.sys | t |
| tstfsredir.sys | tstregredir.sys | tsyscare.sys | t |
| tvmfltr.sys | tvptfile.sys | tvspfltr.sys | t |
| txregmon.sys | uamflt.sys | ucafltdriver.sys | u |
| upguardrealtime.sys | usbl_ifsfltr.sys | usbpdh.sys | u |
| uwfreg.sys | uwfs.sys | v3flt2k.sys | v |
| v3iftmnt.sys | v3mifint.sys | varpffmon.sys | v |
| vchle.sys | vcmfilter.sys | vcreg.sys | v |

| | | | |
|---|---|---|---|
| vfilefilter.sys | vfpd.sys | vfsenc.sys | v |
| vidderfs.sys | vintmfs.sys | virtfile.sys | v |
| vlflt.sys | vmwvvpfsd.sys | vollock.sys | v |
| vraptdef.sys | vraptflt.sys | vrarnflt.sys | v |
| vrfsftm.sys | vrfsftmx.sys | vrnsfilter.sys | v |
| vrsdetri.sys | vrsdetrix.sys | vrsdfmx.sys | v |
| vsscanner.sys | vtsysflt.sys | vxfsrep.sys | v |
| wcsdriver.sys | wdcfilter.sys | wdfilter.sys | v |
| wgfile.sys | whiteshield.sys | windbdrv.sys | v |
| winflahdrv.sys | winfldrv.sys | winfpdrv.sys | v |
| wiper.sys | wlminisecmod.sys | wntgpdrv.sys | v |
| wrcore.x64.sys | wrdwizfileprot.sys | wrdwizregprot.sys | v |
| wrkrn.sys | wrpfv.sys | wsafefilter.sys | v |
| xendowflt.sys | xfsgk.sys | xhunter1.sys | x |
| xiaobaifsr.sys | xkfsfd.sys | xoiv8x64.sys | x |
| yfsd.sys | yfsd2.sys | yfsdr.sys | y |
| zesfsmf.sys | zqfilter.sys | zsfprt.sys | z |
| zxfsfilt.sys | zyfm.sys | zzpensys.sys | |

## Further reading

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on Twitter at https://twitter.com/MsftSecIntel.

## Related Posts

Best practices Incident response Microsoft Security Experts
Jun 6 6 min read

### Why a proactive detection and incident response plan is crucial for your organization >

Matt Suiche of Magnet Forensics talks about top security threats for organizations and strategies for effective incident response.

Research Threat intelligence Microsoft Defender Threat actors
May 24 10 min read

### Volt Typhoon targets US critical infrastructure with living-off-the-land techniques >

Chinese state-sponsored actor Volt Typhoon is using stealthy techniques to target US critical infrastructure, conduct espionage, and dwell in compromised environments.

Research Incident response Threat actors Apr 11 8 min read

### Guidance for investigating attacks using CVE-2022-21894: The BlackLotus campaign >

This guide provides steps that organizations can take to assess whether users have been targeted or compromised by threat actors exploiting CVE-2022-21894 via a Unified Extensible Firmware Interface (UEFI) bootkit called BlackLotus.

Best practices Security operations Microsoft Defender
Apr 27 6 min read

### Why you should practice rollbacks to prevent data loss in a ransomware attack >

Tanya Janca, Founder and Chief Executive Officer of We Hack Purple, shares insights on application security and offers strategies to protect against data loss from ransomware attacks.


Connect with us on social