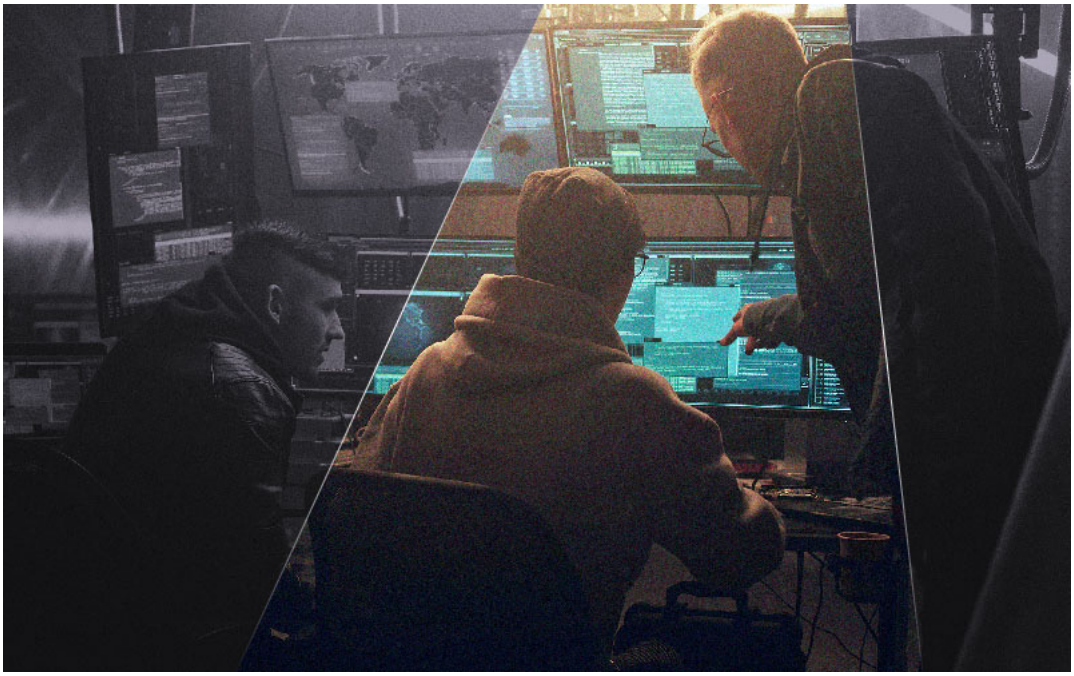
Ransomware Spotlight: BlackByte

trendmicro.com/vinfo/my/security/news/ransomware-spotlight/ransomware-spotlight-blackbyte



X

RANSOMWARE SPOTLIGHT

BlackByte

By Trend Micro Research

BlackByte is a ransomware group that has been building a name for itself since 2021. Like its contemporaries, it has gone after critical infrastructure for a higher chance of a getting a payout. What techniques set it apart?

View infographic of "Ransomware Spotlight: BlackByte"

BlackByte debuted in July 2021. Its first year of activity garnered the attention of the Federal Bureau of Investigation (FBI) and the US Secret Service (USS). According to a joint advisory by these two government agencies, BlackByte had already gone after at least three US critical infrastructure sectors (government facilities, financial, and food and agriculture) by November 2021.

This advisory shows just how BlackByte was actively establishing itself as a new noteworthy ransomware variant. On October 2021, Trustwave released a publicly available decrypter for BlackByte. This however did not stop BlackByte as developers released newer versions that used multiple keys and ramped up operations, going as far as to warn their victims against using the available decrypter on their website.

BlackByte's emergence could be part of a larger scheme. With the purported shut down of Conti, researchers from AdvIntel surmise that BlackByte is one of the chief new ransomware variants part of its rebranding.

At present, BlackByte continues to target organizations from all over the world. However, like LockBit, RansomEXX, and many other ransomware families, BlackByte avoids attacking Russia-based entities.

What do organizations need to know about BlackByte?

While BlackByte operators use their piece of ransomware in attacks for their own gain, they also run on a ransomware-as-a-service (RaaS) model for their affiliates. We have listed down the key highlights of BlackByte here:

- **Initial versions used symmetric keys.** The earlier variant of BlackByte used the same key in each campaign to encrypt files. It also used AES, a symmetric key algorithm. This allowed researchers to create a decrypter to help BlackByte victims, thus forcing the group to change their encryption method in newer variants.
- **It has multiple variants.** The first known version of BlackByte was written in C#. Operators then released two Go-based variants. The more recent Go-variant was introduced around February 2022 and sported modifications particularly in its encryption algorithm.
- **Archives files using WinRAR.** In BlackByte campaigns data exfiltration is done before the ransomware is deployed. This is because the BlackByte ransomware is incapable of exfiltrating data, instead it archives files using WinRAR then uploads the file to sharing sites.
- **Uses trojanized legitimate tools.** Like most modern ransomware variants, BlackByte uses living-off-the-land binaries. For example, it uses the remote tool AnyDesk to gain further control over a system and for lateral movement.
- **Involves phishing emails or a known ProxyShell vulnerability for initial access.** BlackByte has been known to use phishing emails or exploit unpatched ProxyShell vulnerability in Microsoft Exchange Servers to gain initial access into a system.

BlackByte trajectory seems to point to continuing activity. In fact, reports indicate that BlackByte is among the ransomware operations that have set their sights on Latin American governments in May 2022. This report is reflected in our own telemetry data as seen in the next section.

Top affected industries and countries

The data used in this section represent the count of unique machines where BlackByte-related activity had been detected. Based on our telemetry data, BlackByte showed a fairly consistent level of activity from October 2021 to March 2022. However, May 2022 detections showed a drastic uptick in number.

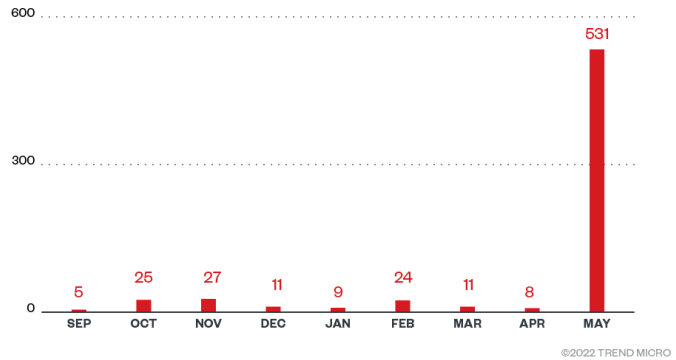


Figure 1. BlackByte monthly unique detections (October 1, 2021 to May 31, 2022)
Source: Trend Micro™ Smart Protection Network™

Based on our telemetry data from April 30, 2021 to May 31, 2022, we detected BlackByte activity all over the globe. However, after the spike in activity in May, Peru outstripped other countries in detection. This is consistent with the reported escalation of ransomware attacks in Latin America, where BlackByte was also reportedly among those that targeted the region.

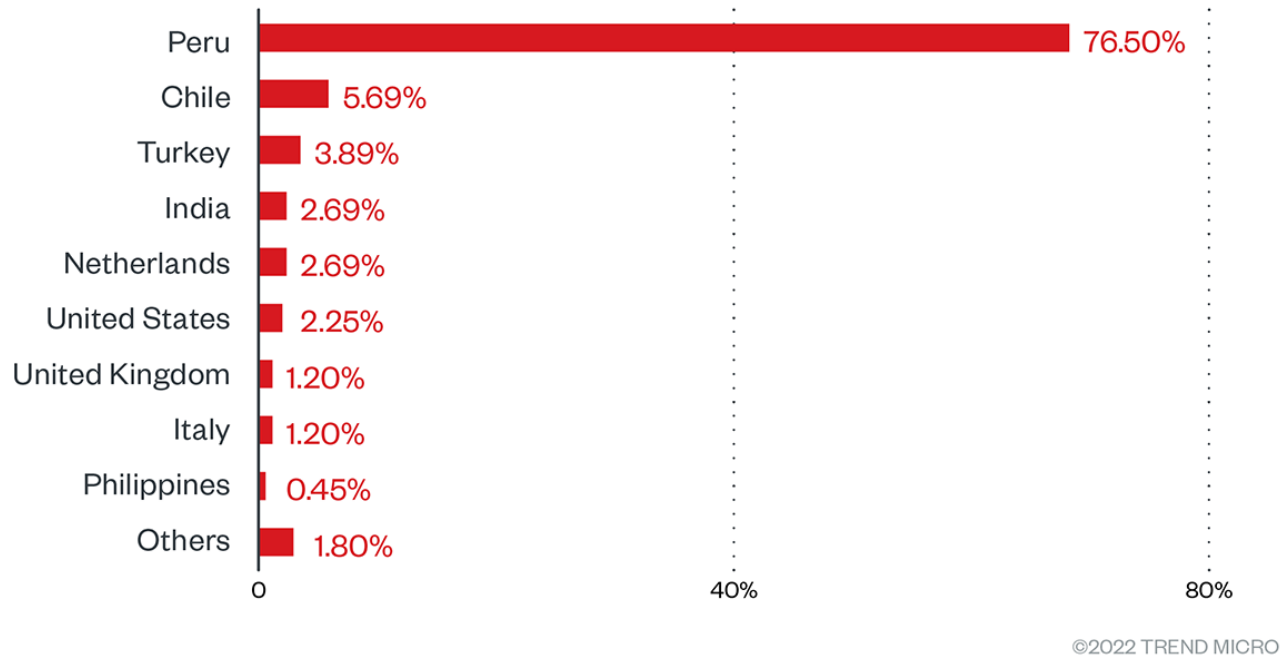


Figure 2. Countries with the highest number of attack attempts for the BlackByte ransomware (April 30, 2021 to May 30, 2022)
Source: Trend Micro Smart Protection Network

Up to the end of April 2022, the technology sector saw the most BlackByte detections, however, in May, detections in the government sector also shot up.

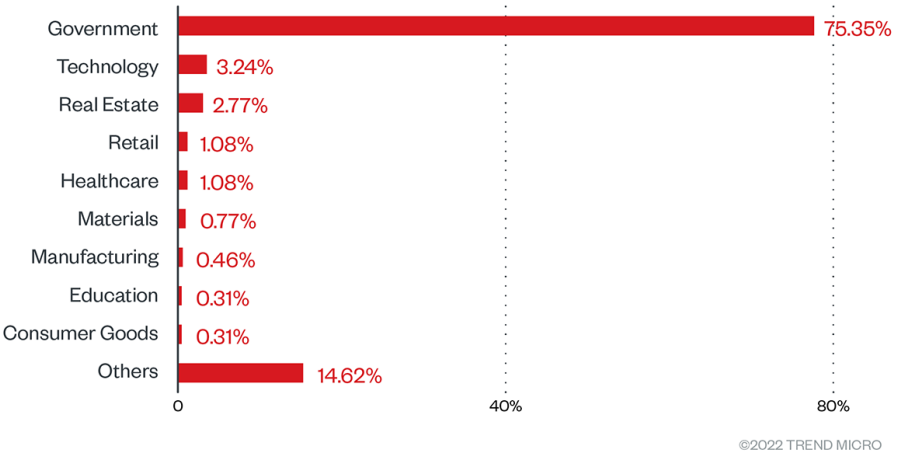


Figure 3. Countries with the highest number of attack attempts for the BlackByte ransomware (April 30, 2021 to May 30, 2022)
Source: Trend Micro Smart Protection Network

One way to interpret these observations is that the drastic increase stemmed from a single attack that affected several machines. Aside from the reports on ransomware groups targeting Latin America, this explanation is also based on the report that, by their own claim, BlackByte operators had compromised a Peruvian government entity around the time of the increased activity.

Targeted regions and sectors according to BlackByte leaksite

In addition to these detections, we delved into BlackByte's leak site to see the number of attacks recorded there. We looked at data from August 1, 2021 to May 31, 2022. Based on what we found in the site, BlackByte's victims were composed mostly of small size businesses. The activity peaked in November 2021.

Overall, the leak site has yet to reflect the focused attack on Latin American governments. The distribution of their attacks per region showed, instead, a proclivity for targeting entities based in North America and Europe.

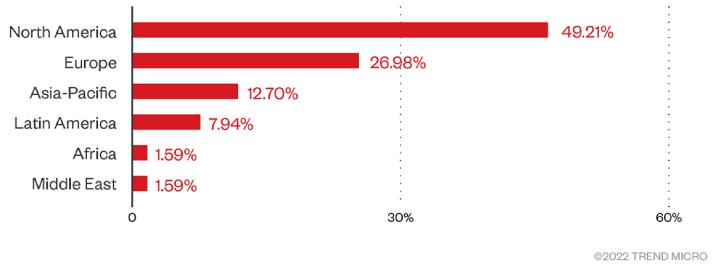


Figure 4. Regional distribution of BlackByte victims according to the group's leak site (August 1, 2021 to May 31, 2022)

Based on the leak site data alone, BlackByte operators and their affiliates have yet to show a marked interest in any one sector. We found a relatively even distribution of attacks across industries, which included the following:

- Construction
- Materials
- Healthcare
- Retail
- Transportation
- Energy & Utilities
- Manufacturing
- Professional services
- Automobile
- Community
- Foods & Staples
- Real Estate
- Government
- IT
- Legal services
- Media and entertainment

Comparing the leak site data of BlackByte to other ransomware families, shows that from January 1, 2022 to May 31, 2022, BlackByte was among the 10 ransomware groups with the greatest number of self-reported victims.

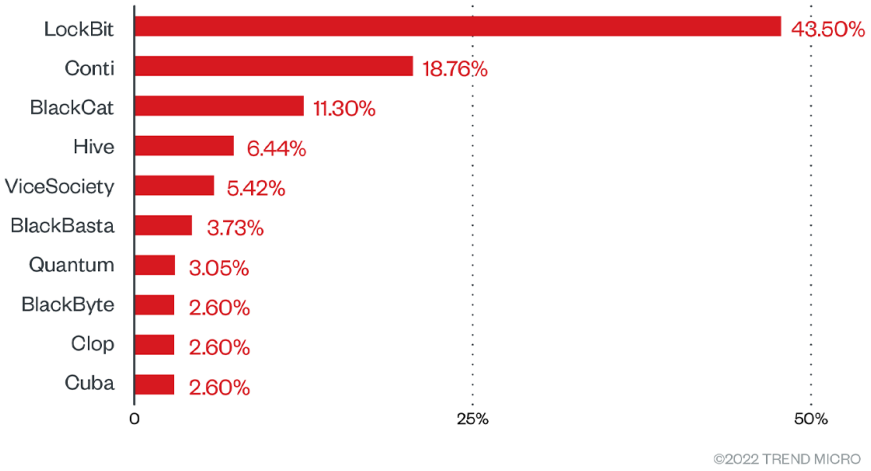


Figure 5. Top ransomware groups with the greatest number of listed victims in their respective leak sites (January 1, 2022 to May 31, 2022)

The data seems to show that BlackByte's operation is beginning to build a name for itself in the threat landscape while still building momentum. The following section shows how it works and how it conducts its attacks.

Infection chain and techniques

Given that BlackByte operates on the RaaS model, its infection chain can vary depending on the target.

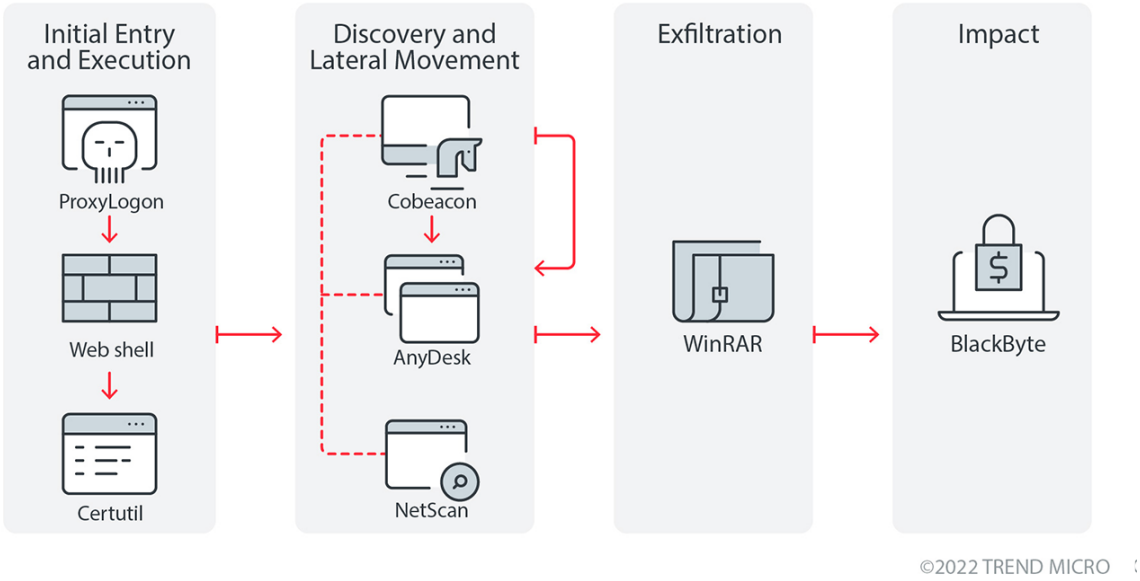


Figure 6. BlackByte infection chain

Initial Access

- BlackByte can arrive in a system by exploiting the ProxyShell vulnerabilities. Exploiting the vulnerable server allows the attacker to create a web shell to the system which is then used to download and drop Cobeacon using Certutil.
- After the initial access into the system, the attackers use Certutil to download and execute the components that it needs to propagate in the network.
- After the deployment of Cobeacon, it is then used to execute BlackByte ransomware.

Discovery and Lateral Movement

- Based on our data, the actors used NetScan as a network discovery tool that allows the attackers to get a good view of the victim's network environment.
- After network reconnaissance, the attackers deploy AnyDesk in the system for an additional level of control over the system. The attackers repeat this process of discovery and deployment of Cobeacon and AnyDesk until it achieves its goals.
- During the execution of BlackByte, it terminates certain processes and services related to security application to evade detection.

Exfiltration

Once the attackers have sufficiently infiltrated into the victim's network and identified valuable files, it exfiltrates them using WinRar to archive the files and upload them into file sharing sites such as anonymfiles[.]com and file[.]io.

Impact

Once the ransomware is executed, it terminates certain services and processes related to security application to evade detections. It also connects to its C&C server where it looks for a certain PNG file that contains information critical to encryption and is used to derive the AES128 key. This key is then protected using an embedded RSA key which will then become undecryptable without the private key. The ransomware then deletes shadow copies in the system using vssadmin.

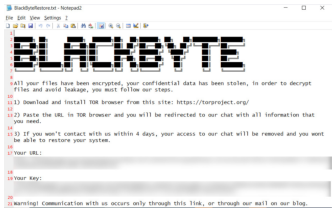


Figure 7. Sample ransom note

Other technical details

- It avoids encrypting the following files with strings in their file name:
  - obamka.js
  - thumbs.db
  - ntdetect.com
  - ntuser.dat.log
  - bootnxt
  - bootsect.bak
  - ntldr
  - autoexec.bat
  - Recycle.Bin
  - iconcache.db
  - bootmgr
  - bootfont.bin

- It avoids encrypting files with the following extensions:
  - 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
  - themepack
  - msstyles
  - icns
  - mpa
  - drv
  - cur
  - diagcab
  - cmd
  - shs
- It terminates the following services:
  - SQLTELEMETRY
  - SQLTELEMETRY$ECWDB2
  - SQLWriter
  - SstpSvc
  - MBAMService
  - wuauserv

- It terminates the following processes if found in the affected system's memory:
  - agntsvc
  - CNTAoSMgr
  - dbeng50
  - dbsnmp
  - encsvc
  - excel
  - firefox
  - firefoxconfig
  - 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
  - anydesk
  - chrome
  - opera
  - msedge
  - firefox
  - iexplore
  - explorer
  - winlogon
  - SearchIndexer
  - wininit
  - SearchApp
  - SearchUI
  - Powershel

MITRE tactics and techniques

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral M
T1190 - Exploit Public-Facing Application *It has been observed to be using the ProxyShell exploit to deliver China Chopper web shell as its initial arrival.*	**T1053.005** - Scheduled Task/Job: Scheduled Task *It creates a scheduled task to execute its java script to proceed with its routine on bootup. Task Name: Joke Trigger: Once, at 00:00 Action: wscript.exe*	**T1134** - Access Token Manipulation *This ransomware modifies the registry to elevate local privilege and enable linked connections.*	**T1140** - Deobfuscate/Decode Files or Information *It initially arrives as an obfuscated Java Script file which will be decoded upon execution.* **T1222** - File and Directory Permissions Modification *It uses mountvol.exe to mount volume names and icacls.exe to modify the access on the volume to "Everyone."* *C:\Windows\System32\icacls.exe" "C:*" /grant Everyone:F /T /C /Q* *It also controlled folder access using PowerShell:* *"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Set-MpPreference -EnableControlledFolderAccess Disabled* *It also modifies firewall settings to enable linked connections:* *"C:\Windows\System32\netsh.exe" advfirewall firewall set rule group="Network Discovery" new enable=Yes "C:\Windows\System32\netsh.exe" advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes* **T1562.001** - Impair Defenses: Disable or Modify Tools *It disables Raccine, which is an anti-ransomware utility, using these commands:* *taskill.exe /F /IM Raccine.exe* *taskill.exe /F /IM RaccineSettings.exe* *schtasks.exe /DELETE /TN \"Raccine Rules Updater\" /F* *Deletes raccine autostart:* *HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* *Name = “Raccine Tray”* *HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\Raccine*	**T1083** - File and Directory Discovery *This ransomware discovers files and directories by first enumerating the logical drives. Once enumerated, it then changes the access control of files and directories so that it can have full access over them. It will then go through the directories and traverse it for target files to encrypt.* **T1069.002** - Permission Groups Discovery: Domain Groups *It uses the RootDSE entry from the active directory to get a listing of the hostname under that domain in preparation for its propagation in the network. It enumerates 1000 hostname in the domain.* Remote System Discovery *After getting the hostname of the remote systems, it attempts to ping the systems to see if it is alive and accessible. Then it proceeds with the*	**T1570** - L Transfer *It checks present: C:\Users (infection system) It doesnt propagat* *It checks system if following accessib \C$\User \Users\Pu* *It then cr infection system, v \Users\Pu \C$\User* *It then co file in the share an through s which wa start of ro*

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral M
				transfer to the public share folder.	

Summary of malware, tools, and exploits used

Security teams can watch for the presence of the following malware tools and exploits that are typically used in BlackByte attacks:

Initial Access	Execution	Discovery	Lateral Movement	Collection	Exfiltration
ProxyShell	Certutil	NetScan	AnyDesk	WinRAR	Exfiltrates to the following C&C • anonymfiles[.]com • file[.]io
China Chopper web shell	Cobeacon		Cobeacon		

Recommendations

Organizations face both established ransomware families as well as newer variants that are just entering the fray. Like many newer ransomware families, BlackByte is readying itself to take the spot of any big-game ransomware operation in decline. However, underneath it all could be a more intricate scheme of threat groups dispersing under new monikers.

As with the case of BlackByte, knowing its notable tactics, while also staying knowledgeable of bigger trends can help organizations create an effective strategy for ransomware attacks. In the case of BlackByte, prevention is key by keeping employees wary of phishing tactics and keeping up with security patches such as those for ProxyShell vulnerabilities.

To help defend systems against similar threats, organizations can establish security frameworks that can allocate resources systematically for establishing solid defenses against ransomware.

Here are some best practices that can be included in these frameworks:

Audit and inventory

- Take an inventory of assets and data
- Identify authorized and unauthorized devices and software
- Make an audit of event and incident logs

Configure and monitor

- Manage hardware and software configurations
- Grant admin privileges and access only when necessary to an employee’s role
- Monitor network ports, protocols, and services
- Activate security configurations on network infrastructure devices such as firewalls and routers
- Establish a software allowlist that only executes legitimate applications

Patch and update

- Conduct regular vulnerability assessments
- Perform patching or virtual patching for operating systems and applications
- Update software and applications to their latest versions

Protect and recover

- Implement data protection, back up, and recovery measures
- Enable multifactor authentication (MFA)

Secure and defend

- Employ sandbox analysis to block malicious emails
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network
- Detect early signs of an attack such as the presence of suspicious tools in the system
- Use advanced detection technologies such as those powered by AI and machine learning

Train and test

- Regularly train and assess employees' security skills
- Conduct red-team exercises and penetration tests

A multilayered approach can help organizations guard possible entry points into the system (endpoint, email, web, and network). Security solutions that can detect malicious components and suspicious behavior can also help protect enterprises.

- Trend Micro Vision One™ provides multilayered protection and behavior detection, which helps block questionable behavior and tools early on before the ransomware can do irreversible damage to the system.
- Trend Micro Cloud One™ Workload Security protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- Trend Micro Apex One™ offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of Compromise (IOCs)

The IOCs for this article can be found here. Actual indicators might vary per attack.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.