Threat Assessment: BlackByte Ransomware

- 419 people reacted
- 2
- 10 min. read

By Amer Elsad

April 21, 2022 at 12:00 PM

Category: Malware, Ransomware

Tags: BlackByte, Cybercrime, RaaS, threat assessment

Executive Summary

BlackByte is ransomware as a service (RaaS) that first emerged in July 2021. Operators have exploited ProxyShell vulnerabilities to gain a foothold in the victim's environment. BlackByte has similarities to other ransomware variants such as Lockbit 2.0 that avoid systems that use Russian and a number of Eastern European languages, including many written with Cyrillic alphabets.

The operators behind this ransomware have been very active since it first emerged. Since November 2021, they have targeted multiple U.S. and global organizations, including a number in energy, agriculture, financial services and the public sector. They also displayed pervasiveness with a notable increase (300%) in the number of attacks associated with the RaaS in October-December 2021, compared with July-September 2021.

Recently, a joint advisory from the U.S. Federal Bureau of Investigation and the U.S. Secret Service noted that the ransomware group had targeted critical infrastructure.

Palo Alto Networks detects and prevents BlackByte ransomware with the following products and services: Cortex XDR and Next-Generation Firewalls (including cloud-delivered security subscriptions such as WildFire).

Related Unit 42 Topics Ransomware, Threat Assessments

Table of Contents

BlackByte Overview

BlackByte is a RaaS that leverages double extortion as part of attacks. The threat actors behind the ransomware deploy a name-and-shame approach to victim shaming, as they operate a Tor .onion auction site where they sell stolen victim data. The operators even go so far as to link the auction site in the ransom note to scare victims.

Unit 42 has observed multiple variants of BlackByte in the wild — this includes variants written in Go and .NET, as well as one variant that appeared to have been written with a mix of both Go and C programming languages. Across the observed samples, these variants use multiple obfuscation and anti-debugging features. The ransomware payloads are UPX Packed and have worm capabilities, which allow them to increase the scope of an attack with little effort.

An earlier variant of BlackByte encrypts files in AES Symmetric encryption, a simple encryption routine where the same key is used to encrypt files. This variant downloads a .png file from the IP addresses 185[.]93.6.31 and 45[.]9.148.114 prior to encryption. Security researchers from SpiderLabs developed a decryptor for BlackByte, which was later published on GitHub.

The ransomware group was made aware of the public decryptor, and this led them to create a newer version of BlackByte that uses multiple keys for each session. The encryption happens without communication with any external IPs.

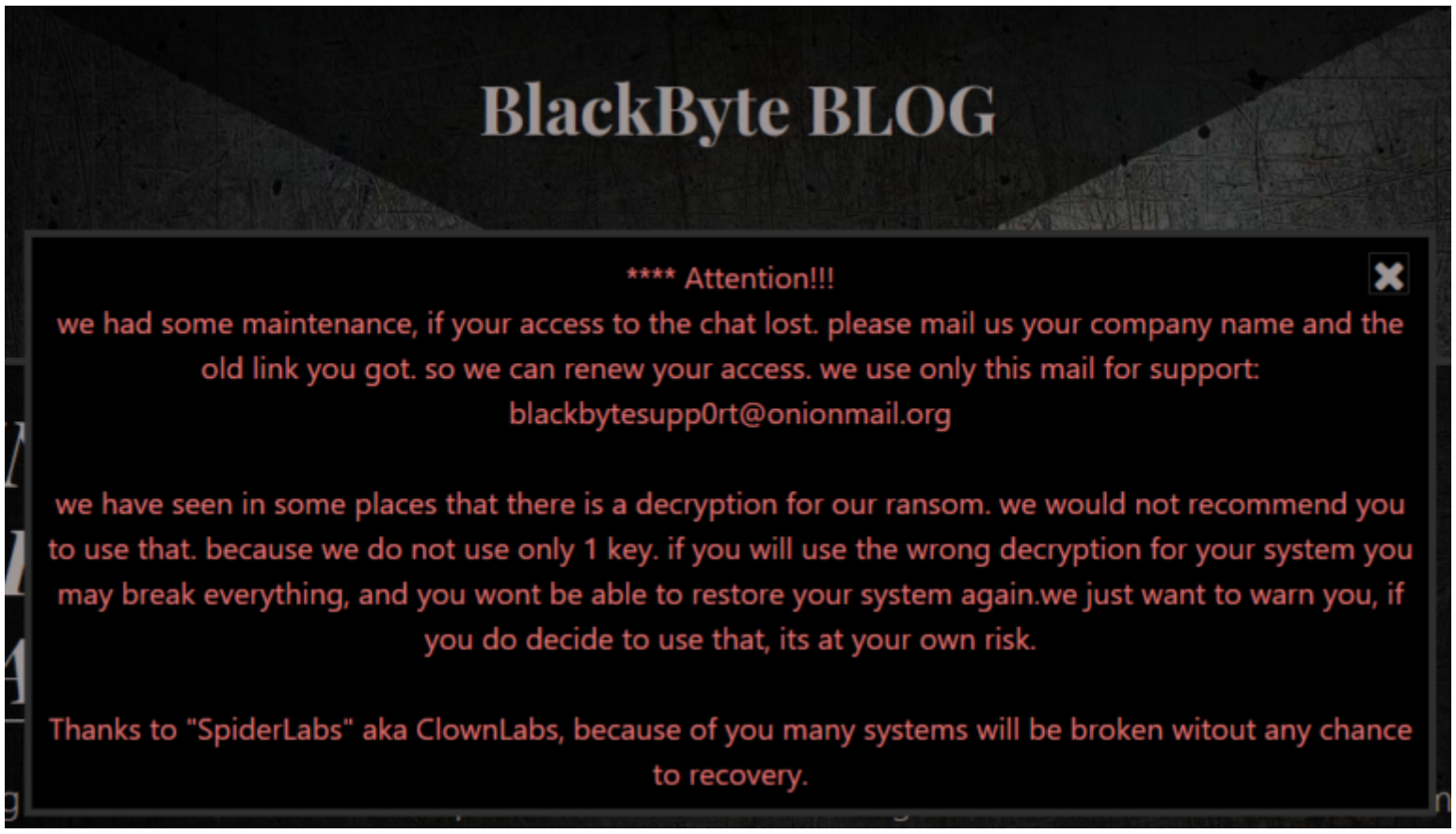

Figure 1. BlackByte warning message from the operators' website.

In addition to developing the latest ransomware variant, BlackByte operators also tried to discourage victims from using the public decryptor. They added a warning message on their site, and also included a warning against using the free decryptor in their ransom notes.

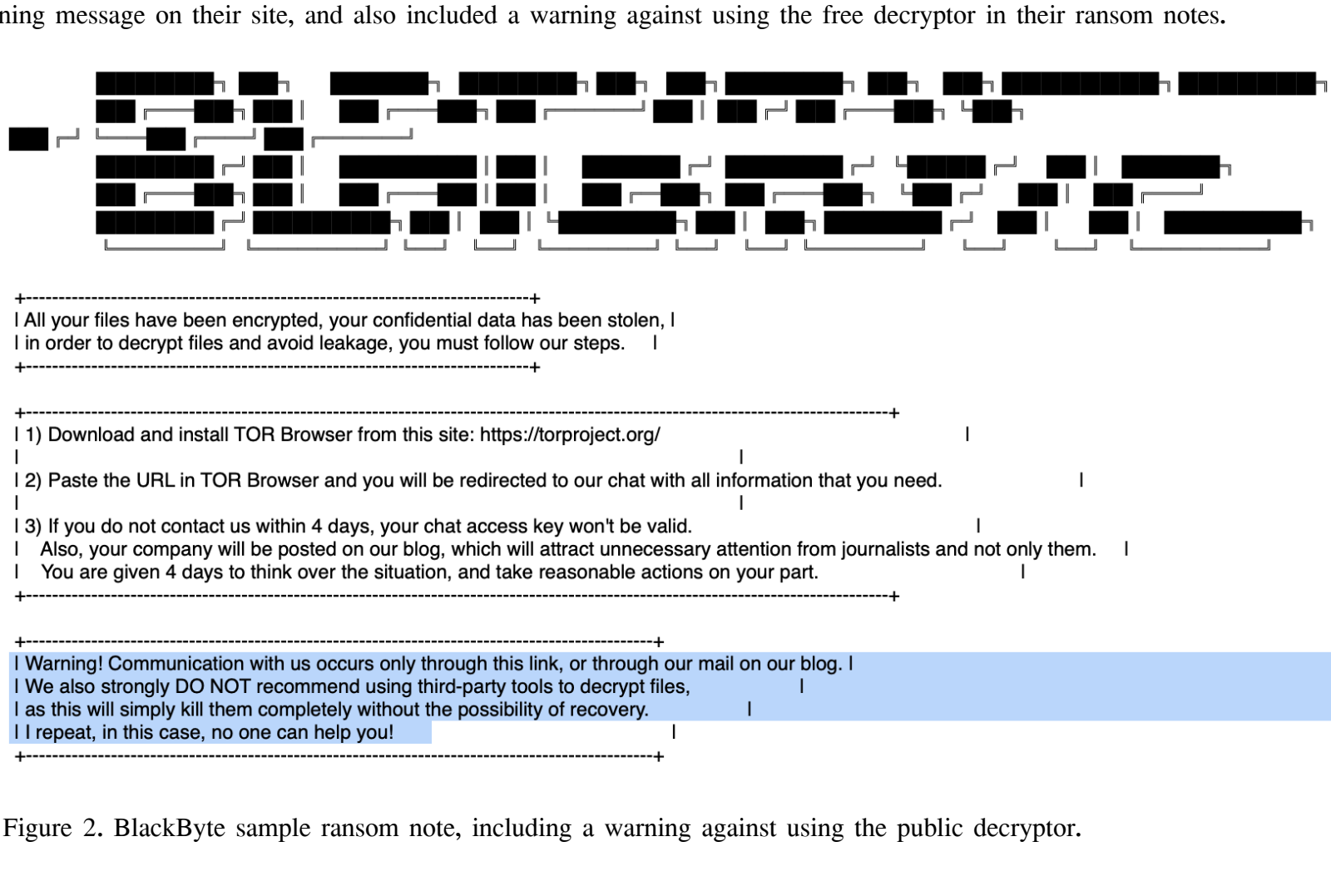

Figure 2. BlackByte sample ransom note, including a warning against using the public decryptor.

The observed BlackByte samples had an icon attached to them resembling the grim reaper (see Figure 3, left). Some of the newer versions updated their executable icons to include the same grim reaper with the addition of BB to their icon, which stands for BlackByte (see Figure 3, right).

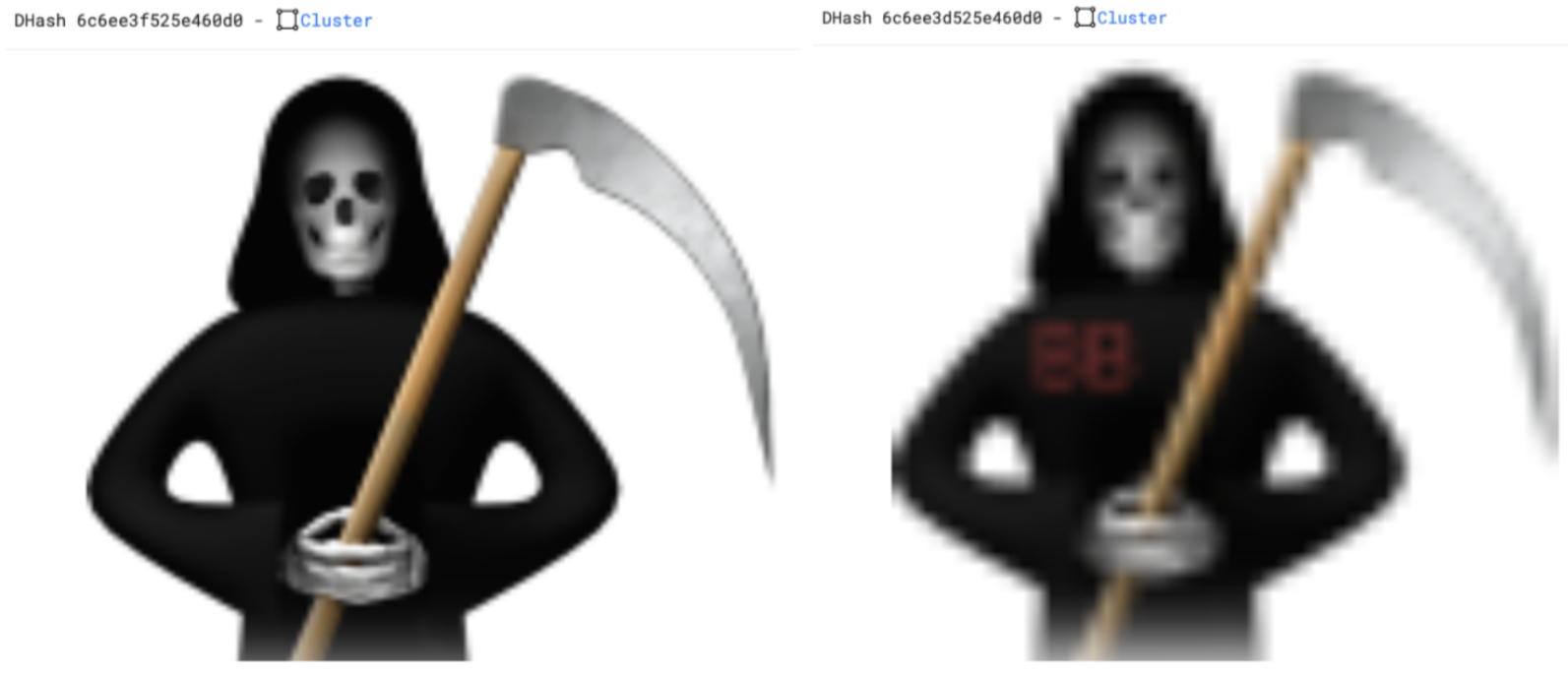

Figure 3. De-hashed images of the ransomware executable icon.

BlackByte also uses product descriptions that present its files as well-known products, likely in an attempt to mask its files as legitimate.

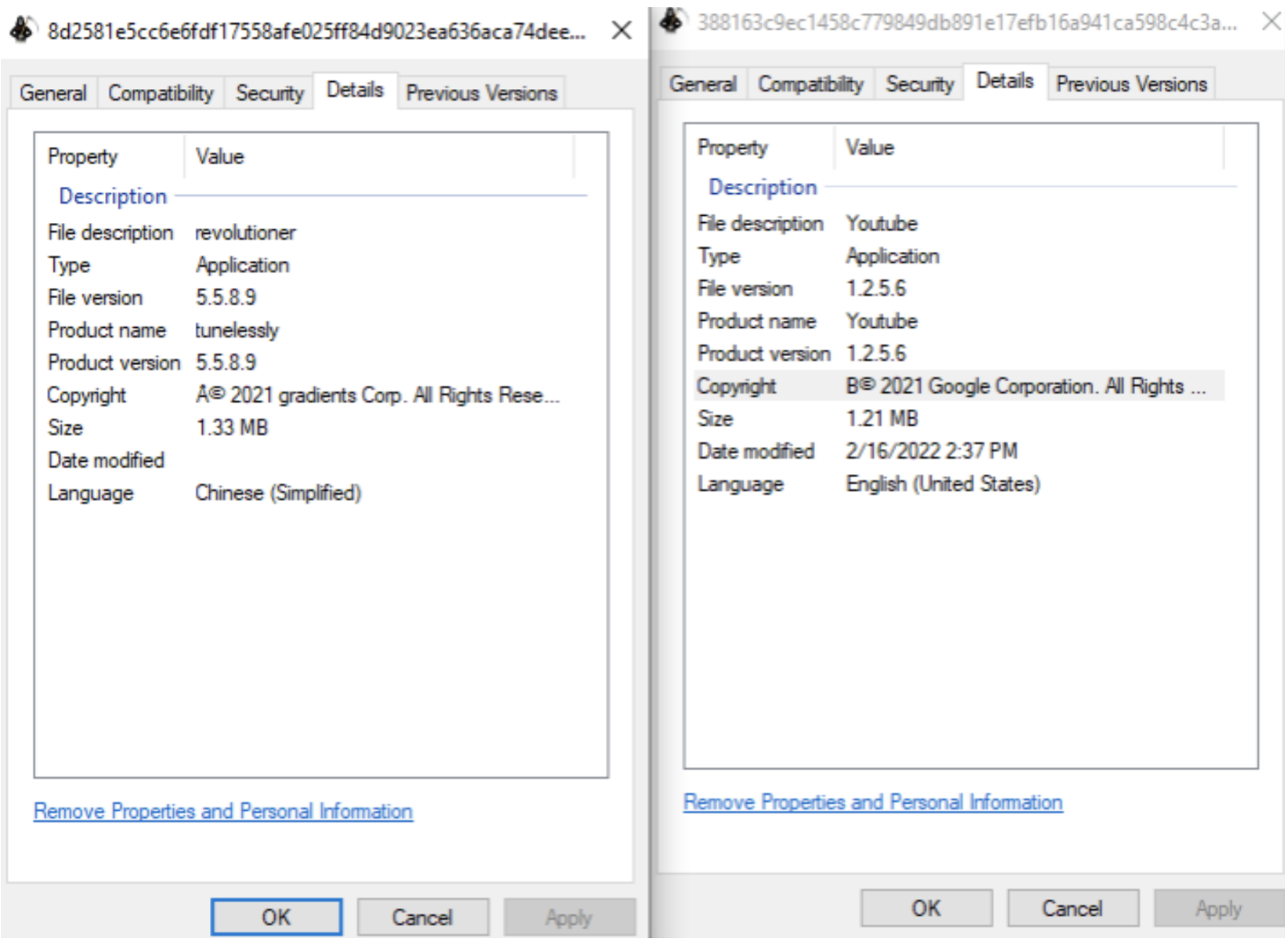

Figure 4. BlackByte using two different product descriptions.

Ransomware Highlights

Analysis of BlackByte variants identified the reuse of multiple tactics, techniques and procedures (TTPs).

Initial Access:

- Use of a known Microsoft Exchange Server vulnerability (ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) to gain access to the victim's networks. In one case, we observed threat actor attempts coming from the following IP addresses: 185[.]219.52[.]229 (RU), 198[.]144.189[.]74 (US), 45[.]137.190.193 (RU), 185[.]70.184.42 (NL) and 198[.]54.131.44 (US), with the 185[.]70.184.42 IP being the most persistent.

Persistence:

- Delivering a malicious web shell allowing remote code execution capability.
- In an effort to maintain persistence, the BlackByte ransomware excludes key system and application folders — as well as key components — from encryption so as not to render the system and ransomware inoperative. The folders excluded are as follows:

Files ignored by the ransomware:

BlackByte, ntdetect[.]com, bootnxt, NTLDR, recycle.bin, bootmgr, thumbs.db, ntuser.dat.log, bootsect.bak, autoexec.bat, iconcache.db, bootfont.bin, Bitdefender, Trend Micro, Avast Software, Intel, common files, ProgramData, WindowsApps, AppData, Mozilla, application data, Google, Windows.old, system volume information, program files (x86), boot, Tor browser, Windows, PerfLogs and MSOCache.

Any file with an extension matching the following list will also be avoided:

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, themepack, msstyles, icns, mpa, drv, cur, diagcab, cmd and shs.

Defense Evasion:

- Cobalt Strike is dropped onto the compromised Exchange Server and injected into another process such as wuauclt.exe
- BlackByte implements multiple obfuscation and anti-debugging features during execution, such as requiring a SHA256 hash passed via the command line, which is a unique identifier for the victim.
- Deleting taskmg, resmon and stopping WinDefend using PowerShell obfuscated command.

Credential Access:

- Use of Cobalt Strike for additional functions, including dumping credentials.

Privilege Escalation:

- BlackByte has been observed modifying the registry in an effort to escalate privileges
  - Elevate local privileges: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
  - Enable OS to share network connections between different privilege levels: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLinkedConnections /t REG_DWORD /d 1 /f

Discovery:

- The ransomware checks if the system includes Russian or a number of Eastern European languages, including many written with Cyrillic alphabets, before execution/encryption, and if found, it will exit.

Impact:

- It should be noted that while the ransomware itself does not have an exfiltration capability, the threat actor was observed using WinRAR to compress local data in preparation to exfiltrate.
- In older versions, BlackByte included a hardcoded RSA public key, believed to be used as part of the encryption algorithm. That could have been used as a backup key if the command and control servers (C2s) were down, or it could be that the threat actors moved away from hosting keys that could be easily retrieved. However, in newer versions, the encryption happened without communicating with any external IP addresses.

Targeting

The ransomware group and its affiliate program reportedly compromised multiple U.S. and global organizations, including some in the energy, agriculture, financial services and public sectors. They have also displayed pervasiveness with a noted increase in the number of attacks associated with the RaaS in October-December 2021, compared to July-September 2021.

The threat actor operates a cybercrime marketplace and victim name-and-shame blog dubbed BlackByte Auction. This site is hosted on a Tor network, and it is where the BlackByte ransomware group lists encrypted victim networks.

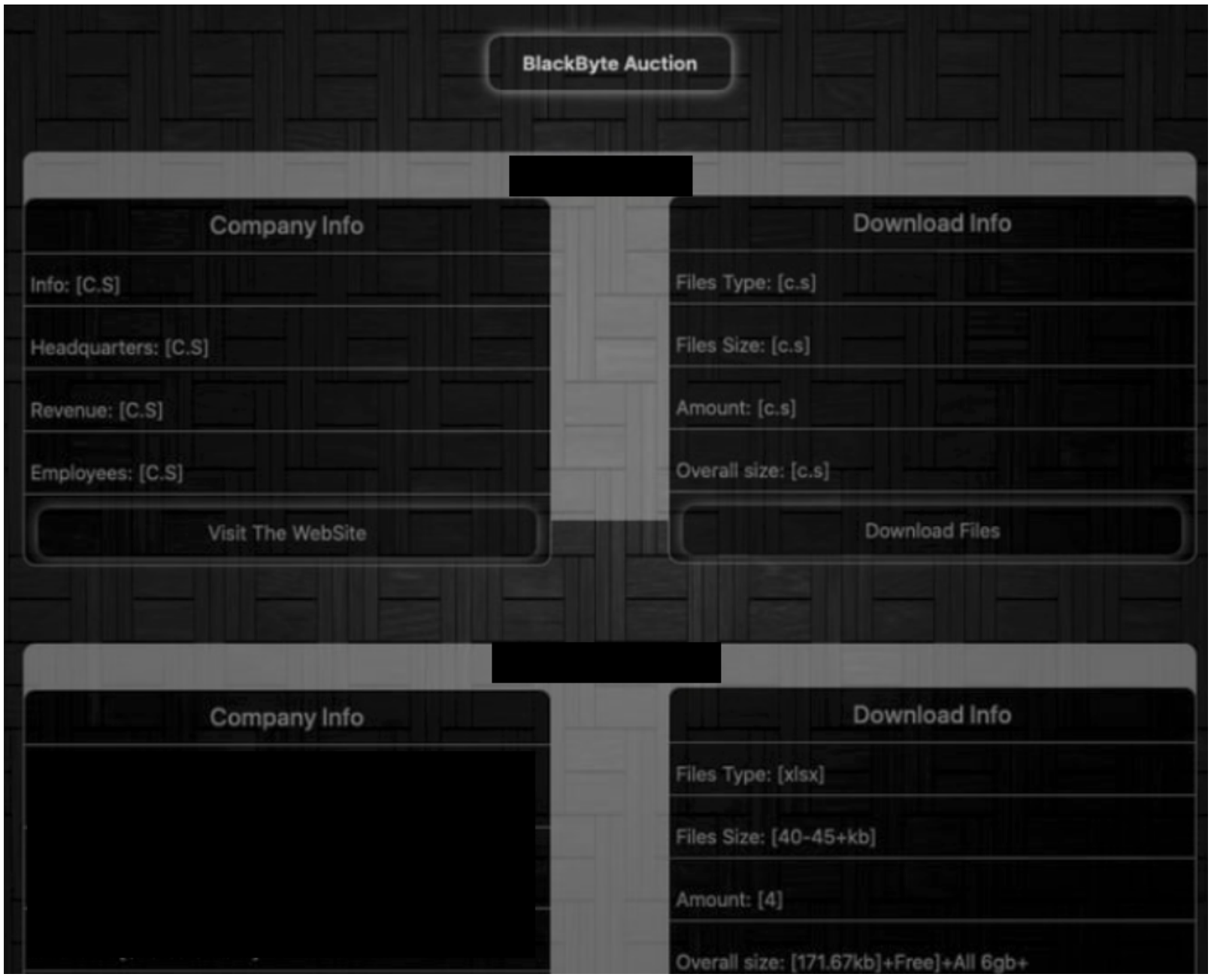

Figure 5. BlackByte Auction site.

Most Notable Recent Attacks

On Feb. 13, 2022, BlackByte operators announced they had compromised the San Francisco 49ers, a U.S. National Football League (NFL) team, and had stolen its financial data.

Given that this attack on the San Francisco 49ers was specifically timed to occur around the 2022 Super Bowl, it is likely that BlackByte operators seek to leverage timing to garner attention and increase profits from an attack.

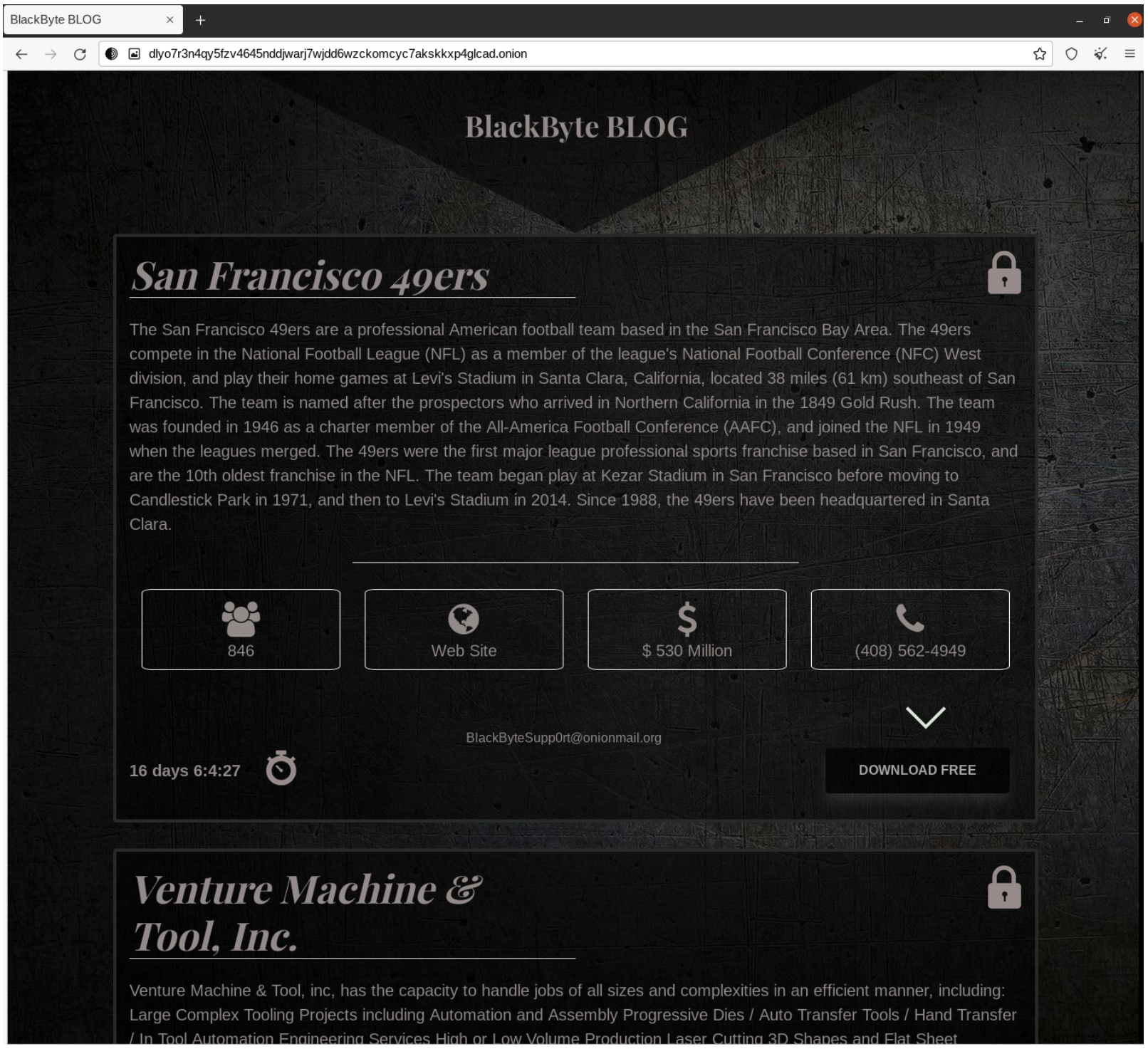

Figure 6. BlackByte .onion blog screenshot.

BlackByte has also reduced its time to pay the ransom from 30 days to 17 days, and then down to 12 days. They have also changed their leak site address multiple times.

According to recent leak site data as well as Unit 42 incident response data, the following industries have been impacted by BlackByte since at least August 2021.

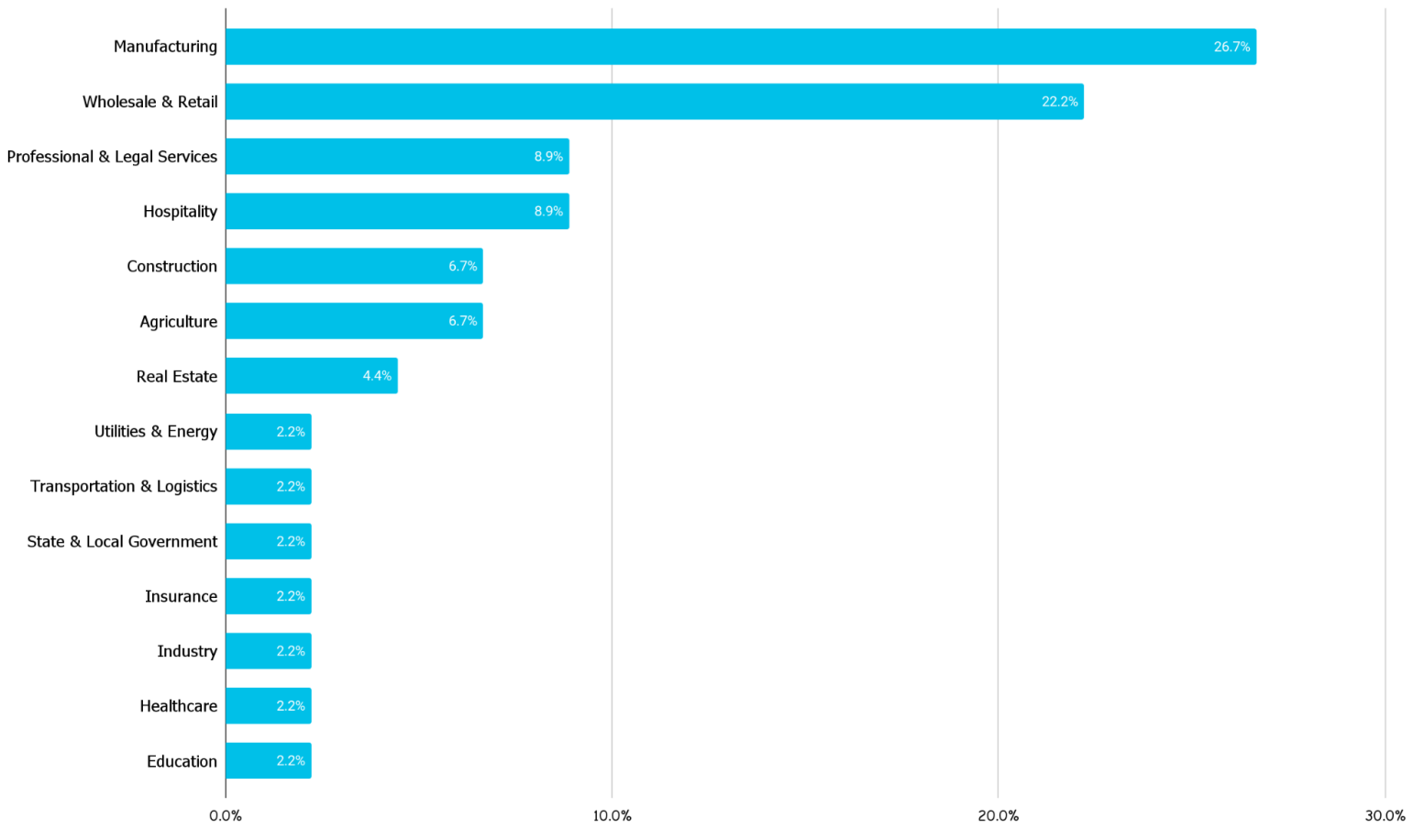

Figure 7. BlackByte targets by industry.

These victims have been observed primarily within the U.S.; however, BlackByte has a global presence and has been observed targeting organizations in the U.S. and Canada, South America, Australia, Europe, Africa and Asia.

Courses of Action

Several adversarial techniques were observed in this activity and the following measures are suggested within Palo Alto Networks products and services to ensure mitigation of threats related to BlackByte ransomware, as well as other malware using similar techniques:

Product / Service	Course of Action
Initial Access	
The below courses of action mitigate the following techniques:	
Exploit Public-Facing Application [T1190]	
THREAT PREVENTION†	Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic
	Ensure a Vulnerability Protection Profile is set to block attacks against critical and high vulnerabilities, and set to default on medium, low, and informational vulnerabilities
WILDFIRE†	Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles
	Ensure that WildFire file size upload limits are maximized
	Ensure a WildFire Analysis profile is enabled for all security policies
	Ensure forwarding of decrypted content to WildFire is enabled
	Ensure all WildFire session information settings are enabled
	Ensure alerts are enabled for malicious files detected by WildFire
	Ensure 'WildFire Update Schedule' is set to download and install updates every minute
CORTEX XSOAR	Deploy XSOAR Playbook Cortex XDR - Isolate Endpoint
NEXT-GENERATION FIREWALLS	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
	Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists
Execution, Persistence, Privilege Escalation, Defense Evasion	
The below courses of action mitigate the following techniques:	
PowerShell [T1059.001], Server Software Component [T1505], Disable or Modify Tools [T1562.001], Modify Registry [T1112], Disable or Modify System Firewall [T1562.004], File Deletion [T1070.004], Scheduled Task [T1053.005], Process Injection [T1055]	
WILDFIRE†	Ensure a WildFire Analysis profile is enabled for all security policies
	Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles
	Ensure alerts are enabled for malicious files detected by WildFire
	Ensure that WildFire file size upload limits are maximized
	Ensure forwarding of decrypted content to WildFire is enabled
	Ensure all WildFire session information settings are enabled
	Ensure 'WildFire Update Schedule' is set to download and install updates every minute
CORTEX XDR PREVENT	Configure Behavioral Threat Protection under the Malware Security Profile
	Enable Anti-Exploit Protection
	Enable Anti-Malware Protection

Credential Access

The below courses of action mitigate the following techniques:

OS Credential Dumping [T1003]

CORTEX XDR PREVENT	Enable Anti-Exploit Protection
	Enable Anti-Malware Protection

Discovery

The below courses of action mitigate the following techniques:

Remote System Discovery [T1018], System Network Configuration Discovery [T1016]

CORTEX XDR PREVENT	Configure Behavioral Threat Protection under the Malware Security Profile
Cortex XDR	XDR monitors for behavioral events via BIOCs along a causality chain to identify discovery behaviors

Lateral Movement

The below courses of action mitigate the following techniques:

SMB/Windows Admin Shares [T1021.002]

Threat Prevention †	Ensure a secure antivirus profile is applied to all relevant security policies
Cortex XDR	Enable Anti-Malware Protection
	Enable Anti-Exploit Protection

Collection

The below courses of action mitigate the following techniques:

Archive via Utility [T1560.001]

Cortex XDR	Monitors for behavioral events via BIOCs including the creation of zip archives

Command and Control

The below courses of action mitigate the following techniques:

Ingress Tool Transfer [T1105]

NEXT-GENERATION FIREWALLS	Ensure that the Certificate used for Decryption is Trusted
	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
	Setup File Blocking
	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
	Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists
	Ensure 'SSL Forward Proxy Policy' for traffic destined to the Internet is configured
	Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS
THREAT PREVENTION†	Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the internet
	Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats
	Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use

	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
	Ensure a secure antivirus profile is applied to all relevant security policies
	Ensure DNS sinkholing is configured on all anti-spyware profiles in use
	Ensure a WildFire Analysis profile is enabled for all security policies
	Ensure 'WildFire Update Schedule' is set to download and install updates every minute
	Ensure alerts are enabled for malicious files detected by WildFire
WILDFIRE	Ensure forwarding of decrypted content to WildFire is enabled
	Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles
	Ensure that WildFire file size upload limits are maximized
	Ensure all WildFire session information settings are enabled
	Ensure that Advanced URL Filtering is used
	Ensure that URL Filtering uses the action of “block” or “override” on the URL categories
URL FILTERING†	Ensure all HTTP Header Logging options are enabled
	Ensure that access to every URL is logged
	Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet
	Deploy XSOAR Playbook - PAN-OS Query Logs for Indicators
CORTEX XSOAR	Deploy XSOAR Playbook - Block URL
	Deploy XSOAR Playbook - Block IP

Impact

The below courses of action mitigate the following techniques:

Inhibit System Recovery [T1490], Data Encrypted for Impact [T1486]

	Deploy XSOAR Playbook - Palo Alto Networks Endpoint Malware Investigation
CORTEX XSOAR	Deploy XSOAR Playbook - Ransomware Manual for incident response.

†These capabilities are part of the NGFW cloud-delivered security subscriptions service

Conclusion

BlackByte ransomware operators have been active since at least July 2021. Due to the high-profile nature and steady stream of BlackByte attacks identified globally in early 2022, the operators and/or affiliates behind the service likely will continue to attack and extort organizations.

Palo Alto Networks detects and prevents BlackByte ransomware in the following ways:

- WildFire: All known samples are identified as malware.
- Cortex XDR:
  - Identifies indicators associated with BlackByte.
  - Anti-Ransomware Module to detect BlackByte encryption behaviors on Windows.
  - Local Analysis detection for BlackByte binaries on Windows.
- Next-Generation Firewalls: DNS Signatures detect the known C2 domains, which are also categorized as malware in Advanced URL Filtering.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call North America Toll-Free: 866.486.4842 (866.4.UNIT42), EMEA: +31.20.299.3130, APAC: +65.6983.8730, or Japan: +81.50.1790.0200.

Indicators of compromise and BlackByte-associated TTPs can be found in the BlackByte ATOM here.

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Additional Resources

- 2022 Unit 42 Ransomware Threat Report

Get updates from

Palo Alto

Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

Please enter your email address!

Please mark, I'm not a robot!

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.