Bee-Ware of Trigona, An Emerging Ransomware Strain

unit42.paloaltonetworks.com/trigona-ransomware-update/

Frank Lee, Scott Roland

March 16, 2023

By Frank Lee and Scott Roland

March 16, 2023 at 6:00 AM

Category: Ransomware, Threat Briefs and Assessments

Tags: ALPHV, BlackCat ransomware, Cortex XDR, CryLock, next-generation firewall, Prisma Cloud, threat assessment, Trigona, WildFire

This post is also available in: 日本語 (Japanese)

Executive Summary

Trigona ransomware is a relatively new strain that security researchers first discovered in late October 2022. By analyzing Trigona ransomware binaries and ransom notes obtained from VirusTotal, as well as information from Unit 42 incident response, we determined that Trigona was very active during December 2022, with at least 15 potential victims being compromised. Affected organizations are in the manufacturing, finance, construction, agriculture, marketing and high technology industries.

Unit 42 researchers identified two new Trigona ransom notes in January 2023 and two in February 2023. Trigona's ransom notes are unique; rather than the usual text file, they are instead presented in an HTML Application with embedded JavaScript containing unique computer IDs (CID) and victim IDs (VID).

Palo Alto Networks helps detect and prevent Trigona ransomware with the following products and services: Cortex XDR, Prisma Cloud and Next-Generation Firewalls (including cloud-delivered security subscriptions such as WildFire) and through incident response.

Related Unit 42 Topics **Ransomware, Ransomware Threat Report, CryLock**

Table of Contents

Trigona Overview

The first mention of Trigona, also the name of a family of stingless bees, comes from a tweet by security researchers in late October 2022. Malware samples were passed to BleepingComputer, which in turn published a blog post on the ransomware on Nov. 29, 2022. Unit 42 consultants also have seen Trigona firsthand in the course of incident response.

Unit 42 researchers have observed Trigona's threat operator engaging in behavior such as obtaining initial access to a target's environment, conducting reconnaissance, transferring malware via remote monitoring and management (RMM) software, creating new user accounts and deploying ransomware.

Ransomware Analysis

Ransomware Binary

Unit 42 obtained and analyzed a sample of the Trigona ransomware binary, named svhost.exe. Upon execution, the ransomware binary uses TDCP_rijndael (a Delphi AES library) to encrypt files. The ransomware then appends the ._locked file extension, modifies registry keys to maintain persistence, and drops ransom notes.

The ransomware binary supports the following command line arguments:

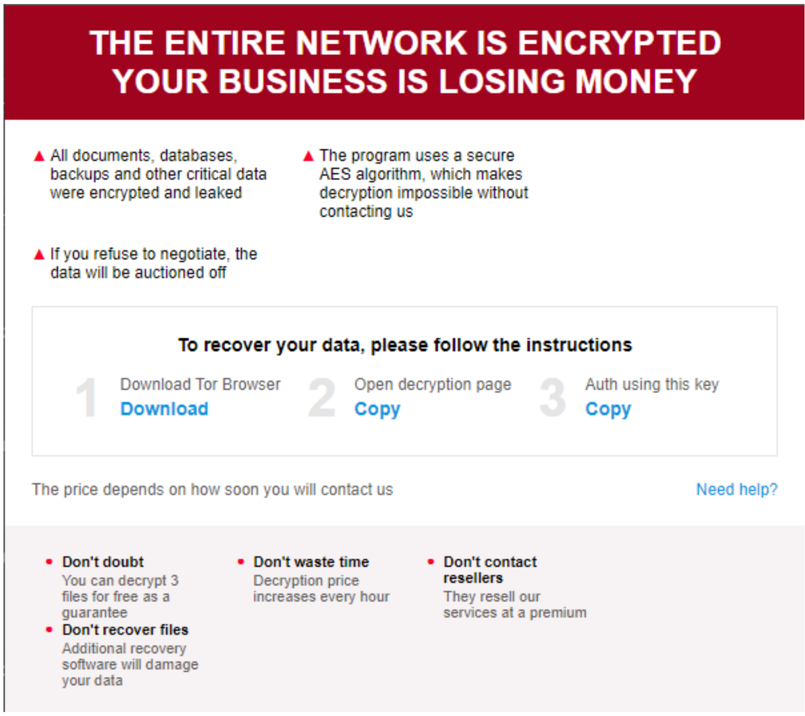
Argument	Description
/full	Performs all functions of the ransomware. Encrypts both local and network files. Creates two registry keys for persistence, one for the ransomware binary and another for the ransom note.
/!autorun	Skips creation of registry keys for persistence
/test_cid "test"	Overwrites default victim generated CID and replace with "test" value
/test_vid "test"	Overwrites default VID and replace with "test" value
/p, /path "path"	Encrypts only files contained within specified path
/!local	Does not encrypt local system files, only encrypts files on local network
/!lan	Does not encrypt local network files, only encrypts files on local system
/autorun_only "path"	Creates registry key for persistence only. Allows for optional "path" to be provided to override default path, does not encrypt files

The ransomware establishes persistence through the creation of two keys in CurrentVersion\Run. Keys found in CurrentVersion\Run contain references to programs that will execute when a user logs in.

One key executes the ransomware binary whenever the user logs in, ensuring that the encryption process would resume upon reboot. The other key ensures that the ransom note is opened every time the user logs in.

Ransom Note

Trigona's ransom note is dropped to the system with the name how_to_decrypt.hta. The HTML code in this file contains embedded JavaScript functionality, which displays ransom note details as shown below in Figure 1.



THE ENTIRE NETWORK IS ENCRYPTED
YOUR BUSINESS IS LOSING MONEY

▲ All documents, databases, backups and other critical data were encrypted and leaked

▲ The program uses a secure AES algorithm, which makes decryption impossible without contacting us

▲ If you refuse to negotiate, the data will be auctioned off

To recover your data, please follow the instructions

1 Download Tor Browser
Download

2 Open decryption page
Copy

3 Auth using this key
Copy

The price depends on how soon you will contact us

Need help?

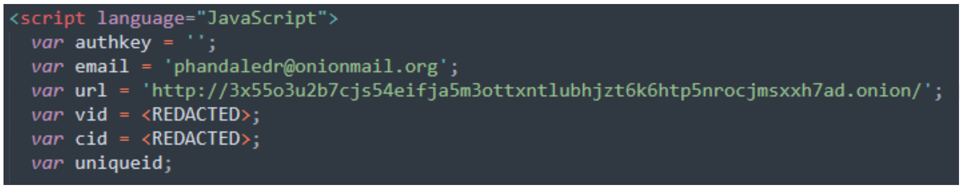
- **Don't doubt** You can decrypt 3 files for free as a guarantee
- **Don't recover files** Additional recovery software will damage your data
- **Don't waste time** Decryption price increases every hour
- **Don't contact resellers** They resell our services at a premium

Figure 1. Sample Trigona ransom note.

Unit 42 researchers observed that the JavaScript within the ransom note contains the following information:

- A uniquely generated CID and VID
- A link to the negotiation Tor portal
- An email address to contact.

The contact email shown below in Figure 2 is phandaledr@onionmail[.]org. We have also seen farusbig@tutanota[.]com used as the contact email in other Trigona ransom notes.



```
<script language="JavaScript">
  var authkey = '';
  var email = 'phandaledr@onionmail.org';
  var url = 'http://3x55o3u2b7cjs54eifja5m3ottxntlubhjzt6k6htp5nrocjmsxxh7ad.onion/';
  var vid = <REDACTED>;
  var cid = <REDACTED>;
  var uniqueid;
```

Figure 2. Embedded JavaScript containing campaign ID and victim ID.

Victimology

By looking at the victim ID in the embedded JavaScript in the Trigona ransom notes, we were able to identify at least 15 potential victims that were compromised in December 2022. We also identified two new Trigona ransom notes in January 2023 and two in February 2023.

Trigona ransomware has been linked to compromises impacting multiple organizations worldwide, in sectors including manufacturing, finance, construction, agriculture, marketing and high technology. The companies impacted were in the United States, Italy, France, Germany, Australia and New Zealand.

Leak Site Analysis

When Trigona was first observed, there was no evidence of this group using a leak site for double extortion. Their ransom note pointed the victims to their negotiation portal instead. During the investigation of this ransomware family, we observed that a researcher identified a leak site attributed to Trigona hosted on the IP address 45.227.253[.]99.

Unit 42 researchers pivoted on the SSH key for 45.227.253[.]99 and identified three other IP addresses related to Trigona's infrastructure:

- 45.227.253[.]106
- 45.227.253[.]98
- 45.227.253[.]107

Each IP shares the same SSH key of ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMjqeylfJyuimtE414TBCxN+lHleN5/P3CNiD4uln5xyHjyw4muLePQj2y3yOJ

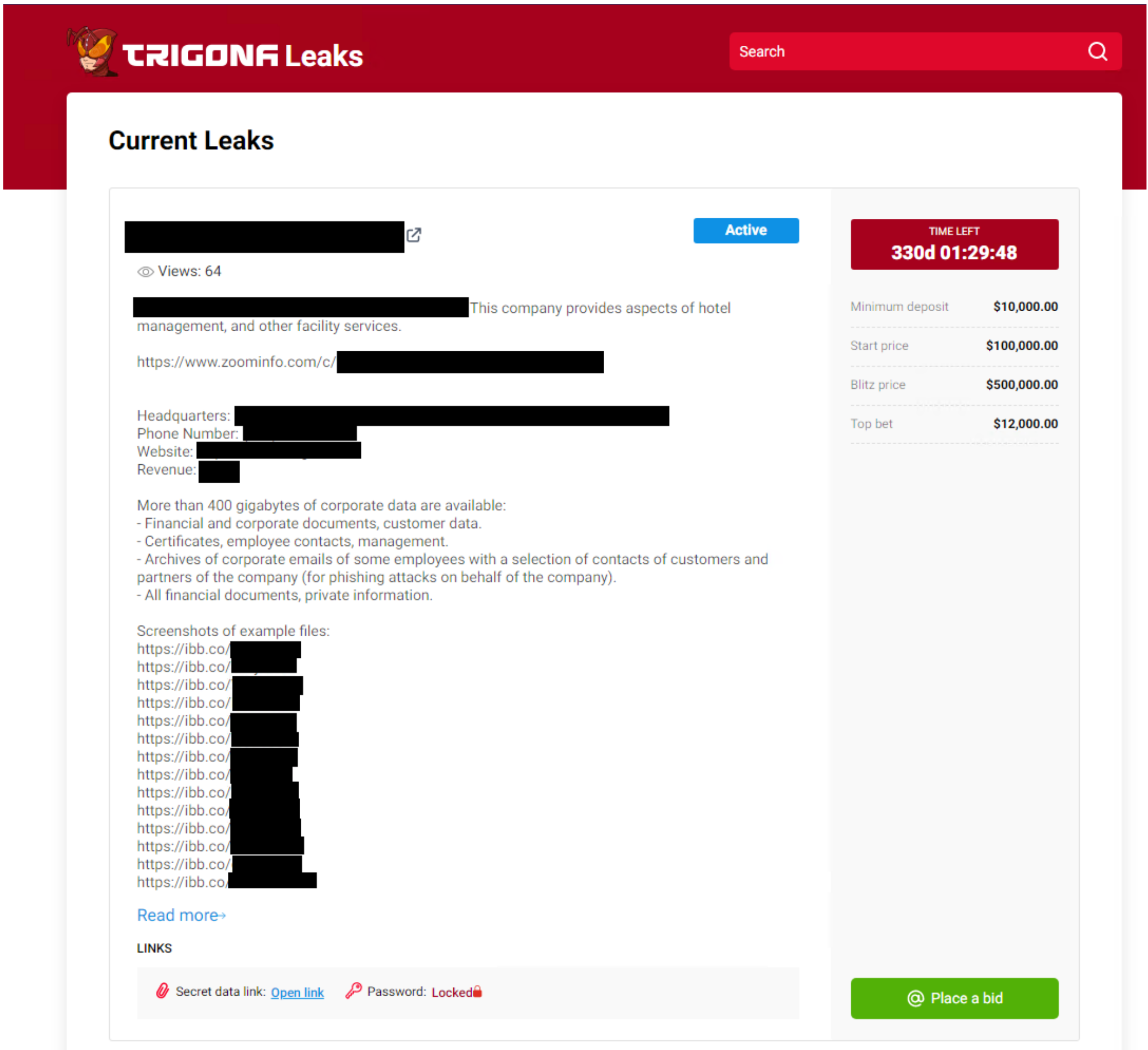
IPs 45.227.253[.]99 and 45.227.253[.]106 hosted web servers on port 8000, while 45.227.253[.]98 and 45.227.253[.]107 hosted no web services.

We identified that 45.227.253[.]99 hosted a web server between Dec. 6, 2022, and Jan. 27, 2023. On Feb. 13, 2023, 45.227.253[.]106 started hosting a web server with the HTML title Trigona Leaks that was active until March 3, 2023.

As shown in Figure 3, each post contained the following information:

- A description of the company
- The victim's ZoomInfo page
- A description of the stolen data
- Links to screenshots of example files
- A countdown timer
- A button to bid for the data.

The "@ Place a bid" button contained a mailto link to auction@mailthink[.]net. Mailthink is a service that allows users to create temporary, disposable email addresses.



Current Leaks

[redacted]

Views: 64

[redacted] This company provides aspects of hotel management, and other facility services.

https://www.zoominfo.com/c/[redacted]

Headquarters: [redacted]
Phone Number: [redacted]
Website: [redacted]
Revenue: [redacted]

More than 400 gigabytes of corporate data are available:
- Financial and corporate documents, customer data.
- Certificates, employee contacts, management.
- Archives of corporate emails of some employees with a selection of contacts of customers and partners of the company (for phishing attacks on behalf of the company).
- All financial documents, private information.

Screenshots of example files:
https://ibb.co/[redacted]
https://ibb.co/[redacted]
https://ibb.co/[redacted]
https://ibb.co/[redacted]
https://ibb.co/[redacted]
https://ibb.co/[redacted]
https://ibb.co/[redacted]
https://ibb.co/[redacted]
https://ibb.co/[redacted]
https://ibb.co/[redacted]
https://ibb.co/[redacted]
https://ibb.co/[redacted]
https://ibb.co/[redacted]
https://ibb.co/[redacted]

Read more→

LINKS

Secret data link: Open link   Password: Locked

TIME LEFT
330d 01:29:48

Minimum deposit	$10,000.00
Start price	$100,000.00
Blitz price	$500,000.00
Top bet	$12,000.00

Figure 3. Trigona leak site.

While the leak site was active, there were four victims:

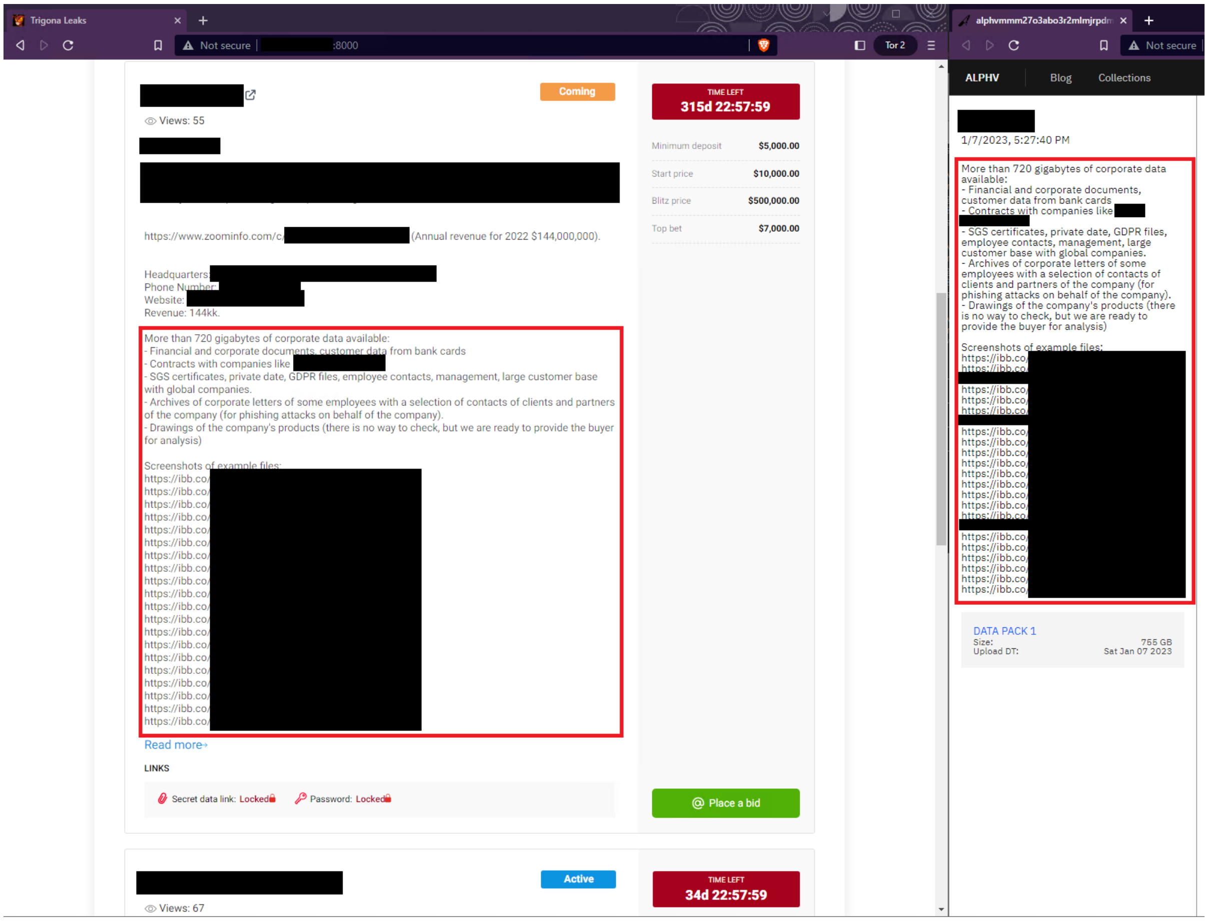
- Victim 1 has a near-duplicate post on the BlackCat (ALPHV) leak site and a countdown timer of over 300 days. Security researchers at Arete Incident Response recently observed Trigona leveraging BlackCat's reputation and data leak site to pressure and extort victims. It's **unclear** whether Victim 1 was impacted by Trigona.
- Victim 2 has a duplicate post on the BlackCat (ALPHV) leak site and a countdown timer of over 300 days. It's **unclear** whether Victim 2 was impacted by Trigona.
- Victim 3 has an associated ransom note on VirusTotal and a countdown timer of just over 30 days. Unit 42 assesses with high confidence that Victim 3 **was impacted** by Trigona.

- Victim 4 is not mentioned on any other ransomware gang’s leak site and has a countdown timer of over 300 days. Unit 42 did not identify any associated ransom notes and it’s **unclear** whether Victim 4 was impacted by Trigona.

The countdown timers of over 300 days for Victims 1, 2 and 4 were well beyond the usual timeframe that we have observed in incident response cases where attackers demand payment, which is between two and four weeks.

Given the following features, the Unit 42 team believes with moderate confidence that the surface web leak page was a development environment to test out features before a possible move to the dark web:

- Several posts appear to be duplicates from the BlackCat leak site (as shown in Figure 4)
- Several of the countdown timers are considerably longer
- The leak site is no longer available on the surface web



[redacted]

Views: 55

[redacted]

[redacted]

https://www.zoominfo.com/c/[redacted](Annual revenue for 2022 $144,000,000).

Headquarters:[redacted]
Phone Number:[redacted]
Website: [redacted]
Revenue: 144kk.

More than 720 gigabytes of corporate data available:
- Financial and corporate documents, customer data from bank cards
- Contracts with companies like [redacted]
- SGS certificates, private date, GDPR files, employee contacts, management, large customer base with global companies.
- Archives of corporate letters of some employees with a selection of contacts of clients and partners of the company (for phishing attacks on behalf of the company).
- Drawings of the company's products (there is no way to check, but we are ready to provide the buyer for analysis)

Screenshots of example files:
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/ [redacted]

Read more→

LINKS

Secret data link: Locked Password: Locked

Minimum deposit	$5,000.00
Start price	$10,000.00
Blitz price	$500,000.00
Top bet	$7,000.00

[redacted]

Views: 67

[redacted]

1/7/2023, 5:27:40 PM

More than 720 gigabytes of corporate data available:
- Financial and corporate documents, customer data from bank cards
- Contracts with companies like [redacted]
- SGS certificates, private date, GDPR files, employee contacts, management, large customer base with global companies.
- Archives of corporate letters of some employees with a selection of contacts of clients and partners of the company (for phishing attacks on behalf of the company).
- Drawings of the company's products (there is no way to check, but we are ready to provide the buyer for analysis)

Screenshots of example files:
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/
https://ibb.co/ [redacted]

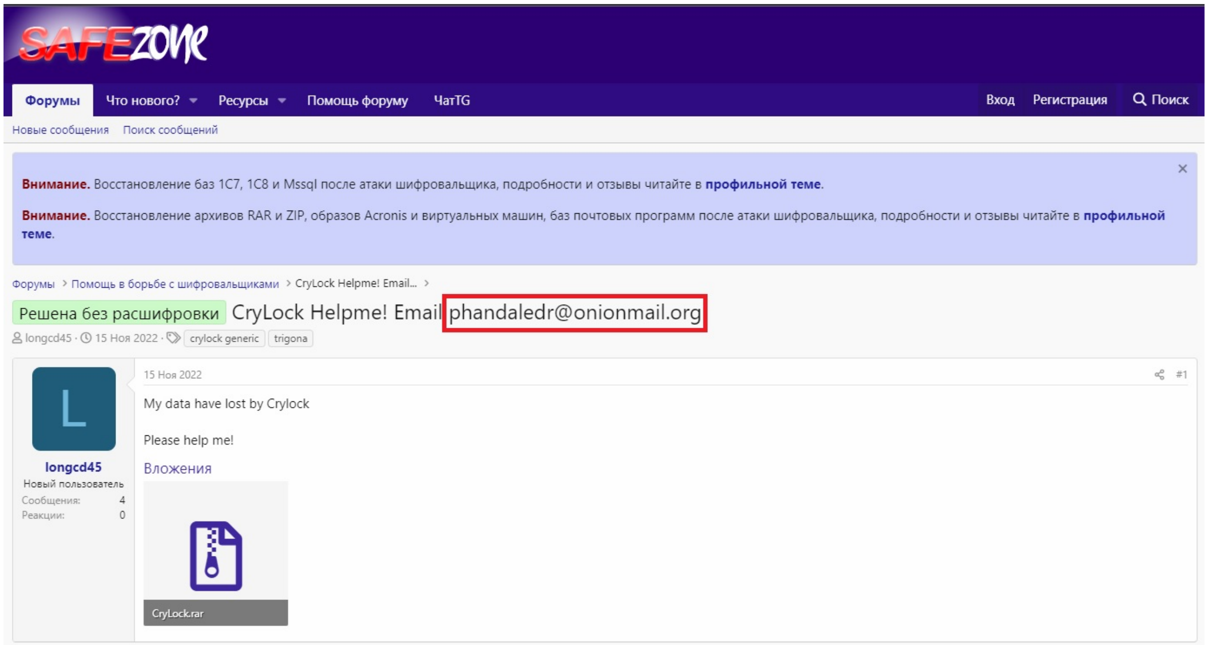
DATA PACK 1
Size: 755 GB
Upload DT: Sat Jan 07 2023

Figure 4.

Comparison between Trigona leak site (left) and BlackCat (ALPHV) leak site (right).

Similarities to CryLock Ransomware

Trigona operators share overlap in tactics, techniques and procedures (TTPs) with CryLock ransomware operators, suggesting that ransomware threat actors that once deployed CryLock ransomware might have moved on to deploying Trigona ransomware. The email associated with Trigona ransom notes analyzed by Unit 42 (phandaledr@onionmail[.]org) was mentioned in an online forum discussing CryLock ransomware, as shown below in Figure 5.



Внимание. Восстановление баз 1С7, 1С8 и Mssql после атаки шифровальщика, подробности и отзывы читайте в **профильной теме**.

Внимание. Восстановление архивов RAR и ZIP, образов Acronis и виртуальных машин, баз почтовых программ после атаки шифровальщика, подробности и отзывы читайте в **профильной теме**.

Решена без расшифровки CryLock Helpme! Email phandaledr@onionmail.org

longcd45 · 15 Ноя 2022

15 Ноя 2022

My data have lost by Crylock

Please help me!

Figure 5. A user on SafeZone, a Russian anti-malware forum, seeking help for Crylock ransomware.

Both ransomware families also drop ransom notes in HTML Application format, named how_to_decrypt.hta. There are also similarities in the ransom message, including:

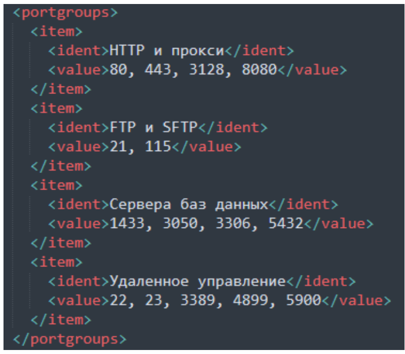
- Their claim that all “documents, databases, backups, and other critical” files and data were encrypted
- AES as their choice of cryptographic algorithm
- Their statement that “the price depends on how soon you will contact us”

Tools and Techniques

Unit 42 has seen evidence of malicious activity associated with Trigona originating from a compromised Windows 2003 server, followed by the threat operators executing NetScan for internal reconnaissance.

NetScan

Unit 42 analysts recovered the NetScan output and noticed that it contained Cyrillic characters, as shown below in Figure 6. Changing the default language of NetScan to Russian is an option that can be configured upon initial installation.



```
<portgroups>
  <item>
    <ident>HTTP и прокси</ident>
    <value>80, 443, 3128, 8080</value>
  </item>
  <item>
    <ident>FTP и SFTP</ident>
    <value>21, 115</value>
  </item>
  <item>
    <ident>Сервера баз данных</ident>
    <value>1433, 3050, 3306, 5432</value>
  </item>
  <item>
    <ident>Удаленное управление</ident>
    <value>22, 23, 3389, 4899, 5900</value>
  </item>
</portgroups>
```

Figure 6. NetScan output that operator(s) left on disk containing Cyrillic characters.

After conducting reconnaissance, Trigona operators used Splashtop – a remote access and management (RMM) tool – to transfer the following malware into the target’s environment.

Threat actors often abuse, take advantage of or subvert legitimate products for malicious purposes. This does not necessarily imply a flaw or malicious quality to the legitimate product being abused.

Start.bat

Start.bat is a batch script that performs the following activities:

- It creates a new folder at C:\temp
- It copies other malicious batch and EXE files from a compromised internal Server Message Block (SMB) server to the newly created temp folder
- It executes Turnoff.bat

Turnoff.bat

Turnoff.bat is a cleanup script used to remove evidence of the attack on a system. It does so by performing the following activities:

- Clearing the Recycle Bin of any mounted drive
- Attempting to use sc stop and taskkill to stop over 100 services related to various areas ranging from remote desktop tools to Windows Defender
- Attempting to stop services related to VMware, Hyper-V and SQL
- Ending several running tasks related to the stopped services mentioned above
- Clear Windows Event Logs (using wevutil cl)
- Deleting Volume Shadow Copies
- Disconnecting all network drives

Unit 42 researchers have observed that cleanup scripts from other threat actors are usually smaller and more specific to the tools used by that actor. The scattershot variety of services and tasks that turnoff.bat stops could suggest that the tool is attempting to ensure that a wider variety of systems are encrypted.

Newuser.bat

Newuser.bat is a batch script that creates a new user with the name fredla and the password Qw123456. It then adds the fredla user to the local groups Administrator and Remote Desktop Users. Threat actors sometimes create privileged user accounts to keep access to target systems without having to install persistent remote access tools on the system.

DC2.exe

DC2.exe contains a password protected version of Mimikatz, which is a tool used for extracting sensitive information such as passwords and authentication credentials from a Windows operating system.

This version of Mimikatz has been compressed using UPX. While UPX is often legitimately used to reduce file size, we have observed threat actors utilizing UPX and other packing programs to evade static detection of the underlying payload.

The tool is also password protected, which adds an extra layer of complexity when ascertaining the program’s functionality.

When the executable is run, the threat actor is prompted for a password to continue. The MD5 hash of the password is then calculated, and if it is equal to 4dbf44c6b1be736ee92ef90090452fc2, the program will continue running.

The password required to achieve the MD5 hash is boris.

Among its many legitimate uses, Unit 42 researchers have most often observed Mimikatz being leveraged maliciously by threat actors in the following ways:

- Credential Loading
  Mimikatz loads credentials from various sources such as Windows memory, Local Security Authority Subsystem Service (LSASS) process and the Windows registry.
- Credential Dumping
  The tool then extracts and dumps the credentials, including usernames and passwords, hashes, and Kerberos tickets to the screen or to a file.
- Credential Manipulation
  Mimikatz allows the user to manipulate the dumped credentials, such as changing passwords, creating new user accounts and adding users to groups.
- Credential Injection
  The tool can also inject the manipulated credentials into other processes, allowing the user to impersonate another user and gain access to restricted resources.

DC4.exe

DC4.exe is a small, UPX-packed password protected binary that generates and executes an embedded batch file. Like DC2.exe, the password to allow the binary to run is boris.

Upon execution, the batch file makes the following changes to the system:

1. Disables the User Account Control (UAC) and sets cmd.exe as a debugger for HelpPane.exe, utilman.exe, Magnify.exe and sethc.exe. This is a common method of creating a “Sticky Keys backdoor” that allows for the creation of a command prompt with NT AUTHORITY\SYSTEM privileges.
2. Opens specific ports on the firewall to allow remote desktop connections using the netsh command.
3. Modifies the Windows registry to allow remote desktop connections.

4. Creates a new user account with the username sys and password Mm1518061+-, and adds this user to the Administrator and Remote Desktop Users groups.

DC6.exe

DC6.exe is an installer for the publicly available tool Advanced Port Scanner, wrapped up in an Inno Setup installer package. Inno Setup is a free software installer for Windows programs. Advanced Port Scanner is a tool that is commonly abused by threat actors for network scanning and mapping, for lateral movement and discovery purposes.

Wrapping Advanced Port Scanner in Inno Setup adds an additional layer of obfuscation to the code, and it is likely to evade static signature detection, forcing dynamic analysis to determine functionality rather than relying on traditional static code signatures.

TTPs

Tactic / Technique	Notes
TA0002 Execution	
T1072. Software Deployment Tools	Trigona operators use Splashtop to move laterally and transfer malware between compromised hosts in the victim's environment.
TA0003 Persistence	
T1546.008. Accessibility Features	DC4.exe creates a batch script that, when executed, creates a "Sticky Keys backdoor" that allows for creation of a command prompt with NT AUTHORITY\SYSTEM privileges.
T1136. Create Account	Newuser.bat creates a new user with the username fredla and password Qw123456.
T1098. Account Manipulation	Trigona operators compromise administrator accounts and use them to conduct malicious activities, such as executing NetScan.
TA0005 Defense Evasion	
T1027. Obfuscated Files or Information	Trigona operators use UPX to pack DC2.exe and DC4.exe to avoid static signature detection. For DC6.exe, Trigona hid the installer for Advanced Port Scanner within Inno Setup installer to evade static signature detection.
T1112. Modify Registry	DC4.exe creates a batch script that, when executed, modifies the Windows Registry to allow remote desktop connections.
T1562.004. Disable or Modify System Firewall	Trigona operators open up an Remote Desktop Protocol (RDP) port in the firewall with DC4.exe.
T1070.001. Indicator Removal: Clear Windows Event Logs	Trigona operators use turnoff.bat to clear event logs via wevtutil cl.
T1070.004. Indicator Removal: File Deletion	Trigona operators delete files such as mim.exe, mim32.exe, zam.exe and zam.bat to cover their tracks. Mim32.exe is associated with Mimikatz while zam.exe and zam.bat are associated with NetScan.
T1036.004. Masquerade Task or Service	Trigona's ransomware binary was named svhost.exe to mimic the legitimate Windows binary svchost.exe.
TA0006 Credential Access	
T1555. Credentials from Password Stores	Trigona operators use Mimikatz to dump passwords.
T1003.001. OS Credential Duping: LSASS Memory	Trigona operators use Mimikatz to dump passwords from LSASS.
TA0007 Discovery	
T1046. Network Service Discovery	Trigona operators use NetScan to enumerate hosts within victims' domains that might be vulnerable to remote software exploitation.
T1069. Permission Groups Discovery	Trigona operators use NetScan to enumerate the security-enabled local group membership of the Administrators group.
T1021.001. Remote Desktop Protocol	Trigona operators utilize RDP to move laterally in the victim's environment.
TA0008 Lateral Movement	
T1570. Lateral Tool Transfer	Trigona operators use Splashtop to transfer malicious tools from computer to computer in the victim's environment.

TA0011 Command and Control	
T1105. Ingress Tool Transfer	Trigona operators utilize Splashtop to transfer netscan.exe*,* netscan.lic*,* netscan.xml*,* newuser.bat*,* start.bat and turnoff.bat.
T1219. Remote Access Software	Trigona operators install and execute remote access tools such as Splashtop on targeted systems.
TA0040 Impact	
T1486. Data Encrypted for Impact	Trigona ransomware encrypts files with the ._locked file extension.
T1489. Service Stop	Turnoff.bat uses sc stop and taskkill to stop services related to remote desktop tools (e.g., ScreenConnect, LogMeIn and TeamViewer), as well as VMware, Hyper-V and SQL.
T1490. Inhibit System Recovery	Trigona operators use Turnoff.bat to delete Volume Shadow Copies.

Conclusion

Trigona is a newer strain of ransomware that, to date, has had minimal coverage by security news articles. This lack of security community awareness allows Trigona to discreetly attack victims while other higher-profile ransomware operations dominate the news headlines. We hope that shining a light on Trigona and its uncommon technique of using password-protected executables to obfuscate malware helps defenders better protect their organizations against this threat.

Due to the stream of victims identified by the Unit 42 team and Trigona's currently developing leak site, the operator and/or affiliates behind the ransomware likely will continue (and possibly even ramp up) its malicious activity.

Palo Alto Networks customers receive protections from Trigona threats through the following products:

- WildFire currently lists all known binaries of Trigona as malicious, which will trigger alerting within Prisma Cloud and Cortex XDR.
- Prisma Cloud will detect any instance of this malware being executed through properly configured Defender agents using Wildfire. Additionally, Prisma Cloud Defender agents can be installed on Windows 2016 and 2019 servers, as well as on Windows Docker Container hosts.

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
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) 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.

Indicators of Compromise

IoC	Note
bef87e4d9fcaed0d8b53bce84ff5c5a70a8a30542100ca6d7822cbc8b76fef13	svhost.exe (Ransomware Binary)
853909af98031c125a351dad804317c323599233e9b14b79ae03f9de572b014e	Splashtop
24123421dd5b78b79abca07bf2dac683e574bf9463046a1d6f84d1177c55f5e5	Netscan
4724EE7274C31C8D418904EE7E600D92680A54FECDAC28606B1D73A28ECB0B1E	Netscan
e22008893c91cf5bfe9f0f41e5c9cdafae178c0558728e9dfabfc11c34769936	Netscan
8d069455c913b1b2047026ef290a664cef2a2e14cbf1c40dce6248bd31ab0067	Netscan
544a4621cba59f3cc2aeb3fe34c2ee4522593377232cd9f78addfe537e988ddc	start.bat
a15c7b264121a7c202c74184365ca13b561fb303fb8699299039a59ab376adc6	turnoff.bat
b7fba3abee8fd3bdac2d05c47ab75fdaa0796722451bed974fb72e442ab4fefd	newuser.bat
e5cf252041045b037b9a358f5412ae004423ad23eac17f3b03ebef7c8147a3bb	Mimikatz

5603d4035201a9e6d0e130c561bdb91f44d8f21192c8e2842def4649333757ab	Mimikatz
69f245dc5e505d2876e2f2eec87fa565c707e7c391845fa8989c14acabc2d3f6	Mimikatz
phandaledr@onionmail[.]org	Ransom note contact email
farusbig@tutanota[.]com	Ransom note contact email
how_to_decrypt.hta	Ransom note name
94979b61bba5685d038b4d66dd5e4e0ced1bba4c41ac253104a210dd517581b8	DC2.exe
9c8a4159166062333f2f74dd9d3489708c35b824986b73697d5c34869b2f7853	DC4.exe
c5d09435d428695ce41526b390c17557973ee9e7e1cf6ca451e5c0ae443470ca	DC6.exe
3x55o3u2b7cjs54eifja5m3ottxntlubhjzt6k6htp5nrocjmsxxh7ad[.]onion	Trigona TOR negotiation portal
45.227.253[.]99	IP address associated with Trigona activity
45.227.253[.]106	IP address currently hosting Trigona leak site
45.227.253[.]98	IP address associated with Trigona activity
45.227.253[.]107	IP address associated with Trigona activity

Additional Resources

Product Protection Guide

Product/Service	Course of Action
Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement	
The below courses of action mitigate the following techniques: Command and Scripting Interpreter [T1059], Create Account [T1136], Account Manipulation [T1098], Local Account [T1136.001], File Deletion [T1070.004], Modify Registry [T1112], Disable or Modify Tools [T1562.001], Disable or Modify System Firewall [T1562.004], Deobfuscate/Decode Files or Information [T1140], Match Legitimate Name or Location [T1036.005], Disable Windows Event Logging [T1562.002], Obfuscated Files or Information [T1027], Clear Windows Event Logs [T1070.001], Masquerade Task or Service [T1036.004], Credentials from Password Stores [T1555], OS Credential Dumping [T1003], LSASS Memory [T1003.001], System Network Configuration Discovery [T1016], System Information Discovery [T1082], Network Service Discovery [T1046], Permission Groups Discovery [T1069], Remote Desktop Protocol [T1021.001], Lateral Tool Transfer [T1570], Software Deployment Tools [T1072], Registry Run Keys / Startup Folder [T1547.001], Accessibility Features [T1546.008], Bypass User Account Control [T1548.002]	
Next-Generation Firewalls	Ensure that the User-ID Agent has minimal permissions if User-ID is enabled
Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones	
Ensure that the User-ID service account does not have interactive logon rights	
Ensure that 'Include/Exclude Networks' is used if User-ID is enabled	
Ensure remote access capabilities for the User-ID service account are forbidden.	
Ensure that User-ID is only enabled for internal trusted interfaces	
Define at least one 'Include Network'.	
Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions	
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 application security policies exist when allowing traffic from an untrusted zone to a more trusted zone	

Cortex XSOAR	Deploy XSOAR Playbook - Access Investigation Playbook
Deploy XSOAR Playbook - Block Account Generic	
Deploy XSOAR Playbook - Impossible Traveler	
Deploy XSOAR Playbook - Port Scan	
Deploy XSOAR Playbook Cortex XDR - Isolate Endpoint	
Cortex XDR Prevent	Configure Behavioral Threat Protection under the Malware Security Profile
Enable Anti-Exploit Protection	
Configure Restrictions Security Profile	
Enable Anti-Malware Protection	
Configure Host Firewall Profile	
Threat Prevention	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats	
Ensure a secure antivirus profile is applied to all relevant security policies	
Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement	
The below courses of action mitigate the following techniques: Create Account [T1136], Account Manipulation [T1098], Local Account [T1136.001], File Deletion [T1070.004], Modify Registry [T1112], Disable or Modify Tools [T1562.001], Disable or Modify System Firewall [T1562.004], Deobfuscate/Decode Files or Information [T1140], Match Legitimate Name or Location [T1036.005], Disable Windows Event Logging [T1562.002], Obfuscated Files or Information [T1027], Clear Windows Event Logs [T1070.001], Masquerade Task or Service [T1036.004], Credentials from Password Stores [T1555], OS Credential Dumping [T1003], LSASS Memory [T1003.001], System Network Configuration Discovery [T1016], System Information Discovery [T1082], Network Service Discovery [T1046], Permission Groups Discovery [T1069], Remote Desktop Protocol [T1021.001], Lateral Tool Transfer [T1570], Software Deployment Tools [T1072], Registry Run Keys / Startup Folder [T1547.001], Accessibility Features [T1546.008], Bypass User Account Control [T1548.002]	
Next-Generation Firewalls	Ensure that the User-ID Agent has minimal permissions if User-ID is enabled
Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones	
Ensure that the User-ID service account does not have interactive logon rights	
Ensure that 'Include/Exclude Networks' is used if User-ID is enabled	
Ensure remote access capabilities for the User-ID service account are forbidden.	
Ensure that User-ID is only enabled for internal trusted interfaces	
Define at least one 'Include Network'.	
Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions	
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 application security policies exist when allowing traffic from an untrusted zone to a more trusted zone	
Cortex XSOAR	Deploy XSOAR Playbook - Access Investigation Playbook
Deploy XSOAR Playbook - Block Account Generic	
Deploy XSOAR Playbook - Impossible Traveler	
Deploy XSOAR Playbook - Port Scan	
Deploy XSOAR Playbook Cortex XDR - Isolate Endpoint	
Cortex XDR Prevent	Configure Behavioral Threat Protection under the Malware Security Profile
Enable Anti-Exploit Protection	
Configure Restrictions Security Profile	
Enable Anti-Malware Protection	
Configure Host Firewall Profile	
Threat Prevention	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats	
Ensure a secure antivirus profile is applied to all relevant security policies	
Persistence, Privilege Escalation, Defense Evasion	
The below courses of action mitigate the following techniques: Create Account [T1136], Account Manipulation [T1098], Local Account [T1136.001], File Deletion [T1070.004], Modify Registry [T1112], Disable or Modify Tools [T1562.001], Disable or Modify System Firewall [T1562.004], Deobfuscate/Decode Files or Information [T1140], Match Legitimate Name or Location [T1036.005], Disable Windows Event Logging [T1562.002], Obfuscated Files or Information [T1027], Clear Windows Event Logs [T1070.001], Masquerade Task or Service [T1036.004], Registry Run Keys / Startup Folder [T1547.001], Accessibility Features [T1546.008], Bypass User Account Control [T1548.002]	
Next-Generation Firewalls	Ensure that the User-ID Agent has minimal permissions if User-ID is enabled
Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones	
Ensure that the User-ID service account does not have interactive logon rights	
Ensure that 'Include/Exclude Networks' is used if User-ID is enabled	
Ensure remote access capabilities for the User-ID service account are forbidden.	
Ensure that User-ID is only enabled for internal trusted interfaces	
Define at least one 'Include Network'.	
Cortex XSOAR	Deploy XSOAR Playbook - Access Investigation Playbook
Deploy XSOAR Playbook - Block Account Generic	

Deploy XSOAR Playbook - Impossible Traveler	
Cortex XDR Prevent	Configure Behavioral Threat Protection under the Malware Security Profile
Enable Anti-Exploit Protection	
Configure Restrictions Security Profile	
Enable Anti-Malware Protection	
Persistence, Privilege Escalation, Defense Evasion	
The below courses of action mitigate the following techniques: File Deletion [T1070.004], Modify Registry [T1112], Disable or Modify Tools [T1562.001], Disable or Modify System Firewall [T1562.004], Deobfuscate/Decode Files or Information [T1140], Match Legitimate Name or Location [T1036.005], Disable Windows Event Logging [T1562.002], Obfuscated Files or Information [T1027], Clear Windows Event Logs [T1070.001], Masquerade Task or Service [T1036.004], Registry Run Keys / Startup Folder [T1547.001], Accessibility Features [T1546.008], Bypass User Account Control [T1548.002]	
Cortex XDR Prevent	Configure Behavioral Threat Protection under the Malware Security Profile
Enable Anti-Exploit Protection	
Configure Restrictions Security Profile	
Enable Anti-Malware Protection	
Privilege Escalation, Defense Evasion	
The below courses of action mitigate the following techniques: File Deletion [T1070.004], Modify Registry [T1112], Disable or Modify Tools [T1562.001], Disable or Modify System Firewall [T1562.004], Deobfuscate/Decode Files or Information [T1140], Match Legitimate Name or Location [T1036.005], Disable Windows Event Logging [T1562.002], Obfuscated Files or Information [T1027], Clear Windows Event Logs [T1070.001], Masquerade Task or Service [T1036.004], Bypass User Account Control [T1548.002]	
Cortex XDR Prevent	Configure Behavioral Threat Protection under the Malware Security Profile
Enable Anti-Exploit Protection	
Configure Restrictions Security Profile	
Enable Anti-Malware Protection	
Defense Evasion	
The below courses of action mitigate the following techniques: File Deletion [T1070.004], Modify Registry [T1112], Disable or Modify Tools [T1562.001], Disable or Modify System Firewall [T1562.004], Deobfuscate/Decode Files or Information [T1140], Match Legitimate Name or Location [T1036.005], Disable Windows Event Logging [T1562.002], Obfuscated Files or Information [T1027], Clear Windows Event Logs [T1070.001], Masquerade Task or Service [T1036.004]	
Cortex XDR Prevent	Configure Behavioral Threat Protection under the Malware Security Profile
Enable Anti-Exploit Protection	
Configure Restrictions Security Profile	

Enable Anti-Malware Protection	
Credential Access	
The below courses of action mitigate the following techniques: Credentials from Password Stores [T1555], OS Credential Dumping [T1003], LSASS Memory [T1003.001]	
Cortex XDR Prevent	Enable Anti-Exploit Protection
Enable Anti-Malware Protection	
Discovery	
The below courses of action mitigate the following techniques: System Network Configuration Discovery [T1016], System Information Discovery [T1082], Network Service Discovery [T1046], Permission Groups Discovery [T1069]	
Next-Generation Firewalls	Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions
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 application security policies exist when allowing traffic from an untrusted zone to a more trusted zone	
Cortex XSOAR	Deploy XSOAR Playbook - Port Scan
Lateral Movement	
The below courses of action mitigate the following techniques: Remote Desktop Protocol [T1021.001], Lateral Tool Transfer [T1570]	
Next-Generation Firewalls	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
Ensure remote access capabilities for the User-ID service account are forbidden.	
Ensure that the User-ID Agent has minimal permissions if User-ID is enabled	
Ensure that User-ID is only enabled for internal trusted interfaces	
Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone	
Ensure that the User-ID service account does not have interactive logon rights	
Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions	
Ensure that 'Include/Exclude Networks' is used if User-ID is enabled	
Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones	
Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists	
Cortex XDR Prevent	Configure Host Firewall Profile

Cortex XSOAR	Deploy XSOAR Playbook - Access Investigation Playbook
Deploy XSOAR Playbook - Block Account Generic	
Threat Prevention	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats	
Ensure a secure antivirus profile is applied to all relevant security policies	
Command and Control	
The below courses of action mitigate the following techniques: Remote Access Software [T1219], 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	
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	
Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist	
Setup File Blocking	
Threat Prevention	Ensure DNS sinkholing is configured on all anti-spyware profiles in use
Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use	
Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet	
Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'	
Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats	
Ensure a secure antivirus profile is applied to all relevant security policies	
URL Filtering	Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet
Ensure all HTTP Header Logging options are enabled	
Ensure that PAN-DB URL Filtering is used	
Ensure that URL Filtering uses the action of “block” or “override” on the URL categories	
Ensure that access to every URL is logged	
Cortex XSOAR	Deploy XSOAR Playbook - PAN-OS Query Logs for Indicators
Deploy XSOAR Playbook - Hunting C&C Communication Playbook (Deprecated)	

Deploy XSOAR Playbook - Block URL	
Deploy XSOAR Playbook - Block IP	
Cortex XDR Prevent	XDR BIOCs / ABIOCs
Impact	
The below courses of action mitigate the following techniques: Data Encrypted for Impact [T1486], Service Stop [T1489], Inhibit System Recovery [T1490]	
Cortex XSOAR	Deploy XSOAR Playbook - Ransomware Manual for incident response.
Deploy XSOAR Playbook - Palo Alto Networks Endpoint Malware Investigation	

Table 1. Product Protection Guide.

Updated March 16, 2023, at 10:13 a.m. PT.