Threat Assessment: Matrix Ransomware

unit42.paloaltonetworks.com/matrix-ransomware

March 26, 2021

By Unit 42

March 26, 2021 at 1:30 PM

Category: Ransomware, Unit 42

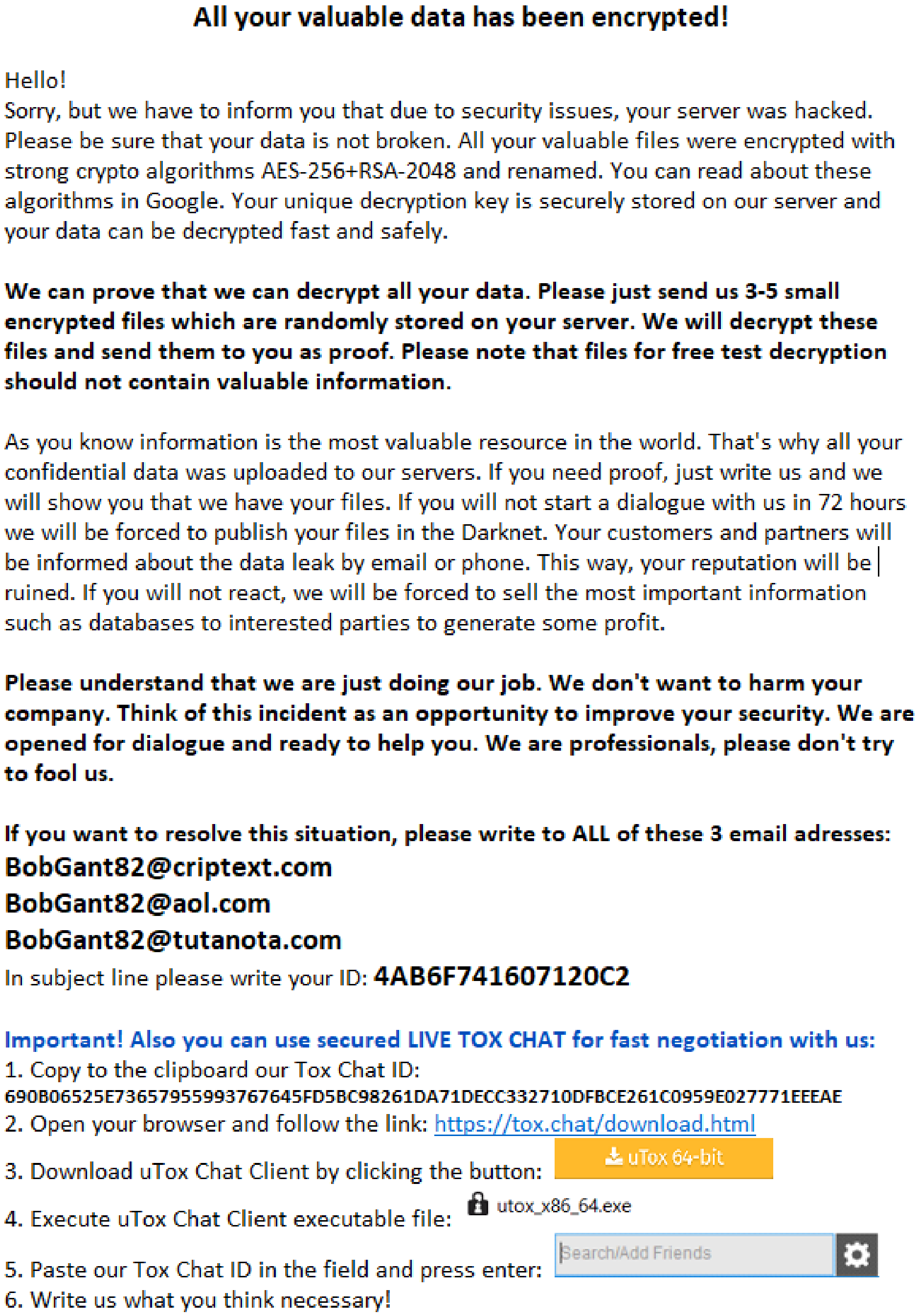
Tags: Matrix, ransomware threat report, threat assessment

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

Executive Summary

Matrix is a ransomware family that was first identified publicly in December 2016. Over the years since its inception, it has primarily targeted small- to medium-sized organizations. As of 2019, it had been observed across geographic locations such as the U.S., Belgium, Taiwan, Singapore, Germany, Brazil, Chile, South Africa, Canada and the UK. While initially leveraging tactics such as spam email campaigns, propagation via Windows shortcuts and the RIG exploit kit for distribution, the primary attack vector for the Matrix ransomware family shifted in 2018 to brute forcing weak Remote Desktop Protocol (RDP) credentials. The shift to this attack methodology appears to be a recurring trend in similar targeted ransomware families such as Dharma, Ryuk and BitPaymer.

Matrix Ransomware Overview



All your valuable data has been encrypted!

Hello!
Sorry, but we have to inform you that due to security issues, your server was hacked. Please be sure that your data is not broken. All your valuable files were encrypted with strong crypto algorithms AES-256+RSA-2048 and renamed. You can read about these algorithms in Google. Your unique decryption key is securely stored on our server and your data can be decrypted fast and safely.

We can prove that we can decrypt all your data. Please just send us 3-5 small encrypted files which are randomly stored on your server. We will decrypt these files and send them to you as proof. Please note that files for free test decryption should not contain valuable information.

As you know information is the most valuable resource in the world. That's why all your confidential data was uploaded to our servers. If you need proof, just write us and we will show you that we have your files. If you will not start a dialogue with us in 72 hours we will be forced to publish your files in the Darknet. Your customers and partners will be informed about the data leak by email or phone. This way, your reputation will be ruined. If you will not react, we will be forced to sell the most important information such as databases to interested parties to generate some profit.

Please understand that we are just doing our job. We don't want to harm your company. Think of this incident as an opportunity to improve your security. We are opened for dialogue and ready to help you. We are professionals, please don't try to fool us.

If you want to resolve this situation, please write to ALL of these 3 email adresses:
BobGant82@criptext.com
BobGant82@aol.com
BobGant82@tutanota.com
In subject line please write your ID: **4AB6F741607120C2**

Important! Also you can use secured LIVE TOX CHAT for fast negotiation with us:
1. Copy to the clipboard our Tox Chat ID:
690B06525E73657955993767645FD5BC98261DA71DECC332710DFBCE261C0959E027771EEEAE
2. Open your browser and follow the link: https://tox.chat/download.html
3. Download uTox Chat Client by clicking the button:
4. Execute uTox Chat Client executable file:
5. Paste our Tox Chat ID in the field and press enter:
6. Write us what you think necessary!

Figure 1. Screenshot of Matrix ransom note

When executed, Matrix encrypts user files and network shares, as well as deleting volume shadow copies and disabling recovery options on the affected device. Like with many other ransomware variants, the ransom note delivered by Matrix demands payment in Bitcoin. Instead of spreading through an organization, past Matrix infections appear to have been more targeted in nature.

Matrix is unique in that instead of delivering a more conventional ransom note that demands a fixed ransom amount, the threat actors behind it ask victims to contact them directly and submit a small sample of about three to five files for decryption. This is done so the threat actors can determine a variable ransom based on factors such as the predicted value of the victim's files or the current dollar value of Bitcoin.

As of 2020, Matrix ransomware has been seen appending the following file extensions on files:
.MTXLOCK, .CORE, .ANN, .FOX, .KOK8, .KOK08, .NEWRAR, .FASTBOB, .FASTB, .EMAN, .THDA, .RAD, .EMAN50, .GMPF, .ATOM, .NOBAD, .TRU8, .FASTA, .JNSS, .FBK, .ITLOCK, .SPCT, .PRCP, .CHRB, .AL8G, .DEUS, .FG69, .JB88, .J91D, .S996, .[barboza40@yahoo.com], .[Linersmik@naver.com][Jinnyg@tutanota.com], .[poluz@tutanota.com], .[Yourencrypt@tutanota.com], .[Files4463@tuta.io], .[RestorFile@tutanota.com], .[RestoreFile@qq.com], .[oken@tutanota.com], .[Vfemacry@mail-on.us], .[d3336666@tutanota.com], and .[Bitmine8@tutanota.com]

In addition, Matrix has other variants, including one dubbed "Fox Ransomware," which adds the ".FOX" extension to encrypted files.

More information on prominent ransomware families can be found in the 2021 Unit 42 Ransomware Threat Report.

Courses of Action

This section documents relevant tactics, techniques and procedures (TTPs) used with Matrix and maps them directly to Palo Alto Networks product(s) and service(s). It also further instructs customers on how to ensure their devices are configured correctly.

Product / Service	Course of Action
Initial Access, Persistence, Lateral Movement	
The below courses of action mitigate the following techniques: **Spearphishing Attachment [T1566.001], Valid Accounts [T1078], Replication Through Removable Media [T1091], Remote Desktop Protocol [T1021.001]**	
NGFW	Set up File Blocking
	Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones
	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
	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 that User-ID is only enabled for internal trusted interfaces
	Ensure that 'Include/Exclude Networks' is used if User-ID is enabled
	Ensure that the User-ID Agent has minimal permissions if User-ID is enabled
	Ensure that the User-ID service account does not have interactive logon rights
	Ensure remote access capabilities for the User-ID service account are forbidden
Threat Prevention†	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 that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned and set to appropriate actions
WildFire†	Ensure that WildFire file size upload limits are maximized
	Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles
	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 XDR	Configure Host Firewall Profile
	Configure Malware Security Profile
	Enable Device Control
Cortex XSOAR	Deploy XSOAR Playbook - Block Account Generic
	Deploy XSOAR Playbook - Access Investigation Playbook
	Deploy XSOAR Playbook - Impossible Traveler

	Deploy XSOAR Playbook - Phishing Investigation - Generic V2
	Deploy XSOAR Playbook - Endpoint Malware Investigation
Credential Access	
The below courses of action mitigate the following techniques: **Brute Force [T1110]**	
NGFW	Customize the Action and Trigger Conditions for a Brute Force Signature
Cortex XSOAR	Deploy XSOAR Playbook - Brute Force Investigation Playbook
Execution, Defense Evasion, Persistence, Privilege Escalation, Impact	
The below courses of action mitigate the following techniques: **Windows Command Shell [T1059.003], Match Legitimate Name or Location [T1036.005], Services File Permissions Weakness [T1574.010], Disable or Modify Tools [T1562.001], Service Stop [T1489], Modify Registry [T1112], Data Encrypted for Impact [T1486], Inhibit System Recovery [T1490]**	
Cortex XDR	Enable Anti-Exploit Protection
	Enable Anti-Malware Protection
	Configure Restrictions Security Profile
	Configure Behavioral Threat Protection under the Malware Security Profile
Cortex XSOAR	Deploy XSOAR Playbook - Ransomware Manual for incident response.
	Deploy XSOAR Playbook - Palo Alto Networks Endpoint Malware Investigation

Table 1. Courses of Action for Matrix ransomware.

†These capabilities are part of the NGFW security subscriptions service.

Conclusion

While targeted ransomware attacks are not new, Matrix is a prime example of how threat actors can enter into the pool of existing ransomware and cash out quickly by targeting low-hanging fruit. The ransom negotiation tactics used by the Matrix threat actors further amplifyies the dangerous impact that such an attack can have on its victims, especially given the volatile state of cryptocurrency value today. Furthermore, this malware family's shift in tactics to RDP exploitation, following a similar shift seen in other ransomware groups, serves to emphasize the need for businesses to stay vigilant on current ransomware trends.

Palo Alto Networks detects and prevents Matrix in the following ways:

- WildFire: All known samples are identified as malware.

- Cortex XDR with:
  - Iindicators for Matrix.
  - Anti-Ransomware Module to detect Matrix encryption behaviors.
  - Local Analysis detection to detect Matrix binaries.
- Next-Generation Firewalls: DNS Signatures detect the known command and control (C2) domains, which are also categorized as malware in URL Filtering.
- AutoFocus: Tracking related activity using the MatrixRansomware tag.

Additionally, Indicators of Compromise (IoCs) associated with Matrix are available on GitHub here, and have been published to the Unit 42 TAXII feed.

Additional Resources

Get updates from Palo Alto Networks!

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