Ransomware Roundup – Trigona | FortiGuard Labs

By Shunichi Imano

Published: 2023-02-02 · Archived: 2026-04-05 15:57:47 UTC

On a bi-weekly basis, FortiGuard Labs gathers data on ransomware variants of interest that have been gaining traction within our datasets and the OSINT community. The Ransomware Roundup report aims to provide readers with brief insights into the evolving ransomware landscape and the Fortinet solutions that protect against those variants.

This latest edition of the Ransomware Roundup covers the Trigona ransomware.

Affected platforms: Microsoft Windows
Impacted parties: Microsoft Windows Users
Impact: Encrypts files on the compromised machine and demands ransom for file decryption
Severity level: High

Trigona Ransomware Overview

The Trigona ransomware variant was first reported in October 2022. Trigona has adopted the double-extortion methodology of encrypting endpoints and/or other infrastructure of value within an organization and then threatening to release exfiltrated data from those machines on the internet if a ransom is not paid. As proof that users can get affected files back, the Trigona threat actor offers free decryption of up to three files.

Some public reports suggest Trigona ransomware activity picked up towards the end of 2022.

Trigona Ransomware Infection Vector

While the infection vector has not been identified, deployment via other malware distributed using emails, Remote Desktop Protocol (RDP), and exploiting vulnerabilities are suspected distribution methods.

Trigona Ransomware Execution

When launched, the ransomware encrypts files on compromised machines and adds a “._locked” file extension to those encrypted files.

It also leaves a “how_to_decrypt.hta” file, shown below. This is an HTML file that contains details on how to recover encrypted data as well as how to contact the Trigona ransomware threat actor. While a download link for the Tor browser is available in the ransom note, it no longer worked at the time of the investigation. As such, users are expected to find and visit the official Tor site to download and install the Tor browser.

Once a link to the decryption page is copied and opened on the Tor browser, Trigona ransomware victims are presented with a sign-up page where they can enter a key left in the ransom note.

In the next screen, victims are asked to enter a username and set a login password.

Some variants of Trigona ransomware do not direct victims to the Tor site. Instead, the ransom note asks victims to email the attacker.

Publicly available reports indicate that victims are asked to buy and pay an unknown amount of ransom in Monero (XMR) cryptocurrency after logging into the Tor site. The Tor site also offers a victim support chat option.

Fortinet Protection

Fortinet customers are already protected from this malware variant through FortiGuard's Web Filtering, AntiVirus, and FortiEDR services, as follows:

FortiGuard Labs detects known Trigona ransomware variants with the following AV signature:

- W32/Filecoder.OLC!tr.ransom

IOCs

File-based IOCs:

SHA256
248e7d2463bbfee6e3141b7e55fa87d73eba50a7daa25bed40a03ee82e93d7db
596cf4cc2bbe87d5f19cca11561a93785b6f0e8fa51989bf7db7619582f25864
704f1655ce9127d7aab6d82660b48a127b5f00cadd7282acb03c440f21dae5e2
859e62c87826a759dbff2594927ead2b5fd23031b37b53233062f68549222311
8f8d01131ef7a66fd220dc91388e3c21988d975d54b6e69befd06ad7de9f6079
97c79199c2f3f2edf2fdc8c59c8770e1cb8726e7e441da2c4162470a710b35f5
a86ed15ca8d1da51ca14e55d12b4965fb352b80e75d064df9413954f4e1be0a7

accd5bcf57e8f9ef803079396f525955d2cfffbf5fe8279f744ee17a7c7b9aac
da32b322268455757a4ef22bdeb009c58eaca9717113f1597675c50e6a36960a
e7c9ec3048d3ea5b16dce31ec01fd0f1a965f5ae1cbc1276d35e224831d307fc
e97de28072dd10cde0e778604762aa26ebcb4cef505000d95b4fb95872ad741b
f29b948905449f330d2e5070d767d0dac4837d0b566eee28282dc78749083684
fa6f869798d289ee7b70d00a649145b01a93f425257c05394663ff48c7877b0d
fbba6f4fd457dec3e85be2a628e31378dc8d395ae8a927b2dde40880701879f2
fd25d5aca273485dec73260bdee67e5ff876eaa687b157250dfa792892f6a1b6

FortiGuard Labs Guidance

Due to the ease of disruption, damage to daily operations, potential impact to an organization's reputation, and the unwanted destruction or release of personally identifiable information (PII), etc., it is vital to keep all AV and IPS signatures up to date.

Since the majority of ransomware is delivered via phishing, organizations should consider leveraging Fortinet solutions designed to train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

Our FREE NSE training: NSE 1 – Information Security Awareness includes a module on internet threats designed to help end users learn how to identify and protect themselves from various types of phishing attacks and can be easily added to internal training programs.

Organizations will need to make foundational changes to the frequency, location, and security of their data backups to effectively deal with the evolving and rapidly expanding risk of ransomware. When coupled with digital supply chain compromise and a workforce telecommuting into the network, there is a real risk that attacks

can come from anywhere. Cloud-based security solutions, such as SASE, to protect off-network devices; advanced endpoint security, such as EDR (endpoint detection and response) solutions that can disrupt malware mid-attack; and Zero Trust Access and network segmentation strategies that restrict access to applications and resources based on policy and context, should all be investigated to minimize risk and to reduce the impact of a successful ransomware attack.

As part of the industry's leading fully integrated Security Fabric, delivering native synergy and automation across your security ecosystem, Fortinet also provides an extensive portfolio of technology and human-based as-a-service offerings. These services are powered by our global FortiGuard team of seasoned cybersecurity experts.

Best Practices include Not Paying a Ransom

Organizations such as CISA, NCSC, the FBI, and HHS caution ransomware victims against paying a ransom partly because payment does not guarantee that files will be recovered. According to a U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) advisory, ransom payments may also embolden adversaries to target additional organizations, encourage other criminal actors to distribute ransomware, and/or fund illicit activities that could potentially be illegal. For organizations and individuals affected by ransomware, the FBI has a Ransomware Complaint page where victims can submit samples of ransomware activity via their Internet Crimes Complaint Center (IC3).

How Fortinet Can Help

FortiGuard Labs' Emergency Incident Response Service provides rapid and effective response when an incident is detected. And our Incident Readiness Subscription Service provides tools and guidance to help you better prepare for a cyber incident through readiness assessments, IR playbook development, and IR playbook testing (tabletop exercises).

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard AI-powered security services portfolio.
