Examining the Cring Ransomware Techniques

trendmicro.com/en_us/research/21/i/examining-the-cring-ransomware-techniques.html

September 24, 2021

In this entry, we look at the techniques typically employed by the Cring ransomware, as well as the most affected regions and industries.

By: Warren Sto.Tomas September 24, 2021 Read time: (words)

Content added to Folio

Here is a more detailed description of this chain:

Initial Access

The Cring ransomware gains initial access either through unsecure or compromised RDP or valid accounts.

The ransomware can also get into the system through certain vulnerability exploits.. The abuse of the aforementioned Adobe ColdFusion flaw (CVE-2010-2861) to enter the system is a new development for the threat. In the past, Cring was also used to exploit a FortiGate VPN server vulnerability (CVE-2018-13379).

Credential Access

Threat actors behind Cring used weaponized tools in their attacks. One of these tools is Mimikatz, which was used to steal account credentials of users who had previously logged into the system.

Lateral Movement and Defense Evasion

Lateral movement was done through Cobalt Strike. This tool was also used to distribute BAT files that will be used later for various purposes, including impairing the system's defenses.

Command and Control and Execution

Cobalt Strike was also used to continuously communicate with the main command-and-control (C&C) server.

BAT files were used to download and execute the Cring ransomware on the other systems in the compromised network. It also uses the Windows CertUtil program to help with the said download.

Impact

Once Cringhas been executed in the system, it disables services and processes that might hinder the ransomware's encryption routine. The threat will also delete backup files and folders. This will make restoring the encrypted files difficult for the victim, thereby placing more pressure on them to pay the ransom.

The ransomware will then proceed with its encryption routine and delete itself using a BAT file.

Regions and industries with the Cring ransomware detections

Based on our data, most of the Cring ransomware detections for attempted attacks were observed in Europe and the Middle East and Africa (EMEA) region. There have also been incidents in the Latin American Region (LAR), Asia Pacific (APAC), and North America (NABU).

The affected countries in the said regions were Azerbaijan, Brazil, Italy, Mexico, Saudi Arabia, the United States, and Turkey. With regard to industries, detections affected the finance and transportation sectors. Indeed, ransomware has been consistently attacking critical industries, as we discuss in our midyear report.

How to protect systems from ransomware

With ransomware, prevention is one of the most potent forms of protection. A proactive approach such as patching vulnerabilities and monitoring systems for signs of unusual behavior helps curb ransomware before it can cause any real damage to a system.

In the larger scheme of things, coming up with ransomware defense plans will help enterprises know which steps to prioritize. Here are some best practices that follow the lead of frameworks set by the Center of Internet Security (CIS)and the National Institute of Standards and Technology (NIST):

- **Audit events and take inventory.** Audit both event and incident logs to spot suspicious behavior.Take note of all assets and data. Identify authorized and unauthorized devices and programs.
- **Configure and monitor.** Manage hardware and software configurations. Only grant administrative privileges when necessary.
- **Patch and update.** Conduct regular vulnerability assessments and patching or virtual patching for operating systems and programs. Update software and applications.
- **Protect systems and recover data.** Administer data protection, backup, and recovery measures. Implement multifactor authentication (MFA).
- **Secure and defend layers:** Perform sandbox analysis to filter malicious emails. Employ security solutions to all layers of the system such as email, endpoint, web, and network.
- **Train and test.** Conduct regular training and security skills assessment for employees. Perform red-team exercises and penetration tests.

Trend Micro solutions

Organizations can benefit from multilayered protection (for layers such as endpoint, email, web, and network) with security solutions that can detect malicious components and help monitor concealed malicious behaviors in the system.

Trend Micro Vision One™ spots suspicious behaviors that might seem insignificant when observed from only a single layer. Trend Micro Apex One™ protects endpoint devices through automated threat detection and response against ransomware, fileless threats, and other advanced concerns.

Trend Micro Cloud One™ Workload Security defends systems against threats that exploit vulnerabilities. This is done through virtual patching, machine learning (ML), and harnessing the latest in global threat intelligence.

Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block ransomware before it gets into the system, since one of the ways ransomware spreads is through malicious emails.