Examining the Cring Ransomware Techniques

By By: Warren Sto.Tomas Sep 24, 2021 Read time: 4 min (1004 words)

Published: 2021-09-24 · Archived: 2026-04-05 16:22:58 UTC

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-2010-2861open on a new tab) 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-2018-13379open on a new tab).

Credential Access

Threat actors behind Cring used weaponized toolsnews- cybercrime-and-digital-threats 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 Cring has 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 Securityopen on a new tab (CIS)and the National Institute of Standards and Technologyopen on a new tab (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™products spots suspicious behaviors that might seem insignificant when observed from only a single layer. Trend Micro Apex One™products protects endpoint devices through automated threat detection and response against ransomware, fileless threats, and other advanced concerns.

Trend Micro Cloud One™ Workload Securityproducts 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 Inspectorproducts 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.

Indicators of Compromise (IOCs)

SHA-256	**Trend Micro Pattern Detection**
f7d270ca0f2b4d21830787431f881cd004b2eb102cc3048c6b4d69cb775511c8	Ransom.MSIL.CRYNG.A
e687308cd4184e17c33fa9e44686e7d6a4d73adf65f7fb3cac9c4ad765b4ffdf	Ransom.Win32.CRING.C
771a680f9a09a7a73ac2678f31f4d82fce49c046cc5f4c415cea5310b833911f	Trojan.BAT.DISABLER.AA
71821ddb0b49f5b91fc520ca3de1c5ea7cee3bf166ddebd625859966fc5221a2	Trojan.BAT.CRING.A
a999e096a9fb6a994f4d58b04001c61bb2d1fd0d4f0fa87a5be0b61b23591f24	Trojan.PS1.COBEACON.FAIN

MITRE ATT&CK Tactics and Techniques

Tactic	**Technique**
Initial access	T1078: Valid Accounts T1190: Exploit Public-Facing Application
Execution	T1059: Command and Scripting Interpreter
Persistence	T1546.012: Event Triggered Execution: Image File Execution Options Injection
Privilege Escalation	T1078.002: Valid Accounts: Domain Accounts

Defense Evasion	T1562.001: Impair Defenses: Disable or Modify Tools T1070.004: Indicator Removal on Host: File Deletion
Credential Access	T1003: OS Credential Dumping T1552: Unsecured Credentials
Discovery	T1083: File and Directory Discovery
Lateral Movement	T1570: Lateral Tool Transfer T1105: Remote File Copy T1021: Remote Services
Command and Control	T1090: Proxy T1105: Ingress Tool Transfer T1043: Commonly Used Port T1188: Multi-hop Proxy T1094: Custom Command and Control Protocol
Exfiltration	T1041: Exfiltration Over C2 Channel
Impact	T1486: Data Encrypted for Impact T1489: Service Stop T1485: Data Destruction T1490: Inhibit System Recovery