JULY 8th, 2021

REvil Ransomware Attack

Metmox's Approach

IT Management Platform **Kaseya** Hit with Sodinokibi/REvil Ransomware Attack.

The Problem

The Cybersecurity and Infrastructure Security Agency (CISA) shared that Kaseya's VSA software was used to push a malicious PowerShell script. The VSA software, which is typically used to remotely distribute software updates and cloud-based monitoring platforms for MSPs/customers, was weaponized.

The Analysis

REvil will fingerprint the target machine and gather system information. Before beginning the encryption routine, REvil will kill certain processes such as email clients, SQL or other database servers, browsers, and Microsoft Office applications to ensure it can encrypt important files belonging to the victim

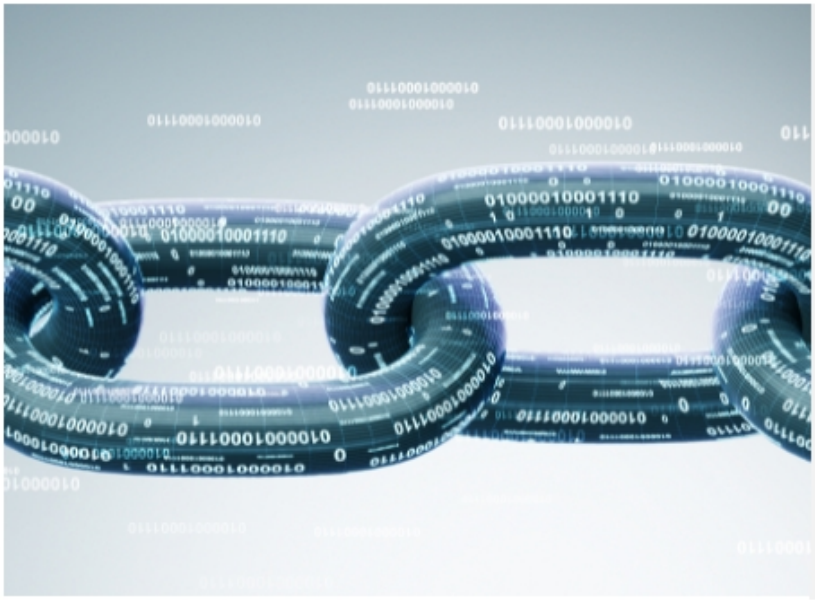
Business Impact

A universal decryptor that could be used to free all the victims—all the customers of Kaseya's customers—and save the attackers the bother of negotiating with each of up to 1,500 victims separately is being sold for USD 70 million in bitcoins as ransom

Here are the IOCs associated with REvil Ransomware:

- AutoRun Registry Key:
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Windows\CurrentVersion\Run\[a-zA-Z0-9]{10}
- Custom Wallpaper Image:
C:\User\<Username>\AppData\Local\Temp\[a-zA-Z0-9]{13}.bmp
- Encrypted Files:
<file_name>.<alpha-numeric_extension>
- URLs for Ransom Payment:
hxxp://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd[dot]onion/4DD2F2803EC112D7
hxxp://decoder[dot]re/4DD2F2803EC112D7

REvil uses curve25519/Salsa20; key encryption utilizes curve25519/AES-256-CTR.



Like decryptor[.]cc and decryptor[.]top in previous REvil/Sodinokibi versions, decoder[.]re is used to grant the victims access to the threat actors WEB-site for further negotiations should their connection be limited via TOR. Decoder[.]re resolves to IP 82.146.34.4 (AS29182) belonging to a Russian ISP/cloud hosting company.

CISA-FBI also issued guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack. Implement allow the listing to limit communication with remote monitoring and management (RMM) capabilities to known IP address pairs, and/or place administrative interfaces of RMM behind a virtual private network (VPN) or a firewall on a dedicated administrative network.

Metmox's Approach to detection of REvil

As a part of threat detection and response services, we have proactively setup use cases/alert policies to detect the following:

- Registry Run Keys / Startup Folder. New Startup Program Creation.
- Modifying the Services registry location
- Changes the autorun value in the registry.
- **Alert if a process:**
    1. Reads the computer name
    2. Checks supported languages
    3. Reads Environment values
    4. Changes internet zones settings
- Manual execution of any executable/process by the user
- Renames names and extensions of the file
- Attempt to create a hardlink to a file
- Detection of encryption activity
- Windows Registry, Process monitoring, Process command-line parameters.

Metmox's Cybersecurity Practitioners, Professional Services (PS), and Security Specialists are available to help determine the next steps beyond the guidance/guidelines for detection of REvil ransomware as briefed.

We provide recommendations, best practices, outcome-based solutions, and value-added tips on how to leverage our services as part of your threat detection and response as we get started.

We are ranked at #63 by MSSP Alert 2020 among the top 250 Cybersecurity companies of the world. Our Intelligence-Driven Expert-Led - IDEAL Fusion SOC Platform - Helps Security Analysts find the needle in the haystack through advanced threat detection and response.

Contact us now for reduced security risk and improved security posture delivered to tight deadlines, stringent SLAs, unbeatable prices, 24×7 visibility, and LIMITED free MSS readiness assessment of your current SOC operations, Or visit our website to know what our clients say about us.

To get in touch: info@metmox.com