SEKOIA.IO

Neutralize Threat Before they Do

FLINT.

SEKOIA.IO THREAT **INTEL**LIGENCE **FLASH** REPORT

Kaseya: Another Massive Heist by REvil

July 2021

Kaseya: Another Massive Heist by REvil

OBJECTIVES:
FINANCIAL GAIN

STATUS:
ONGOING

INTRUSION SET:
REVIL aka SODINOKIBI

AFFECTED SECTORS: **TECHNOLOGY, RETAIL (AT LEAST FOR CONFIRMED VICTIMS)**

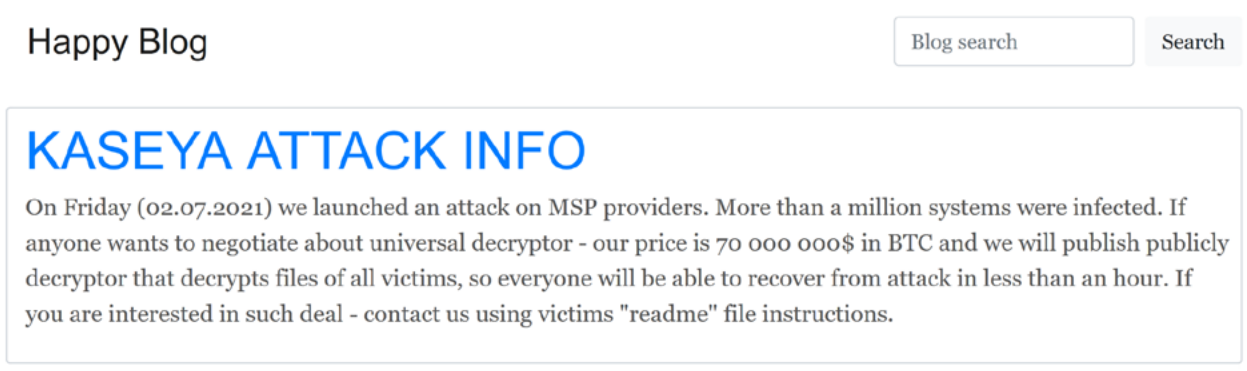
IMPACTED GEOGRAPHIES: **WORLDWIDE**

SUMMARY

On July 2, 2021, the threat actor undoubtedly carried out one of its largest ransomware heists known so far through a third party attack.

The group managed to compromise Kaseya VSA, a solution used by Managed Service Providers (MSPs) to manage their client systems. According to an updated Kaseya notice, fewer than 60 of the company's customers using the VSA on-premises product were directly compromised, with a global impact to fewer than 1.500 downstream businesses. A patch for on-premises clients is to be released within 24 hours after the SaaS Data Center restoration.

On July 5, 2021 REvil group claimed responsibility for the attack on "more than a million systems" and demanded a $70 million ransom payment to release a "universal decryptor".


Happy Blog

Blog search Search

KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

ANALYSIS

A zero day vulnerability to get initial access

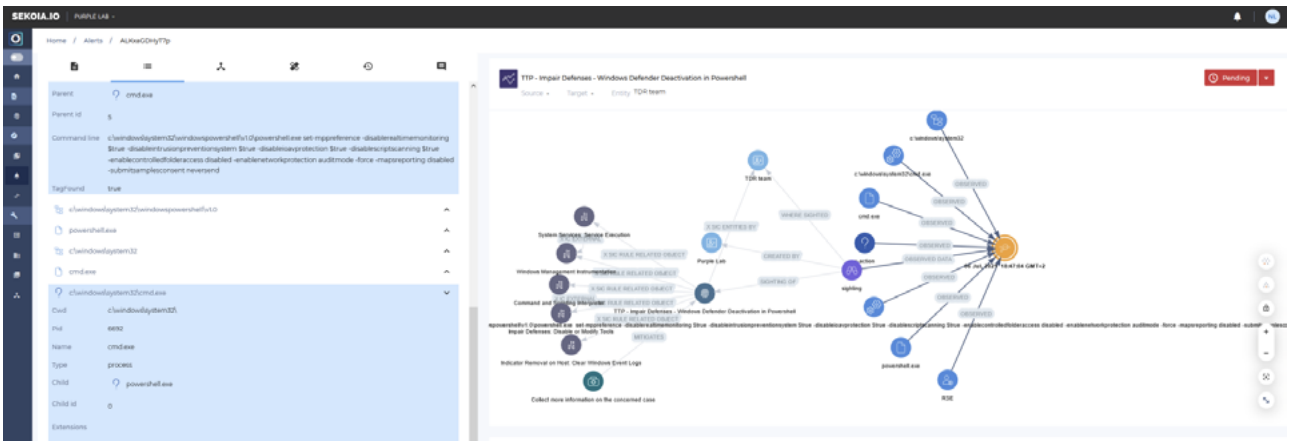
The REvil group got the initial access by exploiting a zero day vulnerability, CVE-2021–30116, in Kaseya VSA. The vulnerability was identified a few weeks ago by a researcher from DIVD, a cybersecurity organization, that reported the vulnerability to Kaseya under responsible disclosure guidelines. Hence, it is likely that Kaseya ran out of time before the vulnerability was exploited in the attack.

At that time, the nature and details of the vulnerability are still undisclosed, however some indications point towards an authentication bypass in the VSA web interface.

A fake update to spread REvil ransomware

Once the attackers have set foot in the VSA system, they dropped a base64-encoded malicious payload agent.crt that was delivered through the 'Kaseya VSA Agent Hot-fix' update. A PowerShell command was then executed to carry out many well-known Impair Defenses techniques that led to Windows Defender deactivation.

These types of attacks are detected by SEKOIA.IO since many rules related to Impair Defenses and other techniques are implemented in our solution.



The powershell command was also designed to masquerade as Windows system utility certutil.exe, which is an admin command line tool intended to be used for manipulating certificates' data and components. Hence, the PowerShell command copied certutil.exe to another location that is not the original one. It was then renamed to cert.exe. This latter was then used to decode the base64-encoded payload agent.crt and save it as agent.exe. To harden forensic analysis, both cert.exe and agent.crt were removed from victim systems.

Then, the execution of agent.exe led to the extraction of two files:

- mpsvc.dll which is the DLL used by REvil to encrypt victim's systems.
- an older version of the legitimate Microsoft Defender executable which was used as a living-off-the-land binary (LOLBin). Hence, this binary which is a trusted Windows executable, was used to launch mpsvc.dll file with DLL side-loading to encrypt the systems.

A complex cryptographic scheme

The unique encryption system (file key – system key – affiliate key) made it possible for REvil affiliates to ask for customized ransoms for each individual encrypted file extension found on a victim's network. However, REvil group is also selling a universal decryption key that would alledgedly be able to decode all victim's data.

Unlike other previous attacks, this time the group is apparently not exfiltrating data so it is not using data theft extortion to force payments.

Anti-virus and Firewall exclusions in the spotlight once again

For the Kaseya Agent to function properly, Kaseya asks its customers to disable anti-virus protection for some system components on which it's running. In fact, this is a very common practice among a considerable number of vendors, which may result in overlooking security incidents.

This is a particularly increasing concern, also knowing that Kaseya already faced a ransomware attack performed by GrandCrab in 2019. The precursors of the REvil group then targeted the same VSA remote monitoring and management tool.

Kaseya response to the incident

Following the incident, Kaseya shut down its cloud-based infrastructures and urged its VSA customers to take servers offline.

According to DIVD, two days after the attack, only 140 servers were still online while they were 2.200 before the attack. This response has probably helped to mitigate the severity of the attack, which could have been much worse.

Victimology

The main victims of the attack were the endpoints (mostly small businesses) managed by the Kaseya's MSP customers. According to TheRecord, five MSPs have publicly admitted to being impacted by the REvil attacks on Kaseya servers, namely VelzArt, Hoppenbrouwers, Visma EssCom, Synnex, and Avtex.

Coop supermarket chain is one of the indirect victims, whose overall picture is not well known yet. After cross checking different sources, the attack appears to have a global scale, with victims in at least 29 countries all over the world.

This is the result of the dramatic amplification effect of a successful third-party attack. The wide third-party attack surface is a real appetizer for ransomware operators, as it provides high returns in case of successful attack.

A well-planned attack timeline

The Kaseya attack occurred on late Friday, just before the 4th of July extended weekend. There is quite a common *modus operandi* behind the most severe attacks operated by REvil: the deployment of ransomware is often performed over a weekend or on holidays to take advantage of understaffed security teams.

Third-party attacks, a further proof of the power of their impact

Apart from Kaseya, one of the most recent third-party attacks targeted SolarWinds. While these campaigns have different goals, i.e: massive intelligence operation vs attempt to extort money, they showed us how powerful and devastating their effects can be.

Hence, the risks associated with a third-party attack are no longer to be demonstrated, and an increasing number of attacks are now taking advantage of third party trusts. At the same time, businesses are relying more and more on outside providers. Thus, it is recommended for organizations to look closely at their software providers, particularly those with privileged access to their systems and implement the least privileges principles as far as possible.

Keep your VSA servers offline until further Kaseya instructions on when it is safe to resume operations.

Apply the VSA patch as soon as Kaseya releases it and keep software patches up to date.

Hunt for indicators of compromise on your network and block malicious traffic.

IOCS & TECHNICAL DETAILS

IP addresses:

- *35.226.94[.]113*
- *161.35.239[.]148*
- *162.253.124[.]162*

Hashes (SHA256):

- *cc0cdc6a3d843e22c98170713abf1d6ae06e8b5e34ed06ac3159adafe85e3bd6 (Mpsvc.dll)*
- *d5ce6f36a06b0dc8ce8e7e2c9a53e66094c2adfc93cfac61dd09efe9ac45a75f (Mpsvc.dll)*
- *d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e (C:\kworking\agent.exe)*
- *0496ca57e387b10dfdac809de8a4e039f68e8d66535d5d19ec76d39f7d0a4402 (MpsVc.dll, MpsVc, mpsvc.dll, MpsVc_.dll)*
- *d8353cfc5e696d3ae402c7c70565c1e7f31e49bcf74a6e12e5ab044f306b4b20 (Mpsvc.dll)*
- *8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd (Mpsvc.dll)*
- *dc6b0e8c1e9c113f0364e1c8370060dee3fcbe25b667ddeca7623a95cd21411f (Updater.exe)*
- *aae6e388e774180bc3eb96dad5d5bfefd63d0eb7124d68b6991701936801f1c7 (p.exe.TXT)*
- *66490c59cb9630b53fa3fa7125b5c9511afde38edab4459065938c1974229ca8 (svchost.exe)*
- *8e846ed965bbc0270a6f58c5818e039ef2fb78def4d2bf82348ca786ea0cea4f (Revil12_browsingDll.dll)*
- *2093c195b6c1fd6ab9e1110c13096c5fe130b75a84a27748007ae52d9e951643 (agent.crt)*
- *f2d6ef0450660aaae62c429610b964949812df2da1c57646fc29aa51c3f031e (Revil1_browsingExe.exe)*

Additional indicators are available here:

- *https://github.com/pgl/kaseya-revil-cnc-domains/blob/main/revil-kaseya-cnc-domains.txt*
- *https://otx.alienvault.com/pulse/60e02f9e498dfdf25caf7753*
- *https://community.sophos.com/b/security-blog/posts/active-ransomware-attack-on-kaseya-customers*
- *https://www.cadosecurity.com/post/resources-for-dfir-professionals-responding-to-the-revil-ransomware-kaseya-supply-chain-attack*

Cado-security provided resources, including IOCs, for DFIR Professionals Responding to the REvil Ransomware Kaseya Attack.

TTPS (ATT&CK)

Exploit Public-Facing Application (T1190)

Supply Chain Compromise: Compromise Software Supply Chain (T1195.002)

Command and Scripting Interpreter: PowerShell (T1059.001)

Hijack Execution Flow: DLL Side-Loading (T1574.002)
Masquerading (T1036)

Impair Defenses: Disable or Modify Tools (T1562.001)

Deobfuscate/Decode Files or Information (T1140)

Indicator Removal on Host (T1070)

Subvert Trust Controls: Code Signing (T1553.002)

Modify Registry (T1112)

Data Encrypted for Impact (T1486)

CONFIDENCE
HIGH

REFERENCES

- SEKOIA.IO Investigation
- [Kaseya] Updates Regarding VSA Security Incident
- [Sophos] Kaseya VSA Supply-Chain Ransomware Attack
- [Sophos] Independence Day: REvil uses supply chain exploit to attack hundreds of businesses
- [DFIR] DFIR Resources REvil Kaseya github repository
- [Doublepulsar] Kaseya supply chain attack delivers mass ransomware event to US companies
- [Welivesecurity] Kaseya supply-chain attack: What we know so far
- [Picus] TTPs Used by REvil (Sodinokibi) Ransomware Gang in Kaseya MSP Supply-Chain Attack

NEUTRALIZE THREATS BEFORE THEY DO

SEKOIA.IO

www.sekoia.io

Follow our news