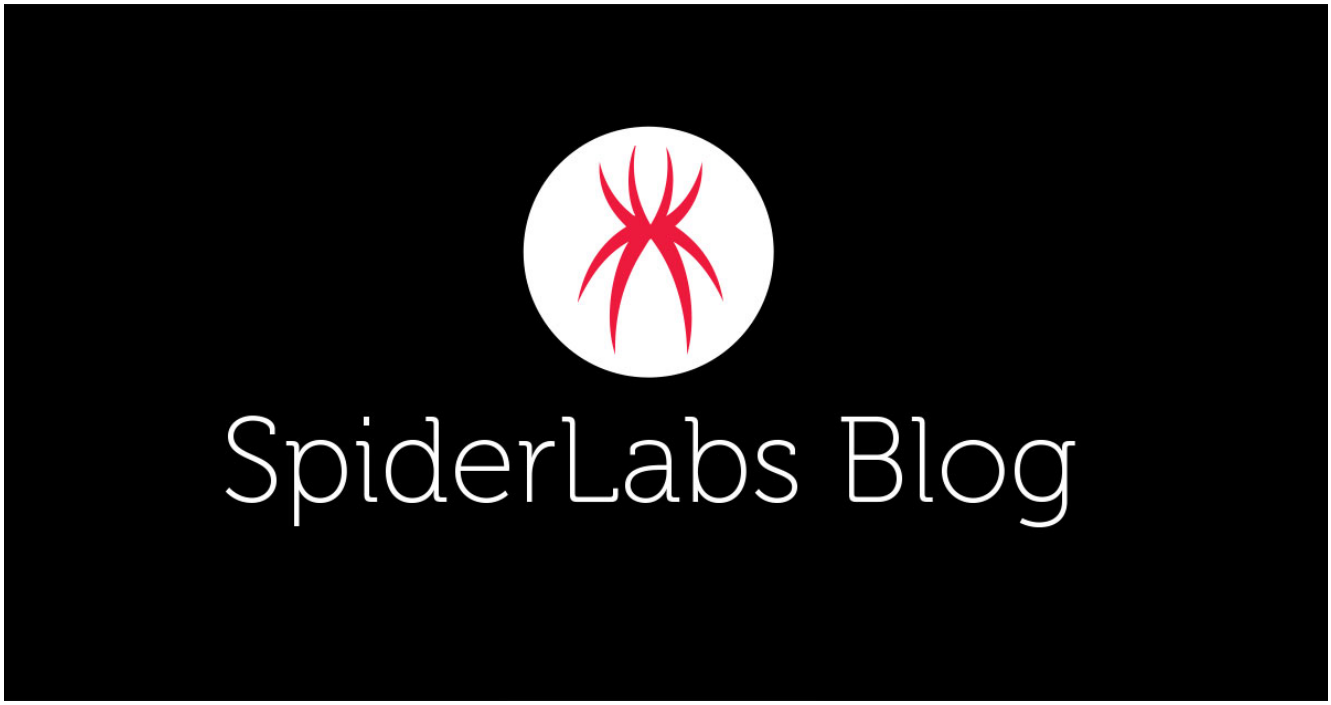
Diving Deeper Into the Kaseya VSA Attack: REvil Returns and Other Hackers Are Riding Their Coattails

trustwave.com/en-us/resources/blogs/spiderlabs-blog/diving-deeper-into-the-kaseya-vsa-attack-revil-returns-and-other-hackers-are-riding-their-coattails/



On, July 2nd, a massive ransomware attack was launched against roughly 60 managed services providers (MSPs) by criminals associated with the REvil ransomware-as-a-service (RaaS) group.

The attack leveraged the on-premises servers deployed by IT Management Software vendor Kaseya. It was initially thought that Kaseya might have been compromised themselves as a root cause -- similar to the compromises associated with SolarWinds software in December of 2020. Instead, the attackers found and leveraged an unpatched zero-day vulnerability in Kaseya's VSA software. At the time of this blog, 1,500 downstream customers of these MSPs have been infected with ransomware.

This vulnerability has been issued CVE-2021-30116 and was discovered and reported to Kaseya by a researcher for the Dutch Institute for Vulnerability Disclosure (DIVD). A patch was being actively worked on by Kaseya according to the DIVD, but not finalized prior to REvil discovering and exploiting the issue. At this point, it is still not clear what the actual issue is or how the exploit may work, although initial reports suggest a potential authentication bypass. A patch has not been released, and Kaseya is recommending that customers with on-premises VSA Servers take them offline until a patch is issued. The REvil group initially demanded $70 million USD to reveal a universal decryptor for all affected victims but has since lowered the demand to $50 million.

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.

In the past, the REvil group has also exfiltrated data either for sale or to pressure a victim even more into paying the ransom. This appears to be the case with this campaign as well, as we've seen REvil call out many customers bragging on their Darknet hosted "Happy Blog" about the amount of data they have in their possession.

[redacted] / 500GB

- Personal data of clients;
- Drawings;
- Projects;
- Contracts;
- Finance reports;
- and other company documents.

Example:

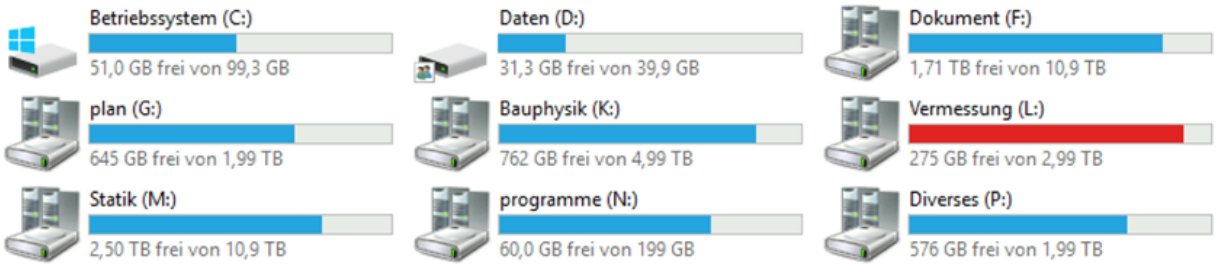


Figure 1: Victim A showing a list of data types REvil has access to and drive mappings as proof

[redacted]

[redacted] and was incorporated in 1919.

All you network has been locked.You sensitive data has been downloaded.
You have 10 days to contact us

proofs

full dump

Click to view all

Figure 2: Victim B with a description of the company and links to proof of compromise

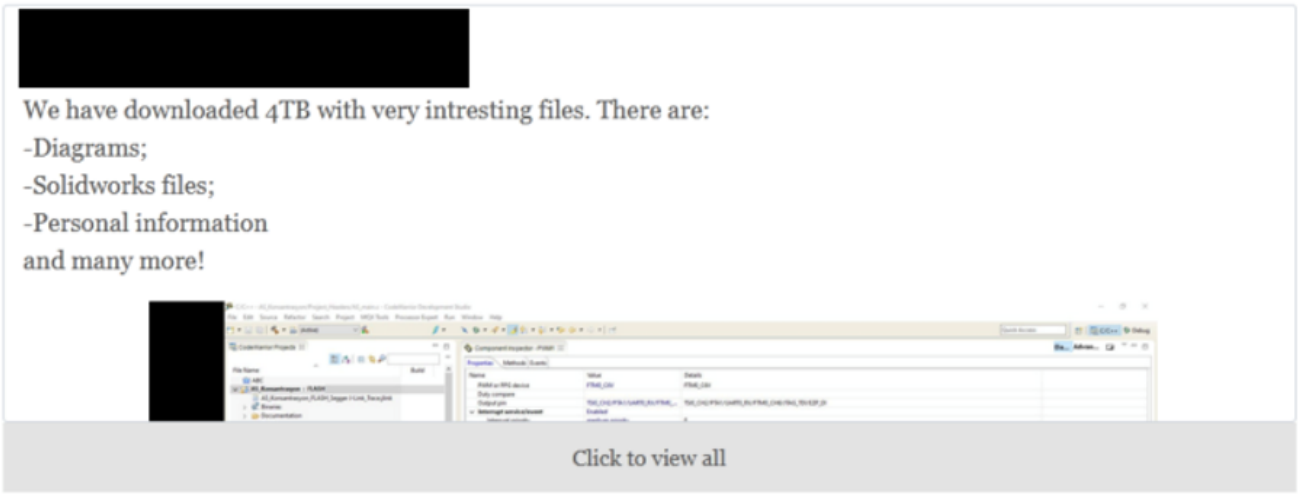


Figure 3: Victim C with 4TB of compromised files and a screenshot as proof of access

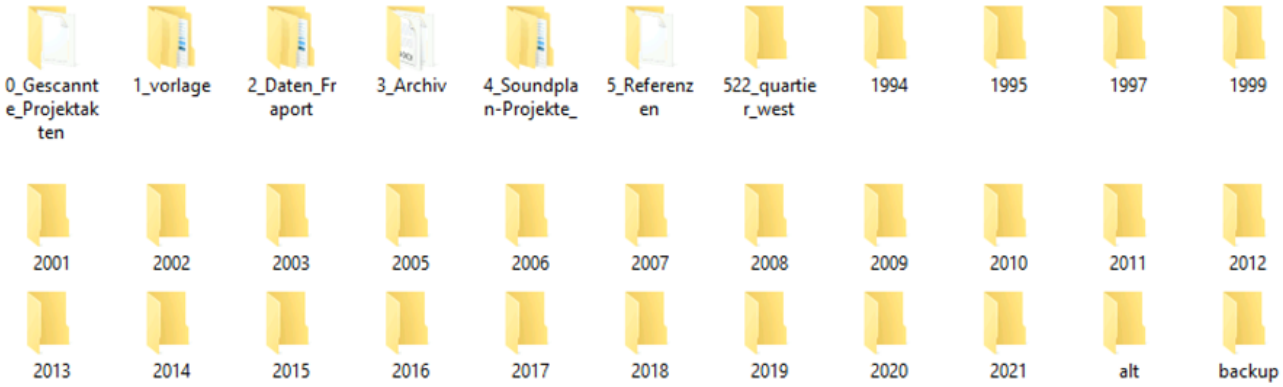


Figure 4: Victim D with screenshot as proof of access showing data going back to 1994

Malware Analysis

Over the course of the weekend, our SpiderLabs Malware Analysis team received a malware submission from our Global Threat Operations group. They were investigating a piece of DLL file they found on one of our customer's critical servers hit by a ransomware attack. This server was running Kaseya VSA. The file is a digitally signed DLL with a file named **mpsvc.dll**

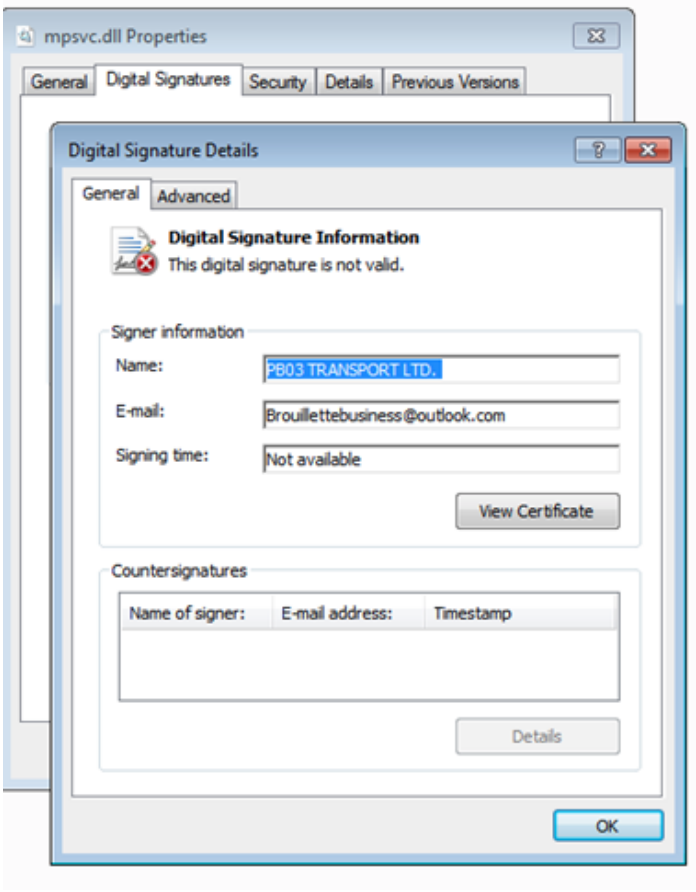


Figure 5: Digitial signature on mpsvc.dll

Upon initial investigation, the DLL is the payload itself - REvil Ransomware. So we thought to step back a little bit and investigate how this DLL got loaded. This pointed us to an ongoing discussion on Reddit. It turns out that this library was side-loaded by a legitimate Microsoft executable (MsMpEng.exe).

MsMpEng.exe is benign and part of the Microsoft Antimalware service. An older version was used by the attackers. As you can see in the screenshot below, it shows the properties of this Microsoft executable and digital signature details.

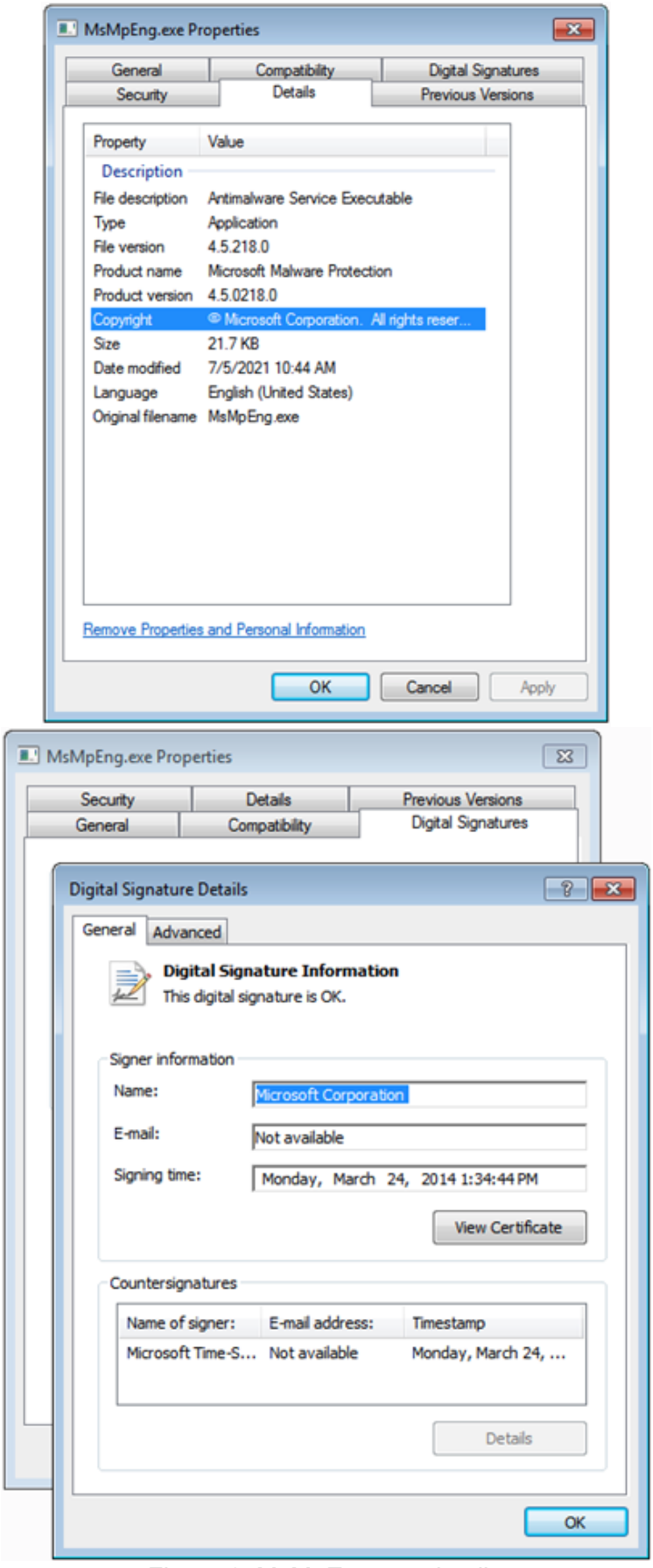


Figure 6: MsMpEng.exe details

When MsMpEng.exe runs, it picks up the attacker's "mpsvc.dll" and loads an exported function from the malicious library called ServiceCrtMain(). This function unpacks and loads the ransomware into the memory and executes it.

Stepping back, MsMpEng.exe and mpsvc.dll were both installed in the infected system by a dropper named Agent.exe.

(Virustotal
detection: https://www.virustotal.com/gui/file/d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e/detection)

"Agent.exe" dropper contains two binaries - **MsMpEng.exe** and **mpsvc.dll** embedded in its body (particularly in the resources section), which when executed, writes (with system privilege) both files into **C:\Windows.** Agent.exe then executes MsMpEng.exe that eventually loaded the malicious "mpsvc.dll" file.

"Agent.exe" was initially dropped as a Base64 encoded file – named as "**Agent.crt"** to the path **C:\kworking**. This ***.crt*** file was deployed through a malicious update by exploiting Kaseya VSA servers, and it eventually sent out this update to the Kaseya VSA Agents running on managed devices. Once the malicious update is deployed to the devices, Kaseya VSA Agents will run a PowerShell command to decode the ***.crt*** file and then execute it.

For the initial vector, Huntress' blog reported that the attacker used an authentication bypass in the web interface of the Kaseya VSA server to gain an authenticated session. They then uploaded the payload and execute a command via SQL injection to deploy the malicious updates

To visualize, this is how post-exploitation execution flows:

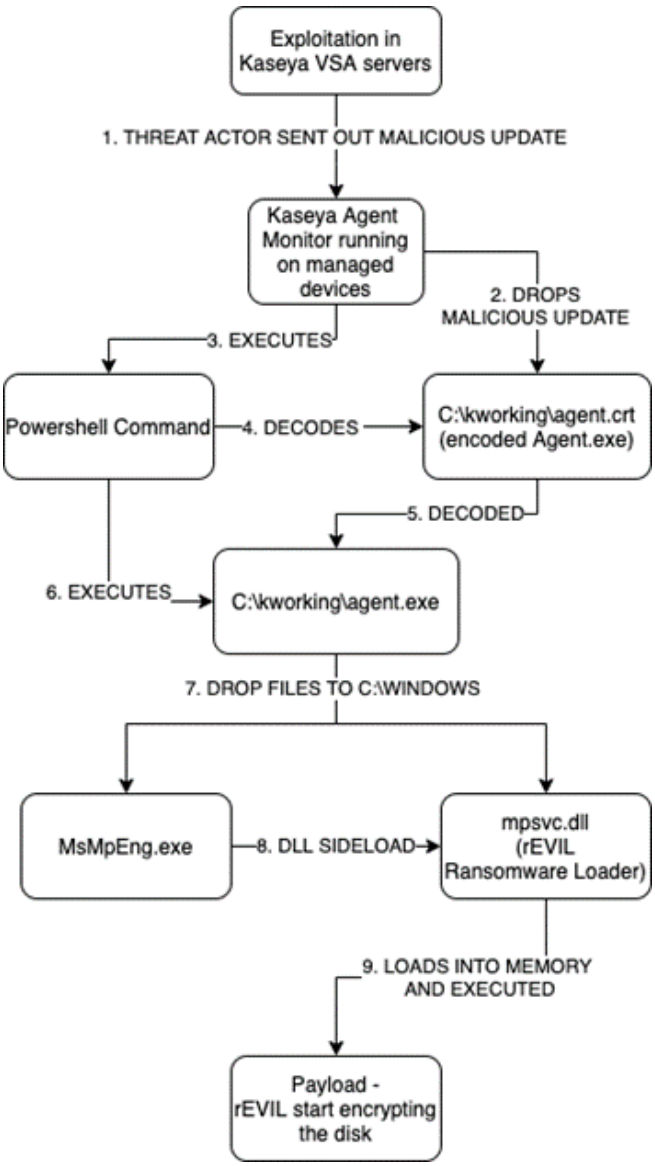


Figure 7: Post-exploitation attack flow

The Ransomware Payload

The payload was found to be REvil ransomware version 2. We have managed to decode the ransomware configuration. A decoded copy can be found here. The configuration file itself is embedded in the ransomware encoded in RC4 with the key ***mXT1QFyEUbrxc4cbP84jbN5wrHeqmFXt***

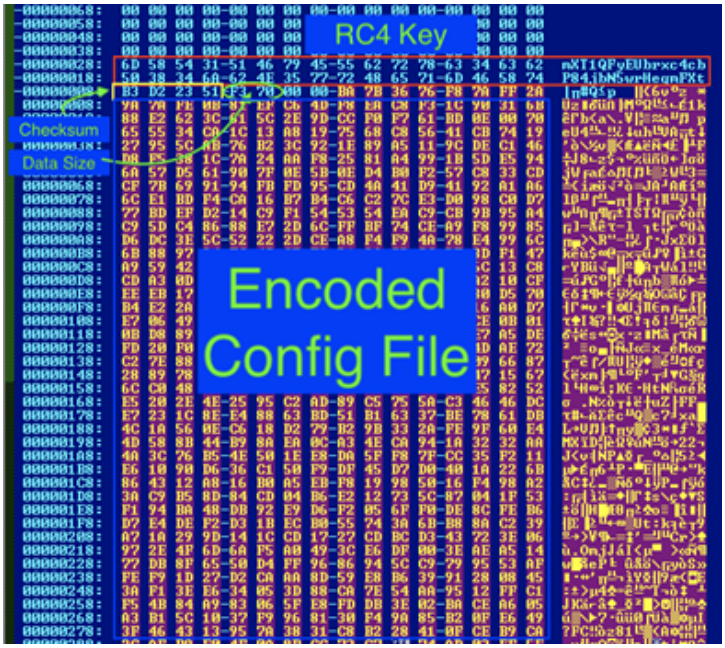


Figure 8: The REvil configuration file embedded and encoded with RC4

Based in the configuration, It avoids encrypting files from this list of directory:

"program files",
"appdata",
"mozilla",
"$windows.~ws",
"application data",
"$windows.~bt",
"google",
"$recycle.bin",
"windows.old",
"programdata",
"system volume information",
"program files (x86)",
"boot",
"tor browser",
"windows",
"intel",
"perflogs",
"msocache"

It also avoids encrypting system files:

"ntldr",
"thumbs.db",
"bootsect.bak",
"autorun.inf",
"ntuser.dat.log",
"boot.ini",
"iconcache.db",

"bootfont.bin",
"ntuser.dat",
"ntuser.ini",
"desktop.ini"

It avoids encrypting any file extension from this list:

"ps1",
"ldf",
"lock",
"theme",
"msi",
"sys",
"wpx",
"cpl",
"adv",
"msc",
"scr",
"bat",
"key",
"ico",
"dll",
"hta",
"deskthemepack",
"nomedia",
"msu",
"rtp",
"msp",
"idx",
"ani",
"386",
"diagcfg",
"bin",
"mod",
"ics",
"com",
"hlp",
"spl",
"nls",
"cab",
"exe",
"diagpkg",
"icl",
"ocx",
"rom",
"prf",
"themepack",

"msstyles",
"lnk",
"icns",
"mpa",
"drv",
"cur",
"diagcab",
"cmd",
"shs"

It terminates running processes if the name is in this list:

"encsvc",
"powerpnt",
"ocssd",
"steam",
"isqlplussvc",
"outlook",
"sql",
"ocomm",
"agntsvc",
"mspub",
"onenote",
"winword",
"thebat",
"excel",
"mydesktopqos",
"ocautoupds",
"thunderbird",
"synctime",
"infopath",
"mydesktopservice",
"firefox",
"oracle",
"sqbcoreservice",
"dbeng50",
"tbirdconfig",
"msaccess",
"visio",
"dbsnmp",
"wordpad",
"xfssvccon"

It also stops the following services if they are running:

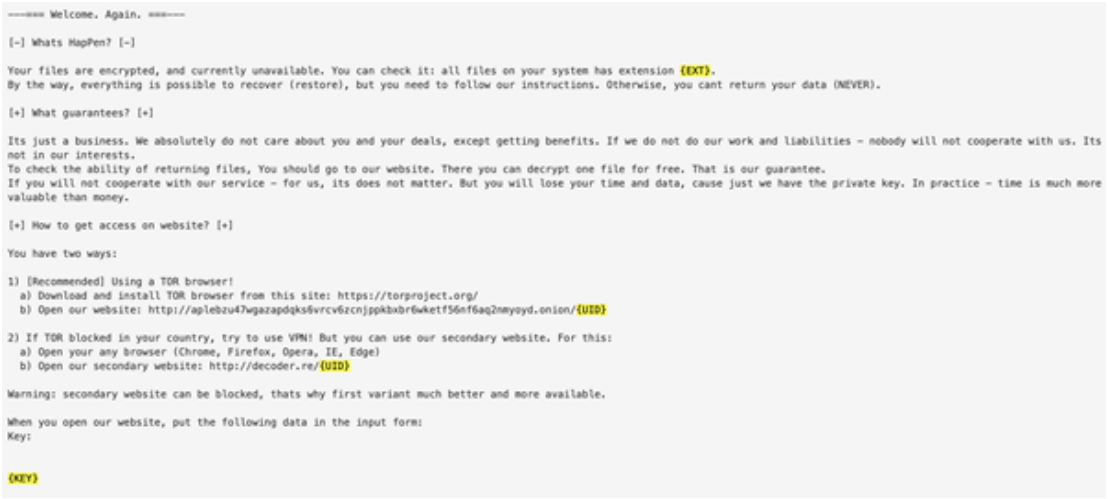
"veeam",
"memtas",
"sql",
"backup",
"vss",
"sophos",
"svc$",
"mepocs"

The configuration also includes the following fields:

Field	Value	Description
pk	9/AgyLvWEviWbvuayR2k0Q140e9LZJ5hwrmto/zCyFM=	attacker's RSA public key – this public key is used to encrypt the session private key used to encrypt the files.
pid	$2a$12$prOX/4eKl8zrpGSC5lnHPecevs5NOckOUW5r3s4JJYDnZZSghvBkq	campaign identifier
dbg	false	used during development stage of this ransomware for debugging purposes
wfld	backup	folder to wipe out
wipe	true	wipe out folders specified in wfld key – in this instance "backup" folder

nname	{EXT}-readme.txt	filename format of the ransomware note dropped in each folder where files are encrypted
exp	false	run privilege escalation exploit
img	QQBsAGwAIABvAGYAIAB5AG8AdQByACAAZgB {TRUNCATED, TOO LONG}	base64 encoded text of the ransomware message set in the desktop background
arn	false	create persistence
rdmcnt	0	max number of ransom notes per drive

The ransom note is also included in the configuration:



```
~~~~~ Welcome. Again. ~~~~~

[-] Whats HapPen? [-]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension {EXT}.
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/{UID}

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/{UID}

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:


{KEY}
```

Figure 9: The ransom letter

Where:
{EXT} - a random extension name of the encrypted file
{UID} - value is taken from the infected system's volume serial number and CPUID. It is used by the attacker to identify the victim

{KEY} - base64 encoded data of the encrypted stat data. Stat data consists of the infected host information including CPU architecture, system default language, host's workgroup name, hostname, and operating system

There is also a list of over 1,200 controller domains that the ransomware supposedly connects to, however, connection to these domains was disabled in the configuration file. You can find the full list in the decoded configuration file here.

Figure 10: list of over 1200 C2 domains

In addition to the configuration, the ransomware also avoids systems that have default languages from what was the USSR region. This includes:

- Russian (Russia)
- Ukrainian (Ukraine)
- Belarusian (Belarus)
- Tajik (Cyrillic, Tajikistan)
- Armenian (Armenia)
- Azerbaijani (Latin, Azerbaijan)
- Georgian (Georgia)
- Kazakh (Kazakhstan)
- Kyrgyz (Kyrgyzstan)
- Turkmen (Turkmenistan)
- Uzbek (Latin, Uzbekistan)
- Tatar (Russia)
- Romanian (Moldova)
- Russian (Moldova)
- Azerbaijani (Cyrillic, Azerbaijan)
- Uzbek (Cyrillic, Uzbekistan)
- Syriac (Syria)

- Arabic (Syria)

The Vultures Circle: Spammers Riding REvil Coattails

Perhaps not surprisingly, spammers have been quick to jump on this issue as a lure in their malicious emails. Today, we encountered spams claiming that Microsoft issued an update which can provide protection against the Kaseya's vulnerability. Below is an example.

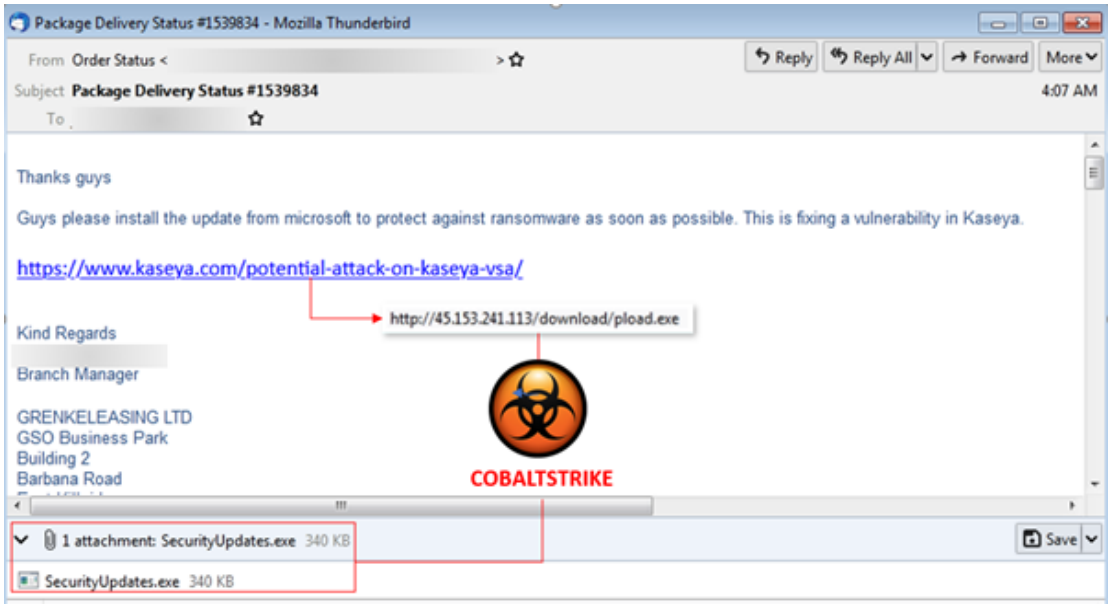


Figure 11: Phishing Email piggybacking on the REvil attack

Both a malicious link and attachment are contained in the spams. A spoofed link to Kaseya's webpage *https://www.kaseya.com/potential-attack-on-kaseya-vsa/*, where the updates about CVE-2021-30116 are posted, is contained in the email body. Clicking this link will lead to an executable file being downloaded from hxxp://45[.]153[.]241[.]113/download/pload[.]exe. The downloaded executable file and the executable attached to the spams are the same file - CobaltStrike malware.

Payload

The executable file loads a Cobalt Strike launcher that unpacks and executes a Cobalt Strike beacon.dll in memory and creates an encrypted tunnel between the infected host and the adversaries. Cobalt Strike is a post-exploitation tool that is used for legitimate purposes by network penetration testers. However, cybercriminals also utilize this tool for malicious purposes to exfiltrate data from compromised hosts, move laterally within the host's network, and also to act as a backdoor.

Extracting the configuration of this Cobalt Strike beacon agent reveals the command and control server, port, the attacker's public key to encrypt exfiltrated data and communications, user-agent, POST URI, among other things, as shown below.

```
{
    "BeaconType": [
        "HTTP"
    ],
    "Port": 80,
    "SleepTime": 60000,
    "MaxGetSize": 1048576,
    "Jitter": 0,
    "MaxDNS": "Not Found",
    "PublicKey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCHFcV/jTWIWbMLGsg/xD-truncated
    "PublicKey_MD5": "0ce7b6482c1f24e42f2935f5026d338d",
    "C2Server": "31.42.177.52,/dpixel",
    "UserAgent": "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0; MANM; MANM)",
    "HttpPostUri": "/submit.php",
    "Malleable_C2_Instructions": [],
    "HttpGet_Metadata": {
        "ConstHeaders": [],
        "ConstParams": [],
        "Metadata": [
            "base64",
            "header \"Cookie\""
        ],
        "SessionId": [],
        "Output": []
    },
    "HttpPost_Metadata": {
        "ConstHeaders": [
            "Content-Type: application/octet-stream"
        ],
        "ConstParams": [],
        "Metadata": [],
        "SessionId": [
            "parameter \"id\""
        ],
        "Output": [
            "print"
        ]
    },
    "SpawnTo": "AAAAAAAAAAAAAAAAAAAAAA==",
    "PipeName": "Not Found",
    "DNS_Idle": "Not Found",
    "DNS_Sleep": "Not Found",
    "SSH_Host": "Not Found",
    "SSH_Port": "Not Found",
    "SSH_Username": "Not Found",
    "SSH_Password_Plaintext": "Not Found",
    "SSH_Password_Pubkey": "Not Found",
    "SSH_Banner": "",
    "HttpGet_Verb": "GET",
    "HttpPost_Verb": "POST",
    "HttpPostChunk": 0,
    "Spawnto_x86": "%windir%\\syswow64\\rundll32.exe",
    "Spawnto_x64": "%windir%\\sysnative\\rundll32.exe",
    "CryptoScheme": 0,
    "Proxy_Config": "Not Found",
    "Proxy_User": "Not Found",
    "Proxy_Password": "Not Found",
    "Proxy_Behavior": "Use IE settings",
    "Watermark": 1359593325,
```

```
    "bStageCleanup": "False",
    "bCFGCaution": "False",
    "KillDate": 0,
    "bProcInject_StartRWX": "True",
    "bProcInject_UseRWX": "True",
    "bProcInject_MinAllocSize": 0,
    "ProcInject_PrependAppend_x86": "Empty",
    "ProcInject_PrependAppend_x64": "Empty",
    "ProcInject_Execute": [
        "CreateThread",
        "SetThreadContext",
        "CreateRemoteThread",
        "RtlCreateUserThread"
    ],
    "ProcInject_AllocationMethod": "VirtualAllocEx",
    "ProcInject_Stub": "DOL1VETkeTUWta/pZ76SVQ==",
    "bUsesCookies": "True",
    "HostHeader": "",
    "smbFrameHeader":
"AAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

    "tcpFrameHeader":
"AAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

    "headersToRemove": "Not Found",
    "DNS_Beaconing": "Not Found",
    "DNS_get_TypeA": "Not Found",
    "DNS_get_TypeAAAA": "Not Found",
    "DNS_get_TypeTXT": "Not Found",
    "DNS_put_metadata": "Not Found",
    "DNS_put_output": "Not Found",
    "DNS_resolver": "Not Found",
    "DNS_strategy": "Not Found",
    "DNS_strategy_rotate_seconds": "Not Found",
    "DNS_strategy_fail_x": "Not Found",
    "DNS_strategy_fail_seconds": "Not Found"
}
```


Adversaries are very opportunistic, often after headliner events like this, we see spam campaigns that ride on a premise of such events. So the usual message applies, keep cautious of email, especially unsolicited ones, and think twice before opening attachments.

Final Words

The notoriety and increasing threat posed by ransomware attacks have been impossible to prevent. We recommend having a good backup solution, and this is crucial and of utmost importance nowadays. Also, implementing a good patch management program could help add an additional layer of security. These previous Trustwave blogs provide more advice on how to be prepared for ransomware attacks.

Trustwave Managed IDS is deploying signatures to detect this campaign. Trustwave MailMarshal has detections in place for the Kaseya-themed scam email. Additionally Trustwave Security Testing Services are deploying checks for Kaseya VSA and customers should be able to scan and detect VSA instances once the check is available. Thanks also to Diana Lopera and Karl Sigler for their help and research in developing this post.

IOCs

IOCs for REvil / Kaseya:

File:

SHA256: d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e
agent.exe

IOCs for Spam Campaign:

File:

SHA1: 7B6621202AC7795E89891B7BD65E769BA6C267C5
SecurityUpdates.exe

Network:

hxxp://45[.]153[.]241[.]113/download/pload[.]exe

hxxp://31[.]42[.]177[.]52/dpixel

hxxp://31[.]42[.]177[.]52/submit.php

References and Further Reading

Trustwave Customer Response:
https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/kaseya-vsa-zero-day-ransomware-attack/

Prior Analysis Trustwave Analysis of REvil:
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/undressing-the-revil/

Analysis of REvil 2.2:
https://intel471.com/blog/changes-in-revil-ransomware-version-2-2

Further Analysis of REvil:
https://blog.amossys.fr/sodinokibi-malware-analysis.html

Kaseya VSA Detection ToolKaseya VSA Detection Tool:
https://kaseya.app.box.com/s/0ysvgss7w48nxh8k1xt7fqhbcjxhas40