


Kaspersky: New hacker-for-hire mercenary group is targeting European law firms

zdnet.com/article/kaspersky-new-hacker-for-hire-mercenary-group-is-targeting-european-law-firms/



Deceptikons

Deceptikons

Long-running espionage group providing mercenary services

Not sophisticated, but using smart approaches and very persistent

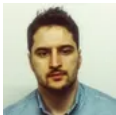
Targeting European law firms deploying PowerShell scripts

In all likelihood, group targets sensitive information of law firms' clientele, negotiations or evidence

GREAT **kaspersky**

[Home Innovation Security](#)

The Deceptikons group is the second major hacker-for-hire mercenary group exposed this year after Dark Basin.



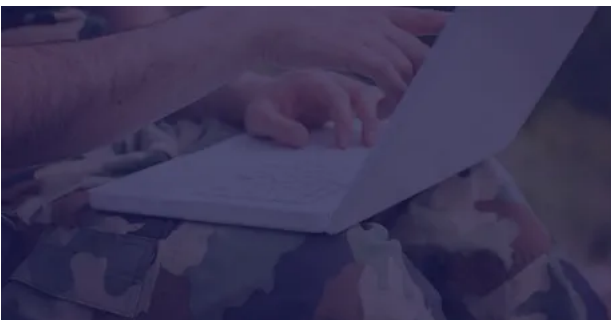
Written by [Catalin Cimpanu, Contributor](#) on July 29, 2020

-
-
-
-
-

deceptikons-apt.png

Image: Screengrab from Kaspersky webinar

Special feature



Cyberwar and the Future of Cybersecurity

Today's security threats have expanded in scope and seriousness. There can now be millions -- or even billions -- of dollars at risk when information security isn't handled properly.

Read now

Russian cyber-security firm Kaspersky said today in a webinar that it discovered a new hacker-for-hire mercenary group that appears to have been active for almost a decade.

The group, which Kaspersky codenamed Deceptikons, has primarily targeted law firms and fintech companies, according to Kaspersky malware analyst Vicente Diaz.

The Kaspersky researcher said the group appears to be focused on stealing business and financial secrets, rather than government-related information.

Diaz said most of the group's targets are located in Europe, and occasionally some Middle East countries like Israel, Jordan, and Egypt.

The Deceptikons' group most recent attacks included a 2019 spear-phishing campaign against a set of European law firms, where the group deployed malicious PowerShell scripts to infect hosts.

Deceptikons doesn't use zero-days

"The group is not technically sophisticated and has not, to our knowledge, deployed zero-day exploits," the Russian security firm said today in a separate written report that accompanied its webinar.

Kaspersky described the group's infrastructure and malware as "clever, rather than technically advanced" and with a focus on gaining persistence on infected hosts.

Most attacks seem to follow a similar patten, starting with a spear-phishing email that carries a malicious modified LNK (shortcut) file.

If the victims download and interact with the file (such as clicking it), the shortcut downloads and runs a PowerShell-based backdoor trojan.

Diaz said Kaspersky would be publishing a more complete technical report on Deceptikons activities in the coming weeks.

Second hacker-for-hire group exposed this year

This is the second major hacker-for-hire mercenary group that came to light this year after Citizen Lab exposed Indian firm BellTroX InfoTech Services as the group behind the Dark Basin APT.

Kaspersky did not link Deceptikons to any real-world entity, however. At least, for the time being.

UPDATE: On August 24, Kaspersky has published an in-depth technical report on this group's operations and hacking tools. The company also changed the group's name from Deceptikons to DeathStalker.

The world's most famous and dangerous APT (state-developed) malware
