Fin7 hacking group targets more than 130 companies after leaders' arrest

By Kaspersky

Published: 2019-05-08 · Archived: 2026-04-05 18:47:24 UTC

Following the arrest in 2018 of a number of suspected leaders of the notorious Fin7/Carbanak cyber-gang, the group was believed to have disbanded. But Kaspersky Lab researchers have detected a number of new attacks by the same groups using GRIFFON malware.

According to the company's experts, Fin7 might have extended the number of groups operating under its umbrella; increased the sophistication of its methods; and even positioned itself as a legitimate security vendor to recruit professional employees and dupe them into helping it steal financial assets.

Fin7 is believed to be behind attacks targeting the U.S. retail, restaurant, and hospitality sectors since mid-2015, working in close collaboration and sharing tools and methods with the infamous Carbanak group. While Carbanak focused primarily on banks, Fin7 targeted mostly businesses, potentially making off with millions of dollars in financial assets, such as payment card credentials or account information on the computers of financial departments. Once the threat actors got what they needed, they wired money to offshore accounts.

According to Kaspersky Lab's new investigation, the group has continued its activity - despite the arrest last year of alleged group leaders - implementing sophisticated spear-phishing campaigns throughout 2018 and distributing malware to each target through specially tailored emails. In different cases, the operators exchanged messages with their intended victims over a period of weeks before finally sending the malicious documents as attachments. Kaspersky Lab estimates that by the end of 2018, more than 130 companies might have been targeted in this way.

The researchers also discovered other criminal teams operating under the Fin7 umbrella. The use of shared infrastructure and the same tactics techniques and procedures (TTPs), shows that Fin7 is likely to be collaborating with the AveMaria botnet and groups known as CobaltGoblin/EmpireMonkey, believed to be behind bank robberies in Europe and Central America.

Kaspersky Lab also found that Fin7 has created a fake company that claims to be a legitimate cybersecurity vendor with offices across Russia. The company website is registered to the server that Fin7 uses as a Command and Control center (C&C). The fake business has been used to recruit unsuspecting freelance vulnerability researchers, program developers and interpreters through legitimate online job sites. It seems that some of the individuals working in these fake companies did not suspect that they were involved in a cybercrime business, with many including the experience of working in the organizations in their CVs.

"Modern cyberthreats can be compared to the mythical creature Hydra of Lerna – you cut off one of its heads and it grows two new ones. Therefore, the best way to protect yourself from such actors is to implement advanced,

multi-layered protection: install all software patches as soon as they are released and do regular security analysis across all networks, systems and devices," said Yury Namestnikov, security researcher at Kaspersky Lab.

To reduce the risk of infection, users are advised to:

- Use security solutions with dedicated functionality aimed at detecting and blocking phishing attempts. Businesses can protect their on-premise email systems with targeted applications inside the Kaspersky Endpoint Security for BusinessKaspersky Security for Microsoft Office 365 helps to protect the cloud-based mail service Exchange Online inside the Microsoft Office 365 suite.
- Introduce security awareness training and teach practical skills. Programs such as Kaspersky Automated Security Awareness Platform will help to reinforce skills and conduct simulated phishing attacks.
- Provide your security team with access to up to date threat intelligence data, to keep pace with the latest tactics and tools used by cybercriminals.

Read the full version of the report on Securelist.com.
