FIN7 sysadmin behind "billions in damage" gets 10 years

By Pieter Arntz

Published: 2021-04-19 · Archived: 2026-04-05 19:44:10 UTC

In 2018 three high-ranking members of a sophisticated international cybercrime group operating out of Eastern Europe were arrested and taken into custody by US authorities. Ukrainian nationals Dmytro Fedorov, Fedir Hladyr, and Andrii Kolpakov, were members of a prolific hacking group widely known as FIN7.

Hladyr is the systems administrator for the FIN7 hacking group, and is considered the mastermind behind the Carbanak campaign, a series of cyberattacks said to stolen as much as $900 million from banks in early part of the last decade. Last week Hladyr was sentenced in the Western District of Washington to 10 years in prison for his high-level role in FIN7.

The Carbanak campaign first made international headlines in 2015 as one of the first malware campaigns that specialized in remote ATM robberies. But FIN7 had already been active for a few years at that point and was involved in a lot more banking and financial malware than just the ATM machines manipulation.

The malware

Since 2013 FIN7 have attempted to attack banks, e-payment systems, and financial institutions using pieces of malware they designed, known as Carbanak and Cobalt. Carbanak is considered a further development of the Anunak malware campaign that targeted financial transfers and ATM networks of financial institutions around the world.

The campaigns all started with spear-phishing targeted at bank employees. When targets executed a malicious attachment the criminals were able to remotely control the victims' infected machine. With access to a bank's internal network, they were able to work their way internally until they gained control of the servers controlling ATMs.

A very detailed analysis of Anunak by Fox-IT and Group-IB can be found here (pdf).

By the following year, the same coders had improved the Anunak malware into a more sophisticated version, known as Carbanak. From then onwards, FIN7 focused its efforts on developing an even more sophisticated wave of attacks by using tailor-made malware based on the Cobalt Strike penetration testing software, but Carbanak remained part of their toolset.

In the US alone, FIN7 successfully breached the computer networks of companies in 47 states and the District of Columbia, stealing more than 15 million customer card records from over 6,500 individual point-of-sale terminals at more than 3,600 separate business locations.

Attribution

Many believe that the Carbanak malware was used by at least two separate entities. FIN7 and the Carbanak Group. This can be very confusing when trying to establish a timeline. Or when trying to solve any "whodunnit" mysteries. Once malware has been released and has proven to be successful you can count on other criminals trying to steal, copy, or rip off the code and techniques. So, if the Carbanak malware was used in a specific attack, it is not always clear which group was behind that attack, although it is clear that FIN7 was one of its users.

The arrest

The leader of the crime gang behind the Carbanak and Cobalt malware attacks was arrested in Alicante, Spain. The arrest was announced by Europol on 26 March 2018. According to Europol, the activities of the gang were believed to have resulted in losses of over EUR 1 billion for the financial industry.

Arresting the leader of that group did not stop the activities of the group though. The FIN7 campaigns appear to have continued, with the Hudson's Bay Company breach using point-of-sale malware in April of 2018 being attributed to the group.

The arrest of Hladyr in August of 2018 at the request of the US Department of Justice, along with two other high-ranking members of the group did not have that effect either. In 2020 a cooperation between FIN7 and the Ryuk operators was suspected when the tools and techniques of FIN7, including the Carbanak Remote Administration Tool (RAT), were used to take over the network of an enterprise.

The conviction

After being extradited to the US in 2019, Hladyr pleaded guilty to one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer hacking, in his role as the systems administrator of the FIN7 group.

According to acting US Attorney Tessa M. Gorman of the Western District of Washington:

> This criminal organization had more than 70 people organized into business units and teams. Some were hackers, others developed the malware installed on computers, and still others crafted the malicious emails that duped victims into infecting their company systems. This defendant worked at the intersection of all these activities and thus bears heavy responsibility for billions in damage caused to companies and individual consumers.

The Department of Justice says that Hladyr joined FIN7 via a front company called Combi Security but soon learned that it was a fake cybersecurity company with a phony website and no legitimate customers. It asserts that Hladyr served as FIN7's systems administrator and played a central role in aggregating stolen payment card information, supervising FIN7's hackers, and maintaining the servers used to attack and control victims' computers. Hladyr also controlled the organization's encrypted channels of communication.

About the author

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.

Source: https://blog.malwarebytes.com/reports/2021/04/fin7-sysadmin-behind-billions-in-damage-gets-10-years/