

The Billion-Dollar Hacking Group Behind a String of Big Breaches

wired.com/story/fin7-carbanak-hacking-group-behind-a-string-of-big-breaches/

Lily Hay Newman

April 4, 2018



This week, Saks Fifth Avenue, Saks Off 5th, and Lord & Taylor department stores—all owned by The Hudson's Bay Company—acknowledged a data breach impacting more than five million credit and debit card numbers. The culprits? The same group that's spent the last few years pulling off data heists from Omni Hotels & Resorts, Trump Hotels, Jason's Deli, Whole Foods, Chipotle: A mysterious group known as Fin7.

Data breaches dog consumers every day, whether they're ordering food from Panera, or tracking their nutrition with an Under Armour app. But if you've particularly had your credit card number stolen from a restaurant, hotel, or retail store in the past few years, you may have experienced Fin7 up close.

While lots of criminal hacking gangs are simply out to make money, researchers regard Fin7 as a particularly professional and disciplined organization. The group—which often appears to be Russian-speaking, but hasn't been tied to a home country—generally works on a normal business schedule, with nights and weekends off. It has developed its own malware tools and attack styles, and seems to have a well-funded research and testing division that helps it evade detection by antivirus scanners and authorities more broadly. In the Saks breach, Fin7 used "point of sale" malware—software secretly installed in the cash register transaction systems customers interact with—to lift the financial data, a signature move.

"They're connected to almost every major point of sale breach," says Dmitry Chorine, cofounder and CTO of Gemini Advisory, a threat intelligence firm that works with financial institutions and that first reported the Saks/Lord & Taylor breach. "From what we've learned over the years the group is operated as a business entity. They definitely have a mastermind, they have managers, they have money launderers, they have software developers, and they have software testers. And let's not forget they have the financial means to stay hidden. They make at least \$50 million every month. Given that they've been in business for many years, they probably have at least a billion dollars on hand."

Name Game

Researchers have carefully tracked Fin7 for years, identifying their tools and watching their techniques evolve and advance. And many of the observers have even gone head-to-head with the group during network attacks, learning the group's ethos by actively sparring with it.

The anonymity of cyberspace makes it difficult to pin down exactly who commits which crimes, though, and whether they're actually all part of the same group or simply using similar tools.

'Given that they've been in business for many years, they probably have at least a billion dollars on hand.'

Dmitry Chorine, Gemini Advisory

As a result, Fin7 is known by many names. *Many*. The "Fin7" name itself is often associated with retail and hospitality credit card number heists, while another group—perhaps another division of the same entity, or a pre-existing gang that Fin7 spun off from—focuses on targeting financial organizations to directly steal and launder money. This bank heist operation has been called Carbanak or Cobalt (after a tool called Cobalt Strike), or some variation; Fin7 is sometimes called by these names as well. The security firm CrowdStrike also has its own versions of the names, Carbon Spider and Cobalt Spider. Carbon Spider targets the retail and hospitality industries; and Cobalt Spider hits financial institutions and ATMs. Adding to the confusion, Gemini Advisory also sometimes calls Fin7 "JokerStash," after the dark web marketplace where the group sells the credit card data it steals.

It's a mess. But while it's virtually impossible to know the exact breakdown, all of these actors evolved from malware campaigns between 2013 and 2015 that used the banking trojans Carberp and Anunak to attack financial institutions. "There's definitely a relationship between what we call Carbon Spider and Cobalt Spider," says Adam Meyers, vice president of intelligence at the security firm CrowdStrike. "There's some overlap in the malware that's used and there are a lot of theories. Did Carbon Spider split from Cobalt? Do they have shared tooling? Did somebody leave the group and bring some of the tools with them?"

Consummate Professionals

Regardless of the name, Fin7's effectiveness stems from a rigorous, professional approach—including devious phishing schemes that trick victims into infecting their own networks—that researchers say is more typical of nation state hacking than criminal skulduggery. The group has also demonstrated a powerful ability to quickly evolve new strategies and adapt tools. Last fall, the security firm Morphisec showed that it only took Fin7 a day to create a fileless malware attack for a newly discovered weakness in Microsoft applications.

'They're not the best-trained, best operations security people on the internet, but they are professional.'

William Peteroy, Icebrg

"The feeling you get working against them on an incident response team is that they aren't going down without a fight," says William Peteroy, CEO of the security firm Icebrg, which has helped clients remediate Fin7 attacks. "They are very committed to getting access to certain targets, they are very committed to maintaining access to those targets, and it's for the overall goal of pulling as much credit card data out of the environment as they can. They're not the best-trained, best operations security people on the internet, but they are professional. They go to work in the morning and their job is to steal credit card numbers."

Based on Icebrg's research and firsthand experience, Peteroy sees the group's focus on evading antivirus scans as one of its biggest assets. Fin7 constantly tests its hacking tools against malware scanners to see if they raise an alarm, and tweaks them if they do to fly under the radar for another day.

"They have a pretty incredible track record of staying one step ahead of antivirus vendors," Peteroy says. "They do constant testing of their toolsets. You would not expect to see a technique like that from a criminal organization. But it's really just like a business maximizing your profitability. You're not trying to develop things that are 10 steps ahead, you're just trying to keep one step ahead."

So far Fin7 has largely succeeded at staying just out of reach, but it works at such a massive scale on so many heists at once that there are bound to be missteps. Just last week, Spanish police working with Europol, the FBI, and a group of other international agencies arrested what they called the "mastermind" behind Carbanak's financial institution hacking, particularly a spree of ATM jackpotting and other money laundering. "The arrest of the key figure in this crime group illustrates that cybercriminals can no longer hide behind perceived international anonymity," Steven Wilson, the head of Europol's European Cybercrime Centre, said of the operation last week.

Though an impressive step, researchers are skeptical that the arrest will really destabilize or neuter such a robust criminal syndicate. "Someone who was using part of the tools was arrested in Spain. He may be at a higher level of the food chain, but it definitely doesn't

necessarily mean the whole group has been dismantled," says Gemini Advisory's Chorine. "Even if you observe the chatter on criminal forums, there's no clear indication of who was arrested."

So as has been the case for years now, Fin7 will likely live to steal another credit card number. Or, more likely, millions of them.

Breach Reads

- The worst hacks of last year included a handful of unprecedented mega-breaches
- Carbanak's bag of tricks includes ATM jackpotting, a clever attack that recently made its way stateside
- If you do find yourself the victim of a big corporate hack, here's how best to protect yourself