August 21, 2017

Advanced malware puts high net worth individuals at greater risk

Hackers, using 'crime as a service' model, put financial institutions, wealthy clients in cross-hairs

FEATURED STORY BY RODIKA TOLLEFSON, THIRDCERTAINTY

Ahead of many other sectors in cybersecurity maturity, the financial industry consistently faces challenges from hackers' ability to circumvent data security. One of the bad guys' latest tactics is to target financial institutions that cannot rely on traditional fraud-detection mechanisms.

According to researchers at F5 Labs, that's the case with the TrickBot banking Trojan, which is heavily targeting financial institutions like private banks and wealth-management firms that cater to high net worth individuals and corporate clients.

***Related video:** How hackers are targeting high net worth individuals*

F5 Labs, part of networking systems supplier F5 Networks, has been monitoring the fast-evolving TrickBot campaigns for the past few months. One of the patterns researchers observed in one of the most recent campaigns is that 50 of the 177 financial institutions targeted were specialty private and public firms like wealth-management services, retirement and investment firms, and banks with commercial accounts.

Sara Boddy, F5 Labs lead

Sara Boddy, F5 Labs lead, says that traditional retail banks that cater to the general public use fraud detection techniques. For example, if a customer's U.S. transaction is immediately followed by an attempted wire transfer originating overseas, that transaction would get flagged.

The rich are different

Wealthy and corporate clients, on the other hand, may have multiple account users who are conducting high-dollar transaction around the world. For those institutions, "it becomes harder to implement those basic fraud-detection controls," Boddy says.

"Attackers probably know that, and that's probably a reason they're targeting these private banking firms," she says.

TrickBot uses malvertising and phishing to get users to install malware on their computers. From there, harvested credentials are used to access accounts for activity such as large wire transfers.

These kinds of campaigns can continue for years. "So they (the bad guys) can get millions and millions of dollars. It's a very lucrative business," Boddy says.

If it works, don't fix it

While the TrickBot campaign has evolved quickly—going through five or six new configurations in just a month and a half—the targets have remained consistent. F5 Labs found that most of the URLs are the same that were once targeted by Dyre, which is believed to be a predecessor to TrickBot.

“If they’ve always been targeting specific users like private banks that are hard to do fraud detection on, maybe they continue to do the same thing because it’s working,” Boddy says.

While these campaigns are targeting primarily European institutions—many of them in the U.K. and Sweden—it’s notable that PayPal is among the targets. Boddy thinks that’s likely because users now keep money in their accounts, and wire transfers are a common PayPal transaction that wouldn’t be flagged.

While researchers can only speculate why the campaign is focused on Europe, the threat is still global.

“This [list] just happens to be part of the TrickBot authors’ attack plan,” Boddy says. “This attack pattern can happen to any bank.”

Malware getting more sophisticated

Ed Cabrera, chief cybersecurity officer with Trend Micro, says the common pattern is the increasing complexity and capability of the banking Trojans. The criminal underground, he says, uses collective intelligence capability to improve the malware and the attack methods.

“The advanced malware that we’re seeing today is highly modular and can be tailored quite easily,” he says.

In a “crime-as-a-service” model of sorts, the malware creators can customize the payload and the outcome based on the needs of their “customers.”

“They understand the criminal consumer, so to speak,” Cabrera says.

In another example of how quickly threats evolve, Trend Micro recently discovered a new attack vector for the GootKit Trojan—it can drop a Trojan when users simply hover over hyperlinked text and images in PowerPoint. The malware is delivered via spam email that masquerades as a purchase order or invoice, which indicates it’s targeting businesses rather than individual consumers.

Mouse-over threat emerges

This is believed to be the first instance of malware that uses the mouse-over method, although GootKit (also known as OTLARD) has been around for five years.

The campaign Trend Micro observed was affecting a cross-section of industries like education, manufacturing and logistics. But traditionally, GootKit had been used for harvesting banking credentials, targeting European financial institutions.

“The mouse-over capability is quite unique because what we tell everyone is not to click on a link or attachment if you feel even remotely suspicious of that email,” Cabrera says.

Hovering over a link or image, on the other hand, is generally considered safe.

“Going deeper and having that [new] capability to be able to infect those intended targets is quite telling,” he says.

Cabrera says that despite its cyber maturity, the sector is still vulnerable because it relies on defense models that are reactionary—focusing on incident response rather than threat response.

“They have to be proactive in developing ways to go after and prevent these types of attacks,” he says. “They need to build hunter teams that can not only find the tactics and strategies that the cyber criminals use within the criminal underground, but also identify their own [organizations’] vulnerabilities.”