Study sheds light on shady world of text message phishing scams

May 28 2024, by Matt Shipman

Credit: CC0 Public Domain

Researchers have collected and analyzed an unprecedented amount of data on SMS phishing attacks, shedding light on both the scope and nature of SMS phishing operations. The work also outlines techniques

that can be used to collect additional data on phishing activities, and identifies avenues that law enforcement officials can use to address phishing operations.

At issue is SMS phishing, which refers to attacks where scammers use text messages to try to trick people into sharing private information —such as credit card numbers or passwords—by impersonating a trusted party, such as a bank or government agency.

"In 2023 the world saw more phishing attacks than ever before, according to data from the Anti-Phishing Working Group," says Alex Nahapetyan, first author of a paper on the study and a Ph.D. student at North Carolina State University.

"These attacks affect online security and privacy for consumers and can be extremely costly, but we have very little data on them," Nahapetyan says. "That's because telecommunications companies are concerned about customer privacy and are reluctant to comb through the private data shared via text messages."

To get around this limitation, the researchers made use of SMS gateways, which are online websites that allow users to obtain disposable phone numbers. The researchers used SMS gateways to obtain a large number of disposable phone numbers. Because SMS phishing is now so widespread, they were able to simply wait for those disposable phone numbers to begin receiving phishing attacks.

Using this technique, the researchers monitored 2,011 phone numbers and identified 67,991 phishing messages over the course of 396 days.

Using text analysis, the researchers determined that those phishing messages could be divided into 35,128 unique campaigns—meaning that they were using virtually identical content. Further analysis found that

those campaigns were associated with 600 distinct SMS phishing operations.

"For example, if we saw multiple campaigns that were directing targets to click on the same URL, those campaigns were part of the same operation," Nahapetyan says. "By the same token, if we saw a single campaign that used multiple URLs, we were able to determine that those URLs were part of the same operation."

Some of the findings were surprising. For example, the researchers found that SMS phishers are using mainstream servers, URL-shortening apps and web infrastructure to support their operations.

"Most people associate cybercrime with some sort of shady infrastructure," Nahapetyan says. "But these phishing scam operations are being run using the same infrastructure as everyone else."

The researchers also found that some phishers are also setting up their own domains, which they are using to host their own URL-shorteners.

"This raises the possibility that the private URL-shortening services provide some additional protection to phishers, or that this is a service being sold to phishers as part of the phishing ecosystem," says Nahapetyan. "That's an area for future research."

The researchers also tested the defenses of telecom services by sending their own (harmless) phishing messages to 10 phone numbers. They did this directly from a privately-owned phone, and again from a bulk messaging service. All of the phishing messages were delivered successfully. However, the bulk messaging service then banned the researcher's account.

The researchers also looked for bulk messaging services that phishers

would be able to use repeatedly—and they found them. The services that enabled phishing attacks were not hiding in shadowy corners of the internet, but advertising openly on public social media platforms, such as LinkedIn.

"Altogether, the findings underscore two things," says Nahapetyan. "First, we already knew that there was an entire email phishing economy, and this work makes clear that this is true for SMS phishing as well. Someone can come in and buy an entire operation ready to go—the code, the URL, the bulk messaging, everything. And if their site gets shut down, or their messaging service gets banned, they don't care—they'll just move on to the next one.

"Second, we found that messages from many phishing operations include what appear to be notes to themselves. For example, a text may end with the words 'route 7' or 'route 9' or whatever. This suggests that phishers are using SMS gateways to test different routes for delivering phishing messages, in order to determine which routes are most likely to let their message through."

In at least four instances, the researchers identified these "test messages"—including the URL the phishers were using—before the phishers had fully deployed their web infrastructure at the URL.

"This tells us that the messages were sent before the phishing attacks were launched in earnest," says Nahapetyan. "That's important because it suggests that, by monitoring SMS gateways, we may be able to identify some phishing URLs before their attacks roll out on a large scale. That would make those phishing campaigns easier to identify and block before any users share private data."

The paper, "On SMS Phishing Tactics and Infrastructure," was presented May 20 at the IEEE Symposium on Security and Privacy, which was

held in San Francisco, Calif.

Corresponding author of the paper is Brad Reaves, an associate professor of computer science at NC State. The paper was co-authored by Sathvik Prasad, a Ph.D. student at NC State; Kevin Childs, a former undergraduate at NC State; Alexandros Kapravelos, an associate professor of computer science at NC State ; and Adam Oest and Yeganeh Ladwig of PayPal.

More information: Aleksandr Nahapetyan et al. On SMS Phishing Tactics and Infrastructure. IEEE Symposium on Security and Privacy October 2023, https://robocall.science/publication/sp24/

Provided by North Carolina State University