Phishing for Finance

Volume 7, Issue 2

EXECUTIVE SUMMARY
Executive Summary

It’s that time again – the launch of another State of the Internet / Security report for 2021. While Akamai has access to some of the largest security data sets in the world, our viewpoint is limited to the traffic that traverses our networks and is seen by our tools.

We worked with threat intelligence company WMC Global for this report, which focuses on the financial services industry. The researchers at WMC Global are experts at understanding SMS phishing (smishing) and the toolkits that criminals devise to make their attacks possible. Our desire is to provide you with both a wide view of the threat landscape and a deep dive into a specific threat.

In 2020, there were 193 billion credential stuffing attacks globally, with 3.4 billion of them in the financial services space, representing a 45% growth over 2019.

Web attacks against the financial services industry represented 12% of the global attacks observed in 2020. Akamai observed 736,071,428 web attacks recorded against financial services in 2020. The number one web attack type targeting financial services was Local File Inclusion (52%), followed by SQL Injection (33%) and Cross-Site Scripting (9%).

The Kr3pto phishing kit, which targets financial institutions and their customers via SMS, has been observed spoofing 11 brands in the United Kingdom, across more than 8,000 domains since May 2020. Akamai and WMC Global have tracked Kr3pto campaigns across more than 80 different hosts (ASNs), including one that housed more than 6,000 Kr3pto domains.

In the report, WMC Global CEO Ian Matthews sets the stage by explaining why SMS phishing is so effective, in his featured guest essay.

“Why is SMS phishing so effective? SMS messaging is ubiquitous in today’s smartphone-saturated communications environment. Each day, mobile users send billions of text messages, opening them quickly and frequently at a reported rate of 98%.

Ian Matthews
WMC Global CEO
Web-based attacks and application attacks remained high in 2020, and show no indication of slowing anytime soon. Akamai observed 6,287,291,470 web attacks globally, with 736,071,428 of them in the financial services sector alone.

DDoS attacks also increased by 15% in 2020 over the previous year’s totals in the financial services sector. Over the past three years (2018–2020), DDoS attacks against the financial services sector grew by 93%, proving that systemic disruption is always an option for criminals, who target services and applications required for daily business.

A consistent and global threat

In this report, we present research related to threat actors and the phishing kits being used to target the financial services industry, or people within it. One relatively new malicious actor poses a serious threat to the financial services industry in the United Kingdom, with the development of dynamic phishing kits that effectively bypass secondary methods of authentication.

The concept of phishing as a service has been around for a few years. Skilled website developers create complex phishing kits, which in some cases are near-flawless replicas of the targeted brand or financial institution. These kits come complete with back-end operational support and functionality, and all the developer needs to do is sell their creations to lesser skilled criminals who will, in turn, unleash them on the public.

Kr3pto gained the attention of WMC Global and Akamai after releasing phishing kits targeting 11 different banks in the United Kingdom. Given the scale and rapid progression of the attacks targeting the banks, both companies were eager to investigate the source.

This phishing kit targets victim usernames and passwords, as well as any secondary authentication method being used, such as security questions and answers, and SMS-based PINs. The workflow used by these kits are seamless and dynamically adapt to the victim’s login experience at their bank.

Kr3pto starts its attack by sending lures to victims via SMS, reporting a locked account or a new payee being set up. Between January 12 and February 12, 2021, WMC Global tracked more than 4,000 campaigns linked to Kr3pto going out across SMS. The reason the lures are sent via SMS is obfuscation. Most enterprise operations, as well as home endpoint security offerings and general email accounts, will prevent malicious emails from hitting the victim’s inbox. These protections aren’t perfect, but they do prevent a majority of the attacks. Therefore, criminals have turned to SMS, and even social media, to deliver their lures.

Dynamic kits like Kr3pto are looking to take advantage of the lack of strong 2FA options, not only in the financial services space, but globally. The process used by Kr3pto to achieve this isn’t new, but the fact it is becoming so widespread means there is a risk of it becoming commonplace in the near future. Financial institutions, as well as other critical consumer brands, need to adopt stronger 2FA/MFA alternatives for protection and mitigation.

This report also takes a look at a corporate phishing kit known as Ex-Robotos. The phishing kits targeting corporate accounts bring particularly high risk, because they expose access that extends beyond what they’re targeting. Credentials compromised by corporate phishing kits instantly expose the account in question, such as office email or document storage.
According to data from the Akamai Intelligent Edge Platform, there were more than 220,000 hits to the API IP address used for Ex-Robotos over a span of 43 days. In fact, traffic to that address hit tens of thousands of targets per day on average between January 31 and February 5, 2021.

While investigating logs related to Ex-Robotos attacks, WMC Global discovered an extensive credential poisoning campaign. Credential poisoning is frequently carried out by online vigilante groups. These groups try to flood a phishing website with fake usernames and passwords in an attempt to dilute the logs with garbage, making it nearly impossible for the threat actor to work through all the data to find real victims.

Phishing kits like Ex-Robotos and Kr3pto are just the tip of the iceberg — hundreds of kits are developed and circulated daily. The attacks are relentless. The phishing economy as a whole has been growing exponentially year over year, as developers leverage the same web technologies and techniques that enable businesses to remain agile and ahead of the curve.

To dive deeper into this research, read the full State of the Internet / Security report.

Phishing for Finance
Visit https://www.akamai.com/soti