Executive Summary:

[State of the Internet] / Security

Volume 5, Issue 4

Financial Services Attack Economy
Overview

The financial services industry has always been a prime target for criminals. The tools used to attack financial organizations are part of an increasingly large criminal ecosystem. For this report, we look at the big picture of attacks against banks, credit unions, trading companies, and other organizations that make up the financial services industry.

SYN-ACK Reflection Attacks

In March 2019, many financial service organizations started seeing a type of attack that is not typically used by criminals: Distributed Denial of Service (DDoS) attacks that leveraged SYN-ACK packets to flood the data centers of their intended targets. We dug a little deeper into two factors that made these particular attacks different from previous SYN-ACK floods: the number of targets being affected and the secondary effects stemming from this traffic. Were banks the target, or did these attacks have a different intent altogether?

Akamai Research

Credential stuffing is a common attack – an automated injection of breached username and password combinations against authentication systems such as login forms. Attackers often utilize All-In-One (AIO) applications to automate credential stuffing at scale, making it relatively easy to set up and conduct a credential stuffing attack.

For this report, Akamai looked into 18 months of credential stuffing data – from November 2017 through April 2019. We observed 57,970,472,311 malicious login attempts. A total of 3,547,533,230 of those attacks were against financial service organizations. Globally, the United States was the source of the most malicious logins against the financial service industry, followed by China, Malaysia, Brazil, and Germany.
Phishing attacks are another important segment of attacks on financial organizations. Between December 2, 2018, and May 4, 2019, Akamai detected 197,524 phishing domains. Of those domains, 66% targeted consumers, while 34% targeted enterprises. In the phishing domains targeting consumers, financial organizations were the top target.

Akamai recorded 4,460,367,847 web attacks across all verticals during the same 18-month period. Just over 9% – 411,409,583 of these attacks – impacted the financial services sector. However, the financial services industry accounted for 14% of all unique targets during this period. Even as the overall volume of web attacks increases, the number of attacks against the financial services industry remains relatively stable.
Most (94%) of the attacks that we saw against the financial services sector during this period came from one of four methods: SQL injection (SQLi), local file inclusion (LFI), cross-site scripting (XSS), or OGNL Java injections. OGNL Java injections account for more than 8 million attempts during this 18-month period. This high volume reminds us that attacks against Apache Struts are still a very popular option for criminals targeting the financial services industry.

DDoS attacks can often serve as a distraction for criminals to conduct credential stuffing attacks or exploit a vulnerability. Akamai observed more than 800 DDoS attacks against the financial industry over the 18-month data set. More than 40% of all unique DDoS targets were in the financial services industry. SYN floods, RESET floods, TFTP floods, and TCP fragment floods were the most commonly launched DDoS attack types against the financial services space during this period.

Since criminals tend to target authentication mechanisms, this often means they are looking at an API or a login application. Financial institutions use the Open Financial Exchange (OFX) protocol to handle data between themselves or to deliver data to a third-party application. Even though the standard has been changed to version 2.2, many organizations are still processing data on older and less secure versions.

For an in-depth look at these stories, please download the full report:

State of the Internet / Security / Financial Services Attack Economy