ThreatMetrix®
The Digital Identity Company™

The Cybercrime Crisis: Evolving Attack Vectors in the Financial Services Sector

By Vanita Pandey

An explosion in stolen identity data helped fuel more than 130 million cyberattacks in the first three months of the year, according to the Q1 2017 Cybercrime Report from ThreatMetrix. That's a 35-percent increase over the same period one year ago.

The report, based on actual attacks detected by the ThreatMetrix Digital Identity Network, provides a reliable barometer of quarterly trends. It's also stoking concerns over mounting global losses from cybercrime, which already exceed $3 trillion—and could double by 2021.

No industry is immune to the threat. But according to the first quarter report, the financial services sector remains an especially lucrative target.

The Move to Mobile

Consumer demand for anytime, everywhere services has resulted in a 250-percent increase in financial services transactions made on mobile devices year over year. During the first quarter of 2017, a full 52 percent of all financial services transactions within the ThreatMetrix network came through mobile devices. In fact, bank customers are now logging-in almost twice as often on mobile devices as they are through the desktop.

Meanwhile, emerging FinTechs continue to disrupt the industry, with an emphasis on convenience and frictionless user experiences. The resulting arms race has incumbent institutions and startup challengers transforming every facet of the business through digital innovation.

The problem is that cybercriminals are exploiting the gaps in those same technologies.

Attacks Surge and Evolve

Despite mobile transactions being generally considered safer than those made via desktop, the year-on-year growth in transactions rejected for suspected fraud hit 40 percent in Q1. And, across all vectors, cyberattacks have now outpaced the growth of legitimate transaction volume by 50 percent.

At the heart of these trends are the more than 6 billion personal identities that have been compromised through data breaches in recent years. In fact, the ThreatMetrix Network saw more than 80 million financial services attacks using stolen or fake credentials in 2016.

The use of personal identity data is becoming more automated, more global, and more coordinated. Instead of just single-point attacks, cybercriminals now combine pitch-perfect social engineering ploys, malware, and the cover of remote access so attacks can have maximum impact. It’s becoming a very complex attack environment.

Adding to the complexity is a dramatic rise in bot attacks, especially against FinTechs and their account application processes, which see four times the cross-industry average. Bot attacks have evolved from their early days as high-velocity spamming, and are now adopting a ‘low and slow’ attack speed to slip under the radar and appear more like legitimate customer traffic.

Three Emergent Threat Tactics

Beyond the evolution of known threats, a handful of key cybercrime tactics are gaining new momentum. Here’s a look at three of those tactics, and approaches that have shown early success in combating them:

The Rise of Loan Stacking

E-lenders are discovering that they are susceptible to loan stacking schemes in which thieves exploit time lags associated with reporting loan agreements to credit bureaus. By leveraging stolen identity data, cybercriminals take out multiple loans in quick succession, before the increased debt load is reflected in credit reports.

Within the ThreatMetrix Network, thwarted attacks have included scammers who used the same device to apply for loans at four different companies within a single hour. Another involved a single fraudster who sent fraudulent loan applications from separate devices in an attempt to avoid detection.

Without the digital identity intelligence on the associations between users and their devices, locations, behaviors and other dynamic data elements, such fraud is virtually impossible to detect.

The Menace of Money Mule

In fraud attacks, stolen funds are usually transferred to offshore accounts. An essential partner in the theft is the money mule — a person who sets up these accounts and then receives, transfers or withdraws stolen funds on behalf of cybercriminals.

In many cases, mules are local crooks. In others, they’re unwitting victims who get hacked or conned. Still others are innocent job applicants who think they’ve been hired to “make thousands working from home.”

By leveraging digital identity intelligence from ThreatMetrix, banks have had success identifying, flagging and blocking mule accounts.

RAT Infestations

> This past quarter saw a sharp rise in Remote Access Attacks (or RATs) that combine phishing and other social engineering tactics along with Malware to target commercial banks.
>
> These tools are very hard to detect, and are controlled remotely by cybercriminals who gain access to a customer bank account once a victim unwittingly logs in. Accounts are then drained — and by all accounts, it appears as if the customer is behind the transaction.
>
> Minus the kind of shared intelligence within the ThreatMetrix Network, many institutions report they’re unable to spot the subtle, tell-tale signs that signal a RAT attack so they can shut it down.

As attacks grow more sophisticated and complex, financial institutions must shore up their defenses against these attacks. After the first quarter financial institutions just faced, that’s an aspiration the entire industry can appreciate.

To learn more about evolving cybercrime attack vectors, download the ThreatMetrix Q1 2017 Cybercrime Report.