ThreatMark

State of Phishing 2020

For Banks & Financial Industry

Findings by ThreatMark SOC Team

ThreatMark's Security Operations Center (SOC) complements our technological solution with human threat detection, analysis and mitigation.

From malware, web injects, man-in-the-middle, to phishing or vishing attacks – the SOC team helps our clients identify and mitigate threats 24/7.

Our clients, retail banks around the world, are under ever-increasing phishing attacks which seem to be increasing by the COVID19 pandemic and highly scalable technologies.

In 2020 our SOC team reviewed 4680 suspicious domains. Out of these, 463 were phishing sites that were successfully mitigated.

Interestingly, we saw an incremental increase in phishing sites until June 2020. After a short pause and a decline during the summer — the numbers of detected suspicious and phishing sites grew by the end of the year.

Key findings

- According to Verizon's 2020 Data Breach Investigations Report (DBIR), 22% of breaches (out of 3 905 in total) involved phishing
- Phishing has been and still is a fruitful method for attackers who use email, 96% of the time
- 90% of organizations experienced targeted phishing attacks, while 88% of organizations worldwide faced spear-phishing attacks
- In comparison to 2019, we are seeing wide, scalable and complex phishing campaigns targeting banks in Europe

INTERESTING TRENDS DISCOVERED in 2020

- The number of SSL enabled phishing websites has increased. APWG's Phishing Activity Trends Report notes that 80% of phishing sites have SSL encryption enabled.
- URL Shortening services (like bit.ly) were very popular for a brief time.
- Phishing site redirects are still popular. Usually, phishing links in emails, which look less suspicious are just redirects to real phishing sites.
- We noted Punycode being used occasionally.
- We see a lot of phishing kits reuse. This points to the proliferation of phishing and the scalability of attacks. Arguably fraudsters are not too willing, or not knowledgeable, to build new phishing kits.
- In our client's industry geofencing is common. This allows phishing to be accessible, and detectable, from only specific countries or regions.
- Similarly, our SOC team encountered IP blocking on almost every phishing site. Fraudsters are keen to block known security company IPs, bots and IP ranges.
- Occasionally, phishing sites are shown only once per victim (based on IP); after that, the victims are shown no content or are redirected to a search engine.
- Almost all the time the phishing flow contains an OTP/SMS token capture page which suggests automated payment action/app registration or other automation on the attacker's end.
- And strangely, we even saw some domains being used for multiple banks in multiple regions, some even weeks after they were compromised.

ThreatMark

State of Phishing 2020

For Banks & Financial Industry

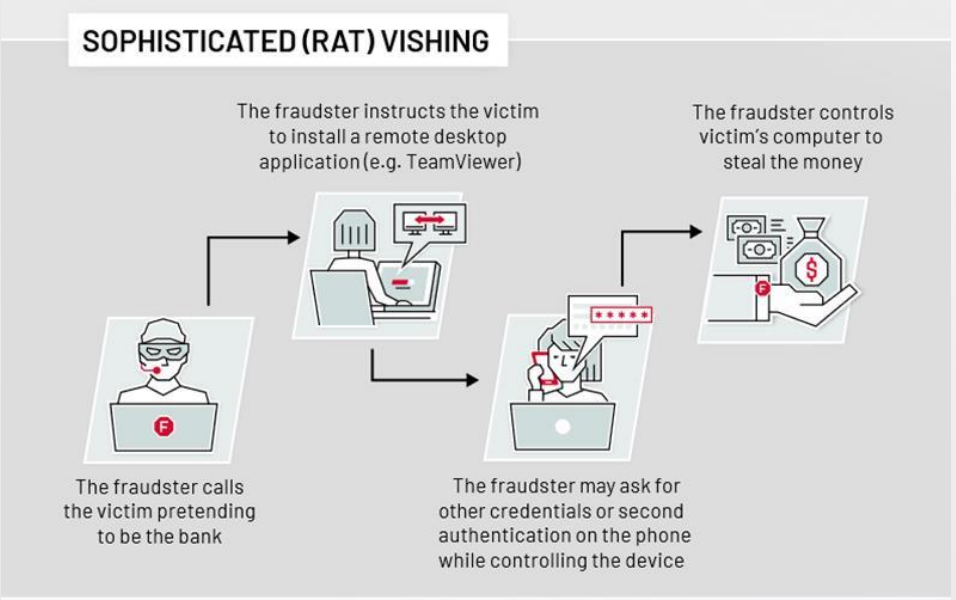
Findings by ThreatMark SOC Team

It is worth noting, that beyond technical prowess, fraudsters are demonstrating skillfulness when it comes to social engineering.

As we came to realize, the goals of fraudsters go beyond acquiring credentials, but to acquire as much information as possible in order to persuade the victim do what they want in elaborate ways.

Such objectives of the frauds are seen in all RAT attacks and authorized push payments scams. These scams can get intricate. We've investigated several cases where the fraudster called the victim, early in the morning; with background noises from the bank and perfect accent, to scare the victim in sending the money to the fraudster.

Such attacks are trending these days and getting more elaborate from case to case. In essence, this is how a sophisticated RAT attack is implemented:



On the mitigation side, we've dealt with many registrars/hosting providers each with various reporting methods and resolution speeds.

While most of the hosting and service providers are diligent and react fast; we had a few encounters which took a lot of persuasions to remove malicious content from their services. These cases took a lot of effort (communication, escalation) to get resolved.

All findings from our team, and other companies, signify that phishing is here to stay and will remain a very prevalent attack vector. Especially, in the financial services industries.

OTHER IMPORTANT & RELEVANT RESOURCES

- On Phishing attacks and how to prevent them – article
- On Vishing attacks and how to prevent them – article infographic
- New phishing campaigns exploiting Google Apps, targeting banks in Europe – article
- Banking Malware & Attack Vectors Outlook For 2020 – Part 1 Part 2