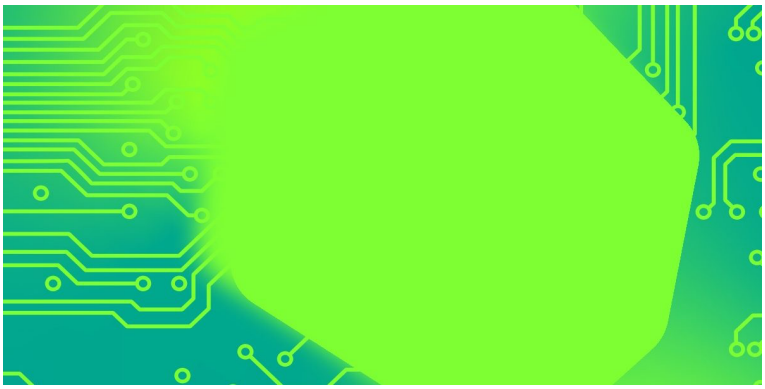
Cyberthreats to financial institutions 2020: Overview and predictions

KASPERSKY SECURITY BULLETIN 03 DEC 2019

12 minute read



// AUTHORS

 YURY NAMESTNIKOV

 DMITRY BESTUZHEV

- Kaspersky Security Bulletin 2019. Advanced threat predictions for 2020
- Cybersecurity of connected healthcare 2020: Overview and predictions
- 5G technology predictions 2020
- Corporate security prediction 2020

Key events 2019

- Large-scale anti-fraud bypass: Genesis digital fingerprints market uncovered
- Multi-factor authentication (MFA) and biometric challenges

- Targeted attack groups specializing in financial institutions: splitting and globalization
- ATM malware becomes more targeted
- Card info theft and reuse: magecarting everywhere and battle of POS malware families in Latin America

Large-scale anti-fraud bypass: Genesis digital fingerprints market uncovered

During the last few years, cybercriminals have invested a lot in methods to bypass anti-fraud systems, because now it's not enough just to steal the login, password and PII – they now need a digital fingerprint to bypass anti-fraud systems in order to extract money from the bank. During 2019, we identified a huge underground market called Genesis, which sells digital fingerprints of online banking users from around the globe.

From an anti-fraud system perspective, the user's digital identity is a digital fingerprint – a combination of system attributes that are unique to each device, and the personal behavioral attributes of the user. It includes the IP address (external and local), screen information (screen resolution, window size), firmware version, operating system version, browser plugins installed, time zone, device ID, battery information, fonts, etc. The device may have over 100 attributes used for browsing. The second part of a digital identity is the behavioral analysis.

As criminals are continuously looking for ways to defeat anti-fraud safeguards, they try to substitute the system's real fingerprint with a fake one, or with existing ones stolen from someone else's PC.

The Genesis Store is an online invitation-only private cybercriminal market for stolen digital fingerprints. At the time of our research, it offered more than 60 thousand stolen bot profiles. The profiles include browser fingerprints, website user logins and passwords, cookies, credit card information, etc. By uploading this fingerprint

to the Tenebris Linken Sphere browser, criminals are able to masquerade as legitimate online banking users from any region, country, state, city, etc.

This type of attack shows that criminals have in-depth knowledge of how internal banking systems work and it's a real challenge to protect against such attacks. The best option is to always use multi-factor authentication.

Multi-factor authentication (MFA) and biometric challenges

MFA is a challenge for cybercriminals. When MFA is used, they have to come up with techniques to bypass it. The most common methods used during the last year were:

- Exploiting vulnerabilities and flaws in the configuration of the system. For example, criminals were able to find and exploit several flaws in remote banking systems to bypass OTPs (one time passcodes);
- Using social engineering, a common method among Russian-speaking cybercriminals and in APAC region;
- SIM swapping, which is especially popular in regions like Latin America and Africa. In fact, despite SMS no longer being considered a secure 2FA, low operational costs mean it's the most popular method used by providers.

In theory, biometrics should solve a lot of problems associated with two-factor authentication, but practice has shown that it may not be so simple. Over the past year, several cases have been identified that indicate biometrics technology is still far from perfect.

Firstly, there are quite a few implementation problems. For example, Google Pixel 4 does not check if your eyes are open during the unlocking process using facial characteristics. Another example is the possibility of bypassing fingerprint authentication using the sensor under the screen on smartphones made by various manufacturers, including popular brands such as Samsung.

There is another trick that has been exploited in Latin America: a visual capturing attack. Cybercriminals installed rogue CCTV cameras and used them to record the PINs people used to unlock their phones. Such a simple technique is still very effective for both types of victims: those who use biometrics and those who prefer PINs to fingerprints or facial recognition. This is because, when a device is dusty or greasy (and the same applies to a user's fingers), the best way to unlock a phone is to use a PIN.

Secondly, there were several high-profile leaks of biometric databases. The most notorious was the leak of the Biostar 2 database that included the biometric data of over 1 million people. The company stored unencrypted data, including names, passwords, home addresses, email addresses and, most importantly, unencrypted biometric data that included fingerprints and facial recognition patterns as well as the actual photos of faces. A similar leak occurred at a US Customs and Border Patrol contractor, where biometric information of over 100,000 people was leaked.

There have already been several proof-of-concept attacks that use biometric data to bypass security controls, but those attacks could still be countered with system updates. With these latest leaks, on the other hand, this won't work because your biometric data cannot be changed – it stays with you forever.

The cases mentioned above, combined with the high-quality research carried out by cybercriminals to obtain a complete digital fingerprint of a user in order to bypass anti-fraud systems, suggest that relying solely on biometric data will not solve the current problems. Today's implementations need a lot of effort and more research to make them truly secure.

Targeted attack groups specializing in financial institutions: splitting and globalization

FROM THE SAME AUTHORS

Cyberthreats to financial organizations in 2022

Targeted ransomware: it's not just about encrypting your data!

AZORult spreads as a fake ProtonVPN installer

Cybersecurity of connected healthcare 2020: Overview and predictions

FIN7.5: the infamous cybercrime rig "FIN7" continues its activities

FIN7

In 2018, Europol and the US Department of Justice announced the arrest of the leader of the FIN7 and Carbanak/CobaltGoblin cybercrime groups. Some believed that the arrest would have an impact on the group's operations, but this does not seem to have been the case. In fact, the number of groups operating under the umbrella of CobaltGoblin and FIN7 has grown: there are several interconnected groups using very similar toolkits and the same infrastructure to conduct their cyberattacks.

The first operating under this umbrella is the now-notorious FIN7 that specializes in attacking various companies to get access to financial data or their PoS infrastructure. It relies on the Griffon JScript backdoor and Cobalt/Meterpreter and, in more recent attacks, PowerShell Empire.

The second is CobaltGoblin/Carbanak/EmpireMonkey. It uses the same toolkit, techniques and a similar infrastructure, but targets only financial institutions and associated software and service providers.

The final group is the newly discovered CopyPaste group, which has targeted financial entities and companies in one African country – leading us to believe that this group is associated with cyber-mercenaries or a training center. The links between CopyPaste and FIN7 are still very weak. It's possible that the operators of this cluster of activity were influenced by open-source publications and don't actually have any ties to FIN7.

All of these groups benefit greatly from unpatched systems in corporate environments and continue to use effective spear-phishing campaigns in conjunction with well-known Microsoft Office exploits generated by their exploitation framework. So far, the groups have not used any zero-day exploits. FIN7/Cobalt phishing documents may seem basic, but when combined with their extensive social engineering and focused targeting, they have proved to be quite successful.

In the middle of 2019, FIN7 fell silent, but returned at the end of the year with new attacks and new tools. We suspect that the silent period is connected to their infrastructure shutdown that occurred after closing a bulletproof hosting company in Eastern Europe.

In contrast to FIN7, the activity of the Cobalt Goblin Group was stable throughout the year, which once again proves that these groups are connected, but operate on their own: their toolsets and TTPs are very similar, but operate independently; and only occasionally can we spot overlaps in infrastructure. At the same time, the intensity of attacks is slightly lower than in 2018. Cobalt Goblin's tactics have remained the same: they use documents with exploits that first load a small downloader and then a Cobalt beacon. The main targets also remain the same: small banks in a variety of countries. Perhaps we have detected a lower number of attacks due to diversification, because some indicators suggest the group could also be engaging in JS sniffing (MageCarting) in order to obtain data about payment cards directly from websites.

JS sniffing was extremely popular throughout the year and we found thousands of e-commerce websites infected with these scripts. The injected scripts act in different ways and the infrastructure of the attackers is very different, which suggests that this type of fraud is used by at least a dozen cybercrime groups.

The Silence group actively expanded its operations into different countries throughout the year. We detected attacks in regions where we have never seen them before. For example, we recorded attacks in Southeast Asia and Latin America. This indicates that they have either expanded their operations themselves or started cooperating with other regionally installed cybercrime groups. However, when we look at the development of their main backdoor, we see that their technologies have barely changed over the last two years.

ATM malware becomes more targeted

When it came to ATM malware, we discovered a number of

completely new families in 2019. The most notable were ATMJadi and ATMDtrack.

ATMJadi is an interesting one because it doesn't use the standard XFS, JXFS or CSC libraries. Instead, it uses the victim bank's ATM software Java proprietary classes: meaning the malware will only work on a small subset of ATMs. It makes this malware very targeted (towards one specific bank).

This is reminiscent of the FASTcach case from 2018, when criminals targeted servers running AIX OS. With a decrease in the number of general-purpose cashout tools, we can say that ATM malware is becoming rarer and more targeted.

Another interesting piece of malware is ATMDtrack, which was first detected in financial institutions in India and is programmed to cash out ATMs. Using the Kaspersky Targeted Attack Attribution Engine (KTAE), we were able to attribute these attacks to the Lazarus group, which supports our prediction from 2018 that there will be "**more nation-state sponsored attacks against financial organizations**". Moreover, similar spyware has been found in research centers, with Lazarus APT group using almost identical tools to steal research results from scientific institutes.

Card info theft and reuse

During the year we saw a lot of malware targeting end users and businesses looking for credit card data. In Brazil, in particular, we saw a couple of malware families fighting it out between themselves to maintain control of infected devices. HydraPOS and ShieldPOS were very active during the year, with new versions that included a lot of new targets; Prilex, meanwhile, reduced its activities in the second half of the year.

ShieldPOS has been active since at least 2017 and, after being malware only, it has finally evolved into a MaaS (malware-as-a-service). This fact shows there's great interest from Latin American cybercriminals in running

their own "business" to steal credit cards. HydraPOS has been mostly focused on stealing money from POS systems in restaurants, parking slot machines and different retail stores.

Compared to ShieldPOS, HydraPOS is an older campaign from an actor we named Maggler, which has been in the credit card business since at least 2016. The main difference is that, unlike ShieldPOS, it doesn't work as MaaS. In both cases, we suspect that the initial infection vector is a carefully prepared social engineering campaign involving telephone calls to the victims.

Analysis of forecasts for 2019

Before giving our forecasts for 2020, let's see how accurate our forecasts for 2019 turned out to be:

The emergence of new groups due to the fragmentation of Cobalt/Carbanak and FIN7: new groups and new geography.

- **Yes**, we saw CobaltGoblin activity, FIN7 activity, CopyPaste activity and the intersection of IoCs and the Silence group.

The first attacks through the theft and use of biometric data.

- **Yes**, hacking of various biometric data databases regularly appeared throughout the year. We also revealed a digital fingerprint market where criminals can buy digital fingerprints, which includes, among other things, behavioral data (component of biometrics).

The emergence of new local groups attacking financial institutions in the Indo-Pakistan region, Southeast Asia and Central Europe.

- **No.** It turned out that well-known groups such as Lazarus, Silence and CobaltGoblin took their place and very actively attacked financial institutions in these

regions.

Continuation of supply-chain attacks: attacks on small companies that provide their services to financial institutions around the world.

- **Yes.**

Traditional cybercrime will focus on the easiest targets and bypass anti-fraud solutions: replacement of POS attacks with attacks on systems accepting online payments (Magecarting/JS skimming).

- **Yes,** the number of groups that started carrying out attacks on online payment systems grew constantly over the year. We detected thousands of websites that were affected by JS skimming.

The cybersecurity systems of financial institutions will be bypassed using physical devices connected to the internal network.

- **Yes**, and not only in financial institutions but even the aerospace industry, namely NASA, has suffered from this type of attack.

Attacks on mobile banking for business users.

- **No.**

Advanced social engineering campaigns targeting operators, secretaries and other internal employees in charge of wire transfers.

- **Yes,** BEC (business email compromise) attacks have been on the rise worldwide. We have seen major attacks in Japan, while there have also been campaigns in South America, particularly in Ecuador.
- Additionally, advanced social attacks have been actively used in Brazil to make POS operators go to a malicious website to download specially crafted remote control modules and run them, for example, in HydraPOS attacks.

Forecast 2020

Attacks against Libra and TON/Gram

The successful launch of cryptocurrencies such as Libra and Gram might lead to the worldwide spread of this type of asset, which naturally will attract the attention of criminals. Given the serious surge in cybercriminal activity during the rapid growth of Bitcoin and altcoins in 2018, we predict that a similar situation will most likely unfold around Gram and Libra. Large players in this market should be especially careful, as there are a number of APT groups, such as WildNeutron and Lazarus, whose interests include crypto assets. They are very likely to exploit these developments.

Reselling bank access

During 2019, we witnessed cases where groups who specialize in targeted attacks on financial institutions appeared in the victims' networks after intrusions by other groups that specialize in selling rdp/vnc access, such as FXMSP and TA505. These facts are also confirmed by underground forums and chat monitoring.

In 2020, we expect an increase in the activity of groups specializing in the sale of network access in the African and Asian regions, as well as in Eastern Europe. Their prime targets are small banks, as well as financial organizations recently bought by big players who are rebuilding their cybersecurity system in accordance with the standards of their parent companies.

Ransomware attacks against banks

This forecast logically follows from the previous one. As mentioned above, small financial institutions often become the victims of opportunistic cybercriminals. If these criminals cannot resell access, or even if it becomes less likely that they will be able to withdraw money, then the most logical monetization of such access is

IN THE SAME CATEGORY

ICS and OT threat predictions for 2024

Privacy predictions for 2024

Dark web threats and dark market predictions for 2024

Story of the year: the impact of AI on cybersecurity

Kaspersky Security Bulletin 2023. Statistics

ransomware. Banks are among those organizations that are more likely to pay a ransom than accept the loss of data, so we expect the number of such targeted ransomware attacks to continue to rise in 2020.

Another ransomware attack vector against small and medium financial institutions will be a "pay-per-install" scheme. Traditional botnets will eventually turn into increasingly popular delivery mechanisms against those financial institutions.

2020: the return of custom tooling

Measures taken by antivirus products to effectively detect open source tools used for pen testing purposes, and the adoption of the latest cyberdefense technologies, will push cybercrime actors to return to custom tooling in 2020 and also invest in new Trojans and exploits.

Global expansion of mobile banking Trojans: result of leaked source

Our research and monitoring of underground forums suggests that the source code of some popular mobile banking Trojans was leaked into the public domain. Given the popularity of such Trojans, we expect a repeat of the situation when the source code of ZeuS and SpyEye Trojans were leaked: the number of attempts to attack users will increase at times, and the geography of attacks will expand to almost every country in the world.

Investment apps on the rise: new target for criminals

Mobile investment apps are becoming more popular among users around the globe. This trend won't go unnoticed by cybercriminals in 2020. Given the popularity of some fintech companies and exchanges (for both real and virtual money), cybercriminals will realize that not all of them are prepared to deal with massive cyberattacks, as some apps still lack basic protection for customer accounts, and do not offer two-factor authentication or

certificate pinning to protect app communication. Several governments are deregulating this area and new players are appearing every day, becoming popular very quickly. In fact, we have already seen attempts by cybercriminals to substitute the interfaces of these apps with their own malicious versions.

Magecarting 3.0: even more attacker groups and cloud apps to become prime targets

Over the past couple of years, JS skimming has gained immense popularity among attackers. Unfortunately, cybercriminals now have a huge attack surface that consists of vulnerable e-commerce websites and extremely cheap JS skimmer tools available for sale on various forums, starting at $200. At the moment we are able to distinguish at least 10 different actors involved in these types of attacks and we believe that their number will continue to grow during the next year. The most dangerous attacks will be on companies that provide services such as e-commerce as a service, which will lead to the compromise of thousands of companies.

Political instability leading to the spread of cybercrime in specific regions

Some countries are experiencing political and social upheaval, resulting in masses of people seeking refugee status in other countries. These waves of immigration include all sorts of people, including cybercriminals. This phenomenon will result in the spread of geographically localized attacks in countries that have not previously been affected by them.