A look at the ATM/PoS malware landscape from 2017-2019

securelist.com/atm-pos-malware-landscape-2017-2019/96750/

Authors

Expert Kaspersky

From remote administration and jackpotting, to malware sold on the Darknet, attacks against ATMs have a long and storied history. And, much like other areas of cybercrime, attackers only refine and grow their skillset for infecting ATM systems from year-to-year. So what does the ATM landscape look like as of 2020? Let's take a look.

The world of ATM/PoS malware

ATM attacks aren't new, and that's not surprising. After all, what is one of the primary motives driving cyber criminals? Money. And ATMs are cash hubs—one successful attack can net you hundreds of thousands of dollars. In the past, even high-profile threat actors have made ATMs their prime target.

However, attacking ATMs is a bit different from traditional financial-related threats, like phishing emails or spoofed websites. That's because ATMs operate in a unique space in the tech world: they're still connected to the corporate networks but at the same time must be accessible to anyone that passes by. The resulting technical differences means the attack methods differ from those used for traditional endpoints.

ATMs also share several common characteristics that make them particularly vulnerable to attacks:

- Traditional software that is part of the warranty offered by the vendors → If major changes occur that are not approved by the ATM vendor, including installing AV software, then sometimes this warranty is lost.
- Regular use of outdated operating systems and the apps its runs on
- Locations chosen in a way that provide access to as many customers as possible, including those in remote regions → These isolated locations often lack any reasonable physical security

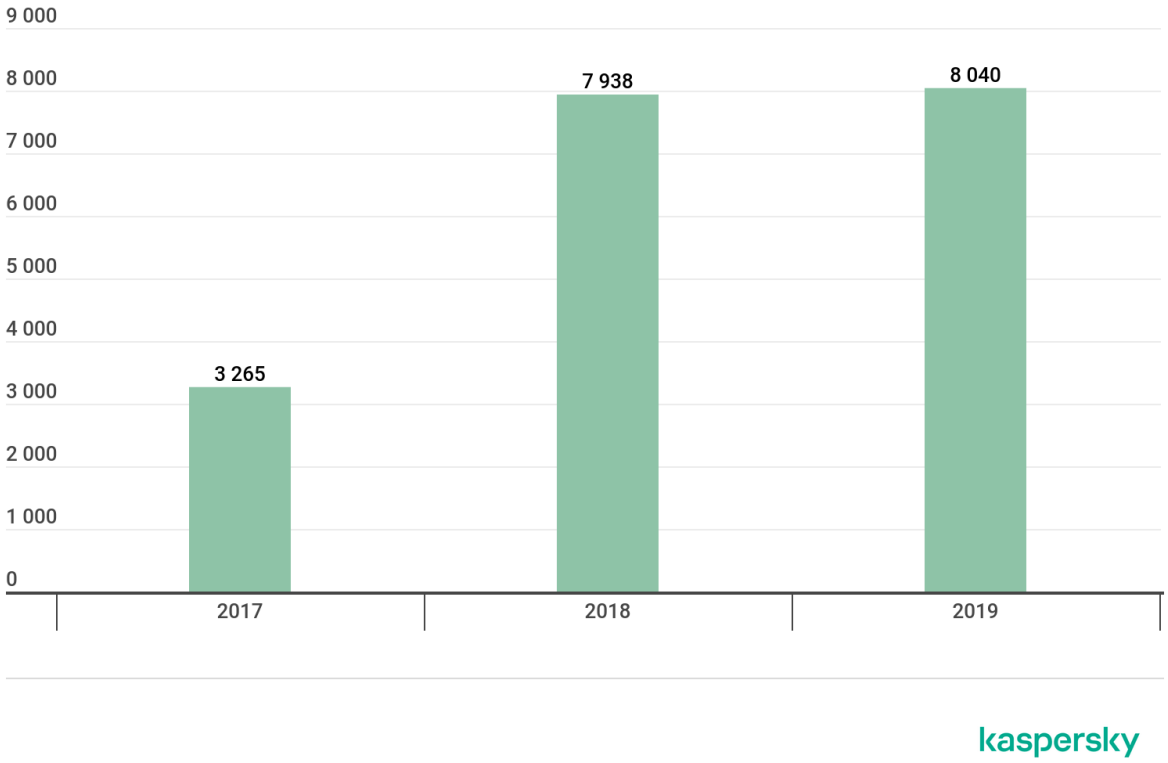
Old software means unpatched vulnerabilities—ones criminals can exploit—and isolated areas makes it easier for criminals to gain physical access to the internal ports of the motherboard. This is especially typical for the old ATM machines located in many regions with low resources and no budgets for ATM upgrades. When combined, ATMs become not only a highly profitable target—but an easy one.

From 2017 to 2019, there has been a marked increase in ATM attacks, due to a few families being particularly active. These target systems around the globe, regardless of the vendor, and have one of two goals: either stealing customers' information or funneling funds directly from the bank.

Considering all of the above, we decided to delve further into what has been happening in the world of ATM/PoS malware for the last few years.

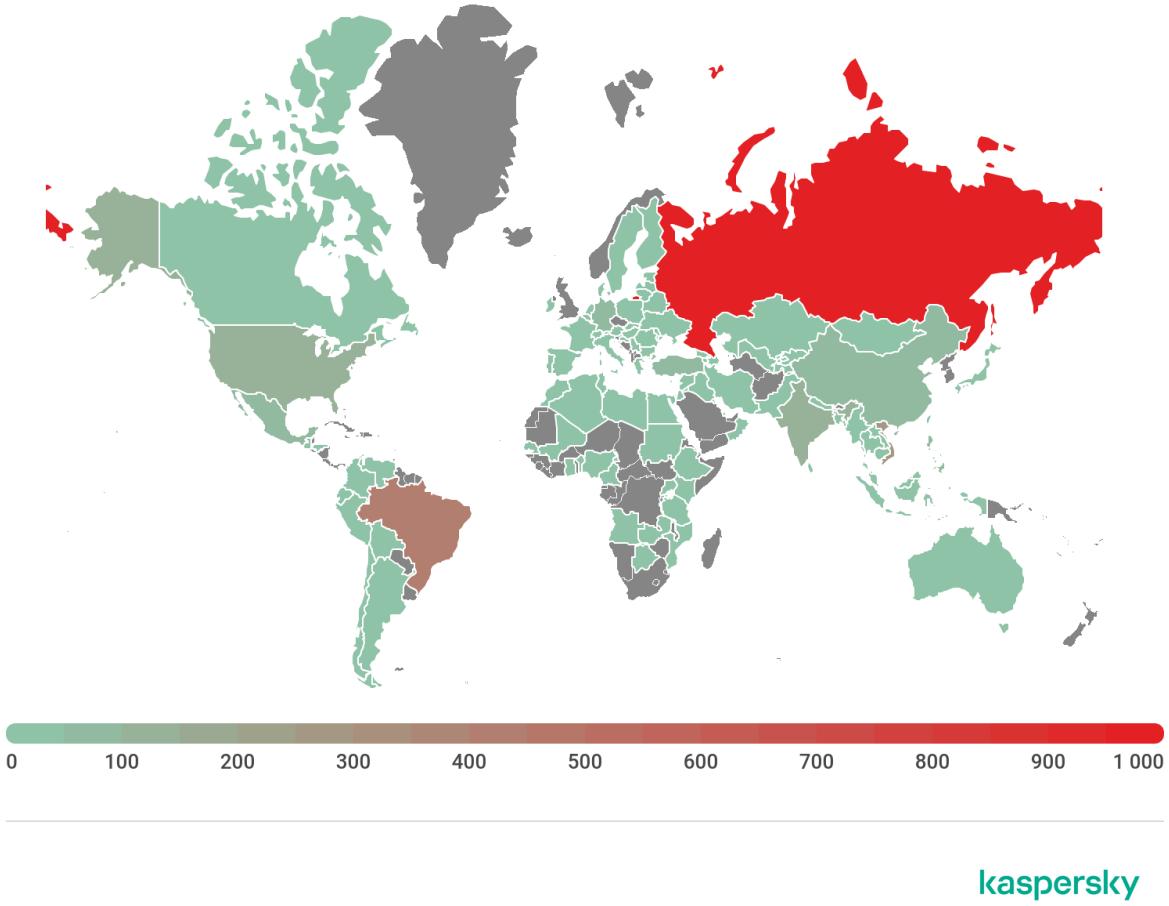
ATM/PoS malware attacks: by the numbers

To gain a closer look at ATM malware worldwide, we utilized the statistics processed by Kaspersky Security Network (KSN) over the course of the past three years globally.



Number of unique devices that encountered ATM/PoS malware, 2017-2019 (download)

The results showed that the number of unique devices protected by Kaspersky that encountered ATM/PoS (point-of-sale) malware at least once experienced a two-digit growth in 2018—and this number held steady, even increasing slightly, in 2019.



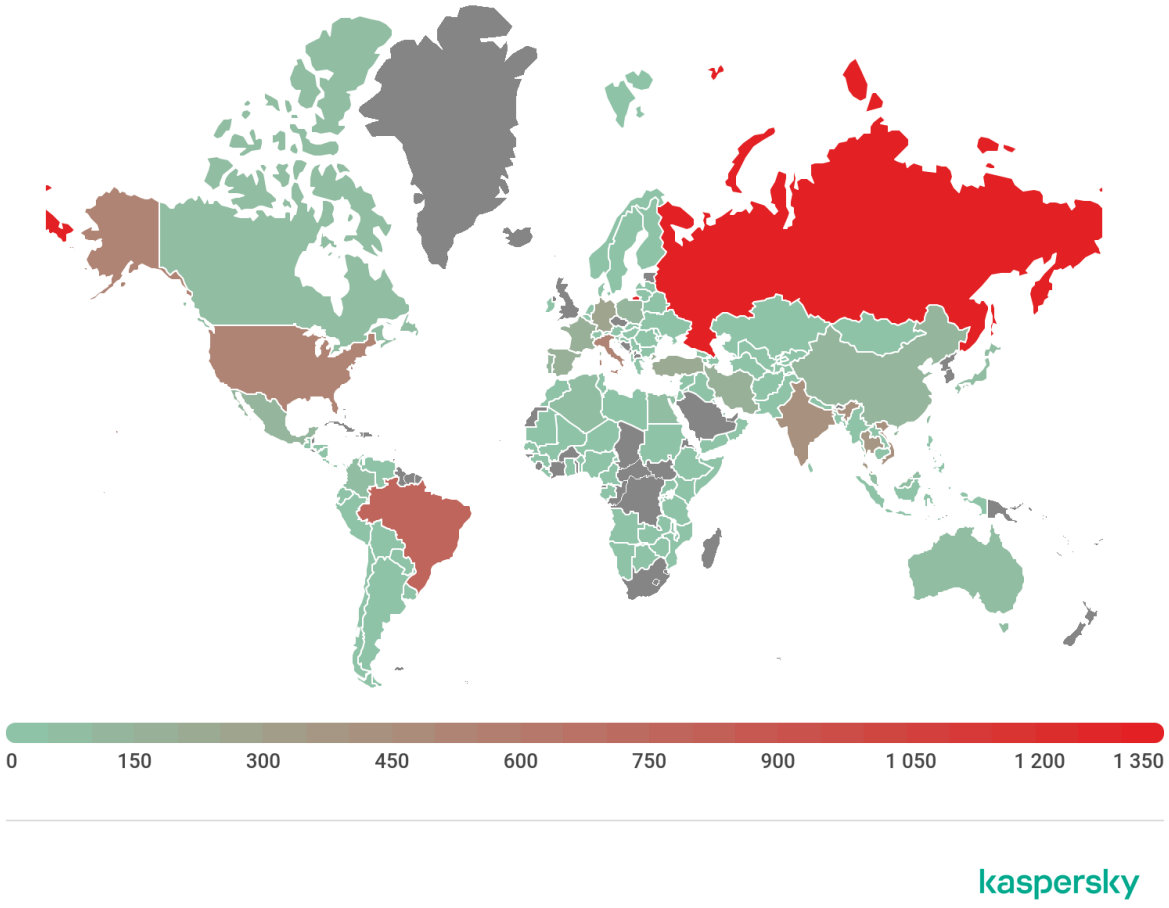
Geography of unique devices that encountered ATM/PoS malware, 2017 (download)

TOP 10 countries by number of unique devices that encountered ATM/PoS malware in 2017

	Country	Devices
1	Russian Federation	1016
2	Brazil	423
3	Vietnam	281
4	United States	148
5	India	137
6	Turkey	96
7	China	94
8	Germany	58

9	Philippines	53
10	Mexico	51

The ten countries that had the greatest number of unique devices affected by ATM/POS malware were relatively dispersed around the globe, with the highest number in Russia. Russia has had a long history of threat actors targeting financial institutions. For example, it was in 2017 that Kaspersky researchers uncovered an ATM malware dubbed "ATMitch" that was gaining remote access control over ATMS at Russian banks. In addition, the relatively high rates in both Brazil and Mexico can be partially attributed to Latin and South America's longstanding history as a hotspot of ATM malware.



Geography of unique devices that encountered ATM/PoS malware, 2018 (download)

TOP 10 countries by number of unique devices that encountered ATM/PoS malware in 2018

	Country	Devices
1	Russian Federation	1370

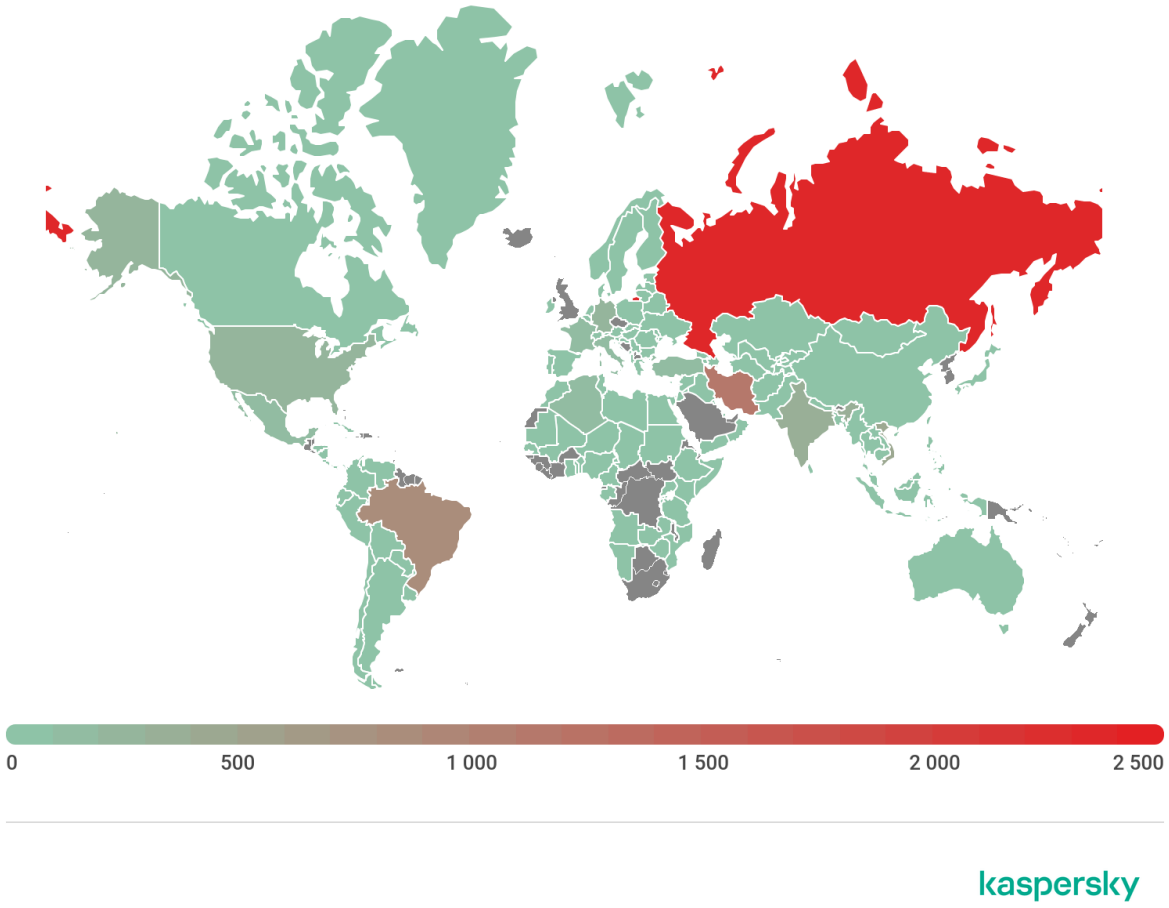
2	Brazil	753
3	Italy	537
4	United States	519
5	Vietnam	433
6	India	408
7	Thailand	369
8	Germany	277
9	Turkey	224
10	Iran	198

In 2018, the countries with the greatest number of ATM/PoS malware incidents recorded by unique devices remained distributed worldwide, but the countries remained similar to 2017, with the highest activity recorded in Russia and Brazil.

The overall increase in the number of devices affected can be attributed to both the reappearance of new ATM malware and the development of new families:

- **ATMJackpot** first appeared in Taiwan back in 2016. It infects the banks' internal networks, allowing it to withdraw funds directly from the ATM. ATMJackpot was able to reach thousands of ATMs.
- **WinPot** was discovered at the beginning of 2018 in Eastern Europe and was designed to make the infected ATM automatically dispense all cash from its most valuable cassettes. Because of its time counter, its execution is time-dependent: if the targeted system's time does not fall within the preset period during which the malware was programmed to work (e.g. March), WinPot silently stops operating without showing its interface.
- **Ice5** originated in Latin America. Its engineering tool is written in a scripting language that allows the attackers to achieve a significant level of manipulation over the infected ATMs. The initial infection occurs via the USB port.
- **ATMTest** is a multi-stage infection in 2018. It requires console access to the ATM, meaning the attackers have to gain remote access to the bank's networks. This malware was originally coded to steal money in rubles.
- **Peralta** was an evolution of the infamous ATM malware project called Ploutus, which led to losses of $64,864,864.00 across 73,258 compromised ATMs. Both Peralta and Ploutus originated in Latin America.
- **ATMWizX** was discovered in the fall of 2018 and dispenses all cash automatically, starting with the most valuable cassettes.

- **ATMDtruck** also appeared in the fall of 2018 with indications that the first victims were in India. It collects enough information from the credit cards inputted into the infected ATM that it can actually clone them. It drops the malware “Dtrack”, which is a sophisticated spy tool.



Geography of unique devices that encountered ATM/PoS malware, 2019 (download)

TOP 10 countries by number of unique devices that encountered ATM/PoS malware in 2019

	Country	Devices
1	Russian Federation	2306
2	Iran	1178
3	Brazil	819
4	Vietnam	416
5	India	353

6	Germany	228
7	United States	220
8	Italy	197
9	Turkey	149
10	Mexico	114

This past year, the ten countries with the highest level of ATM/PoS malware activity remained the same, with only one change: Mexico once again entered the top ten, while Thailand left.

Overall, the total number of devices affected increased once again. In fact, ATM/PoS malware activity reached new levels by the spring of 2019 with a string of operations: ATMqot, ATMqotX, and ATMJaDi. ATMgot operates directly on the ATM using the dispenser to withdraw the maximum number of banknotes allowed; if it cannot do this, it will default to 20 notes. This malware also possesses anti-forensic techniques that allow it to delete traces of the infection from the ATMs, as well as some video files, which could potentially be used as part of video monitoring.

ATMJadi orginated in Latin America and is capable of cashing out ATMs. Since it's a Java-based project, it's platform-dependent—and thus highly targeted. In order to be installed, the attackers must gain access to the bank's network. This suggests the attackers first compromise the bank's infrastructure. But what's perhaps most interesting is the false flag section with strings in the Russian language.

The problem of cyberattacks is compounded by the use of outdated and unpatched systems. That means that, even as new 2019 malware families were developed, the old ATM families from the previous years can still be used to launch successful attacks.

A look towards the future

ATM/PoS malware will only continue to evolve, and so, we will continue to monitor the ecosystem closely. We've already seen WinPot, first discovered in 2018, active this year in different parts of the world.

Latin America has long been known as a region of innovative cybercriminals who adopt techniques other region uses. It's not surprising then that a new trend was recently discovered in development: an ATM MaaS project whereby a group in Latin America is attempting to sell ATM malware developed for each major vendor on the market. Projects like these provide further evidence that the world of ATM malware is still evolving, with cybercriminals continuously developing better attack strategies.

Our research has also shown that, beyond Latin America, countries in Europe and the APAC region are of particular interest to ATM attackers, as is the United States. This signifies that ATM malware is a truly global threat. After all, ATMs are located in nearly every country and few systems offer access to such massive amounts of fund.

How, then, can you protect your money? No matter how digital banking has become, ATMs are still an inevitable part of managing your funds. While you can't control whether or not an ATM machine is attacked, by conscientiously monitoring your accounts and financial transactions, you can make sure suspicious activity is quickly identified and the proper channels duly notified. This should help mitigate the damage caused by any attack.

For financial institutions, staying secure requires a comprehensive, multi-step approach:

1. Evaluate which attack vectors are more likely to be used and generate a threat model. This will depend, for example, on what network architecture is in place and where the ATM is installed – a place not controlled by your organization, such as a wall on the street, or an office under video surveillance, etc.
2. Determine which ATMs are outdated or have an OS version that's reaching the end of its vendor support. If you cannot replace the legacy devices, pay attention to this fact in your threat model and set the appropriate security solution settings, which do not affect the device's productivity.
3. Regularly conduct security assessments or pentests of ATMs to find possible cyberattack vectors. Kaspersky's threat hunting service can also help you find sophisticated cybercriminals.
4. Regularly review the physical safety of ATMs to detect abnormal elements implemented by attackers.

1. If ATM configurations permit it, install a security solution that protects the devices from different attack vectors, such as Kaspersky Embedded Systems Security. If the device has extremely low system specs, the Kaspersky solution would still protect it with a Default Deny allowlisting scenario

PoS terminals are in many aspects similar to ATMs, but still possess a number of differences to be mindful of—and tackled accordingly. Apart from the steps mentioned above (which remain applicable), the following must be taken into account:

1. Often more powerful when compared to an average ATM, Windows-based PoS terminals offer greater spaces for attackers' maneuvering and are capable of running a broad range of modern malware and hacking tools. This makes implementation of multi-layered protection a must.
2. While also residing in public spaces, they generally lack ATMs' heavy armor. Therefore, they are more susceptible to direct attacks using unauthorized devices. This makes properly configured Device Control even more valuable.

3. As they are frequently involved not only in financial, but also personal, data processing, this adds to their attractiveness for cyberattacks and also subjects them to more legislation. In combination with direct attack scenarios, implementation of file integrity monitoring and log inspection are mandatory, preferably in a way that allows tracking changes offline.
4. Embedded systems should be protected not only by host-based security, but also by application of network-level security, such as Secure Web Gateways or Next-gen Firewalls capable of detecting and blocking unsolicited communications and other systems both inside and outside of the company's infrastructure.

- ATM attacks
- Financial malware
- Malware Descriptions
- Malware Statistics
- Targeted attacks

Authors

Kaspersky

A look at the ATM/PoS malware landscape from 2017-2019

Your email address will not be published. Required fields are marked *