Banking Trojans: A Reference Guide to the Malware Family Tree

By Authors & Contributors

Archived: 2026-04-05 23:34:50 UTC

Introduction

F5 Labs attack series education articles help you understand common attacks, how they work, and how to defend against them.

What is a Trojan?

A trojan is any type of malicious program disguised as a legitimate one. Often, they are designed to steal sensitive information (login credentials, account numbers, financial information, credit card information, and the like) from users.

Trojan malware takes its name from the classic Trojan horse ploy from the war between the Greeks and the independent city of Troy. The ancient Greeks were able to defeat the city of Troy by hiding soldiers inside a giant wooden horse they left behind as a gift while they feigned retreat following a 10-year war. Little did the Trojans realize that by taking the horse as a trophy of war, they were bringing an elite Greek fighting force right inside the walls of their city, ultimately leading to the fall of Troy. A malicious gift thus became known as a Trojan Horse.

A banking trojan operates in much the same way—disguising itself as something good or beneficial to users, but having a far more sinister, hidden purpose. Even a mobile app that appears to serve a genuine purpose (for example, a game, flashlight, or messaging service) can secretly be a trojan looking to steal information. Trojans evade detection by having dormant capabilities, hiding components in other files, forming part of a rootkit, or using heavy obfuscation.

Every individual family of malware has its own “signature moves,” and with each iteration, malicious actors grow more sophisticated. Banking trojans are a specific kind of trojan malware. Once installed onto a client machine, banking trojans use a variety of techniques to create botnets, steal credentials, inject malicious code into browsers, or steal money.

How Banking Trojans Began

It took almost 20 years for banking customers to get comfortable with the idea of online banking, which began in the 1980s. With the majority of banks offering online banking by the year 2000, it wasn’t long before attackers found ways to exploit this new attack surface using banking malware. Banks were quick to realize that they were attractive targets to attackers, and they responded by hardening their systems. In turn, cybercriminals soon realized that it was difficult to attack the institutions themselves, so they pivoted, targeting customers instead. Stealing customer credentials was a more feasible avenue of attack, and out of this the first banking trojans were created.

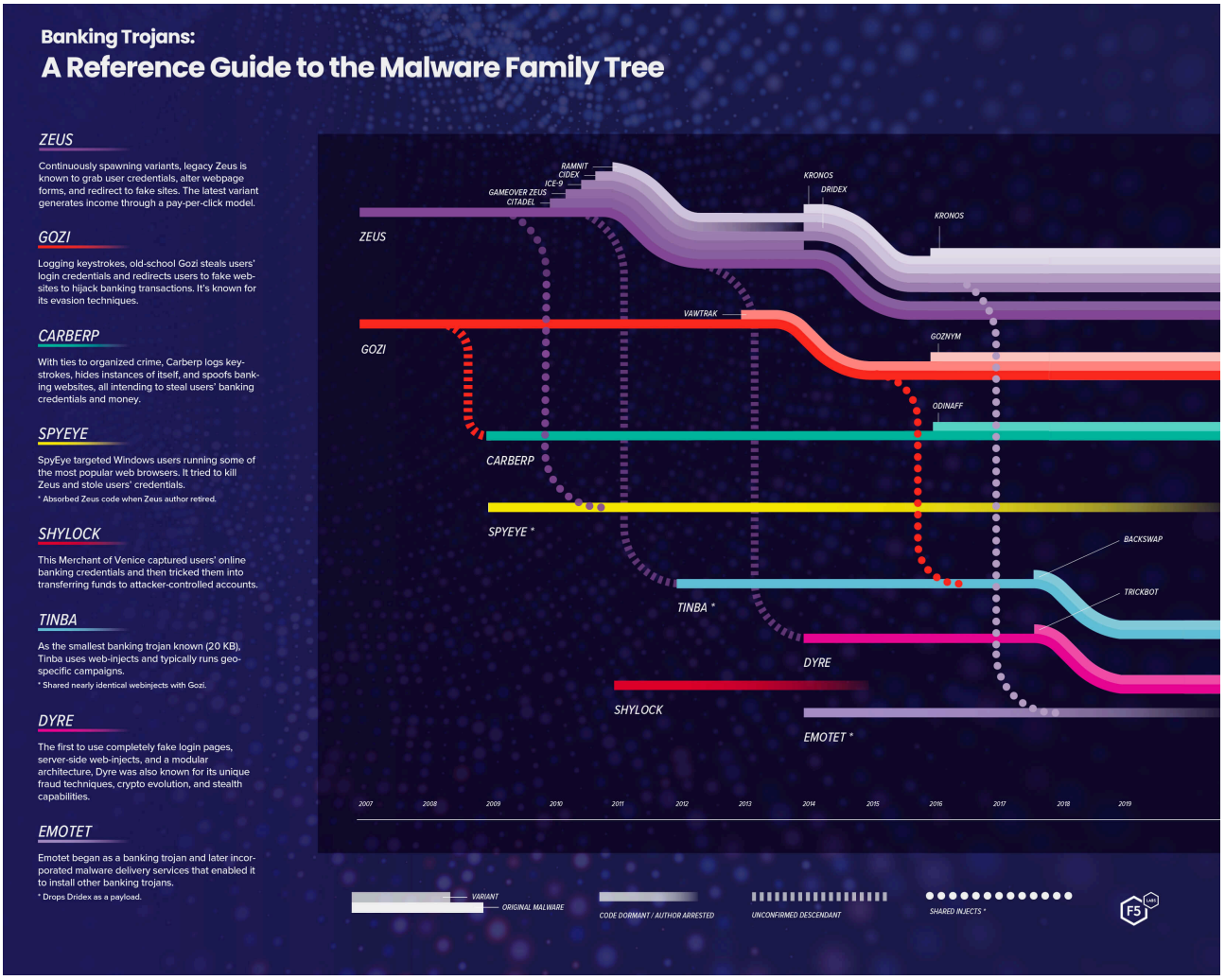
Banking trojans targeted users primarily through spam, phishing, advertising, drive-by-downloads, or social engineering. They can falsely advertise themselves as attachments or games.

Since then, the scope, technical ability, and focus of the malware authors has changed. What first started as malware that primarily targeted customers of financial institutions evolved to target a range of industries, including online advertisers, digital analytics firms, financial tech companies, social media sites, and communication platforms. Today, banking trojans are pervasive across the Internet, and all sorts of institutions—not just financial institutions—need to be aware of how to protect themselves and their customers.

Speaking the Language

Before we look at specific banking trojans, there's a bit of malware jargon that helps make these descriptions easier to understand:

- **Malware family.** A collection of malware that's produced from the same code base.
- **Variant.** Malware that's built from an existing code base, but with a new signature that is not included in the list of known bad signatures used by anti-virus and anti-malware solutions.
- **Strain.** Another name for a malware variant.
- **Malware version.** Another name for a malware variant.
- **Descendant.** Similar to a variant, descendant refers to malware that's based on an existing code base and integrates different tools or techniques.
- **Campaign.** A series of operations undertaken by malware authors intended to infect a specific set of targets.
- **Rootkit.** Code that targets the lowest level functions of an operating system. It is often used by malware to hide, both from users and from the operating system itself.
- **Bootkit.** Code that targets the operating system when it starts up. It often runs automatically when the system starts.
- **Dropper.** Usually used at the first stage in a malware infection, droppers are designed to install some other kind of malware onto a target system.
- **Sample.** A single example of a malware variant that is studied by engineers to determine characteristics of the malware variant.



A Reference Guide to the Malware Family Tree

Active and Notable Trojan Banking Malware Families

The number of banking malware families—and strains within those families—is constantly evolving. What follows is not a comprehensive list of all banking trojans, but includes some of the most destructive banking trojan families seen since 2007.

- **Zeus.** Also known as ZBOT, Zeus is the most widespread banking malware. First seen in 2007 grabbing user credentials, altering webpage forms, and redirecting users to fake sites (among other things), it consistently evolved. Zeus and was pervasive across the Internet until 2010 when, according to Kaspersky Lab, its author reportedly "retired" and sold the source code to the developer of SpyEye, another family of banking trojans.[1] Zeus has been attributed to an anonymous developer in Russia, however, cybercriminal gangs can easily cross national borders. The source code has been publicly available since 2011, and a number of variants have been developed. The original version of Zeus malware worked on Microsoft operating systems and was spread through spam and drive-by downloads. Since then, Zeus variants have evolved in technique and sophistication. Some are able to evade detection and others were designed to generate income through a pay-per-click model. Although the original version of Zeus has been largely neutralized by anti-virus software, it continues to be dangerous through its numerous descendants. Zeus

and its spinoffs can be seen all over the web, as there are thousands of variants, including notable ones such as Citadel, Gameover, and Atmos.

- **Gozi.** Also known as Ursnif, Gozi is one of the oldest banking trojans. To put it simply, Gozi tricks users into completing financial transactions in accounts that aren't theirs. It's been around since 2007 and, as one of the original banking trojans, has caused millions of dollars in damages. In 2010, the Gozi source code was leaked, which lead to the creation of several different versions of the malware. It was leaked for a second time in 2015, which led to further modularization and development of new versions of the malware. In 2016, Latvian hacker Deniss Calovskis was sentenced to time served (21 months) for developing the original Gozi code.[9] Arresting a key developer often stops banking trojans, but it appeared to have little affect with Gozi. After more than ten years, Gozi continues to be one of the most sophisticated and constantly evolving malwares. When first developed, Gozi used rootkit components to hide its processes. More recently it has added both client-side and server-side evasion techniques and has continued to evolve. Recently, Gozi and Tinba have been connected through their use of shared web injection techniques. Although the scope has expanded for many banking trojans, Gozi continues to target financial institutions. As of March 2019, Gozi has been connected to DanaBot for targeting some of the same Italian banks. Gozi shows no signs of stopping and is considered one of the most dangerous pieces of banking trojan malware.

- **GozNym.** GozNym is a hybrid of Gozi and Nymaim. The Nymaim malware itself is a dropper. It acts solely as a gateway—a delivery system for other strands of malware. GozNym uses Nymaim's advanced stealth capabilities to unload the previously mentioned Gozi malware. Researchers originally tracked both pieces of malware individually. Nymaim on its own is famous for its sophisticated evasion techniques and was seen as early as 2013.[10] As of late 2015, security researchers noticed that Nymaim was fetching a Gozi module and using it to launch attacks. Attacks by the first GozNym hybrid malware were detected in April 2016 targeting Polish banks. These attacks were quickly followed up with another geo-centric campaign targeting major US banks and e-commerce platforms.[11] GozNym continued its operations all over the world, targeting a range of countries from Canada to Spain to Brazil and Japan.
  GozNym was one of the most notorious banking trojan hybrids but its reign was short lived. In September 2016, security researchers at Talos were able to "sinkhole" the GozNym botnet, essentially stopping operations.[12] In November 2016, US authorities indicted Krasimir Nikolov, a Bulgarian national, for the distribution of the GozNym banking trojan[51] and in April 2019 he pled guilty to the charges.[52] Operations with GozNym slowed after Nikolov's arrest, however Nymaim remains an active threat and there has been some recent speculation that parts of GozNym may yet reemerge in new malware forms.[53]

- **Carberp.** This malware first emerged in 2009. Its purpose was to steal banking credentials. Along with hooking network APIs,[13] Carberp works like many other banking trojans by logging keystrokes, spoofing websites, and hiding instances of itself in specific locations.[14] In 2012, eight individuals involved with Carberp's operations were arrested by Russia's Ministry of Affairs. In 2013, however, Carberp made a comeback with improved paid versions and mobile app variants available in the wild. In 2013 Carberp's code and bootkit were leaked; components of Ursnif (also known as Gozi) and Citadel were also found inside.[15] Carberp was adopted by the Carbanak gang in 2016 and was spotted attempting to steal money from banks all over the world.[16] This organized cybercrime gang allegedly began in 2013 and is suspected

of other organized criminal activity, including money laundering and drug and human trafficking. In 2018 the alleged leader of the Carbanak criminal gang was arrested.[17] Since then, Carberp has remained quiet, though still an active threat. Silence, another group that has used many of the same techniques as Carbanak, has been active in the cybercrime scene targeting banks in Russia, Armenia, and Malaysia.[54] Carberp is still a threat, and it is very possible that it will make a strong resurgence.

- **SpyEye.** First spotted in the wild in 2009, SpyEye targeted Windows users running some of the most popular web browsers. It logged keystrokes and used form grabbing techniques to steal users' credentials. As well as being a banking trojan in its own right, it attempted to target and remove the competitive malware, Zeus. SpyEye originally had a “kill Zeus” feature in its toolkit that claimed to remove Zeus from an already infected machine. SpyEye never reached the same distribution of Zeus, though it had many of the same features. In 2010, one of Zeus’ authors allegedly shared Zeus’ source code with the SpyEye developers and they merged the two toolkits.[18] SpyEye was particularly destructive from 2010 through 2012 and allegedly caused close to $1 billion in financial damages.[19] In 2016, Russian Aleksandr Andreevich Panin, who went by the moniker, Gribodemon, and Algerian Hamza Bendelladj, who went by the moniker of Bx1, were sentenced to a combined 24 years 6 months in prison for developing and distributing SpyEye.[20]

- **Shylock.** Shylock’s authors clearly had an appreciation for Shakespeare as this trojan took its name from The Merchant of Venice and contained snippets from the play in its files.[21] Shylock began its campaign in 2011, capturing users' online banking credentials and then tricking them into transferring funds to attacker-controlled accounts. It used modular, adaptable functionality that responded quickly to security countermeasures. Shylock was first detected in July 2011. By the end of 2011, its distribution had grown significantly. It continued to expand over the course of 2012 and maintained its presence up until 2014.[22] Unlike many other banking trojans, Shylock was privately owned and was not sold in an underground marketplace. Also, unlike some other banking trojans, Shylock maintained a narrow geographic remit throughout its active time, notably focusing its attention on the UK with some US banking institutions also appearing on the target list. Shylock’s authors ran it as a business, working typical 9 to 5 hours with code compilations occurring on specific days.[23] In July 2014, an eastern European gang connected with Shylock had its domains and command-and control servers shut down.[24] Activity for shylock trailed off after the assets were confiscated.

- **Citadel.** First identified in 2011, Citadel, a Zeus variant, primarily targeted credentials that were stored in password managers using its keylogging capabilities. Citadel was especially active from 2012 through 2014. In 2017, prosecutors asserted that Citadel had infected over 11 million machines.[25] Using advanced evasion techniques, Citadel achieved unprecedented distribution. IBM researchers estimated that, at one point, 1 in every 500 machines worldwide was infected with the malware.[26] Citadel offered a unique interactive feature on underground markets for customers (that is, other criminals) that enabled them to file bug reports and get technical support.[27] This feature ultimately led to its demise. In 2015, “Rainerfox,” also known as Dimitry Belorossov, was arrested and sentenced to nearly five years in prison for distributing Citadel. In 2017, Mark Vartanyan, a Russian national who went by the moniker “Kolypto,” pled guilty to fraud for helping to develop part of the Citadel malware. He was sentenced to five years in

prison for his part.[28] Since 2017, news about Citadel has slowed but, like many other banking trojans that have reemerged from dormancy, it remains an active threat.

- **Tinba.** Also known as Tiny Banking Trojan, Tinba was first discovered in the wild in 2012 when it was found to have infected a number of computers in Turkey. It is the smallest banking trojan known, consisting only of a 20 KB file. It typically runs geo-specific campaigns, though varies its regions. Tinba's code was first leaked in 2014 and proved to be a useful resource for malware researchers to analyze.[29] Tinba has also been linked to other banking trojans in the past. It is allegedly a highly modified version of Zeus, as it has a similar architecture.[30] In 2016, F5 labs reported that Tinba and Gozi used almost identical web injects. They seem to have been bought from the same webinject workshop. Tinba has not been in the news recently, but it would be naive to think that it is gone for good.

- **Vawtrak.** Also known as Neverquest or Snifula, Vawtrak is a descendent of the Gozi banking trojan. First discovered in 2013, Vawtrak was active in geographically targeted campaigns and employs a Cybercrime-as-a-Service business model. This is not unique to Vawtrak, as other trojans, including Gameover Zeus, also use this business model. Instead of selling the malware outright, Vawtrak's authors offer malware delivery based on a service agreement. For example: A Number of Passwords stolen from X number of Users, using bank Y in country Z.[31] There have been a few technical papers detailing the analysis of the Vawtrak malware and its evolution over the years.[32] In January 2017, Vawtrak's alleged author, Russian national Stanislav Vitaliyevich Lisov, who went by the moniker "Black" and "Blackf," was arrested and as of February 2019, pled guilty to creating, running, and infecting users with the Vawtrak banking trojan.[33] Vawtrak's activity declined after Lisov's arrest, however, another banking trojan, Bokbot (also known as IcedID) has been connected to the group behind Vawtrak.[34]

- **Emotet.** This malware was first identified by security researchers in 2014 as a simple banking trojan. Later versions of the malware evolved and included the addition of malware delivery services, including the ability to install other banking trojans.[35] In August 2017, Emotet was connected to another banking trojan, Dridex—Emotet "dropped" Dridex as an additional payload.[36] The technique of using one piece of malware to drop another is not new, but it is significant to see banking trojans "working together." As of September 2018, Emotet was utilizing the EternalBlue Windows vulnerability (first seen with the WannaCry ransomware) in order to propagate.[37] This powerful vulnerability has had a patch out, however, there are still devices out there that haven't yet patched against the SMB (file sharing) vulnerability. Emotet is not a continually running malware; it tends to run through geographically centered campaigns, yet its techniques are constantly evolving and it continues to be dangerous.

Kronos. Kronos is known in Greek mythology as the "Father of Zeus." Kronos malware was first discovered in a Russian underground forum in 2014 after the takedown of Gameover Zeus. It was more expensive than many other banking trojans, costing $7,000 to buy outright or $1,000 for a one-week trial. Many other banking trojans could be bought from underground forums for hundreds, not thousands, of dollars. Kronos marketed itself as one of the most sophisticated trojans, and many malware researchers commented that its author(s) clearly had prior knowledge of malware techniques. [2] The code is well obfuscated using many different techniques. Security researchers from Kaspersky Lab postulated that Kronos may be a spin-off of the Carberp banking trojan, The code

is well obfuscated using many different techniques. Security researchers from Kaspersky Lab postulated that Kronos may be a spin-off of the Carberp banking trojan, [3] and IBM analysts also connected Kronos to Zeus through its compatible HTML injection mechanism. [4] In August 2017, Marcus Hutchens, the security researcher who single handedly put a halt to the WannaCry ransomware outbreak, was indicted and charged with writing with intent to distribute Kronos malware. In April 2019, Hutchins pled guilty to two of the ten charges laid against him. [5] As of July 26th 2019, Hutchins was sentenced to time served with supervised release. [6] Unlike many other banking trojans, Kronos did not die out with the arrest of a supposed key author. In July 2018, Kronos reemerged with three distinct campaigns targeting Germany, Japan, and Poland. There is also some circumstantial and speculative evidence in the malware research community suggesting that Kronos has been rebranded and is being sold as the Osiris banking trojan. [7] Kronos is still active and continues to be a threat.

- **Dyre.** Also known as Dyreza, Dyzap, and Dyranges, Dyre first emerged in 2014 targeting major online banking services. Dyre is allegedly a variant of Zeus malware, though no official attribution to the source code can be confirmed.[8] When Dyre first emerged, it sent shock waves through the malware analysis world with its sophistication and destructiveness. Dyre caused losses in the tens of millions of dollars for large US-based banks. F5 labs reported in April 2015 that Dyre was the first trojan to use completely fake login pages, server-side web-injects, and modular architecture. F5 labs published a comprehensive report on Dyre detailing its unique fraud techniques, its crypto evolution, and stealth abilities. Along with its technical evolution, Dyre moved on from targeting just banks to targeting software-as-a-service (SaaS) companies such as Salesforce and browsers such as Microsoft Edge. In February 2016, researchers reported that Dyre had stopped spreading in November 2015 after Russian authorities arrested a number of gang members who were the alleged authors of Dyre's code.[38]

- **Trickbot.** Known as one of the successors to the infamous Dyre botnet, Trickbot continues to grow in sophistication and technique. F5 labs first reported on it as a pure banking trojan targeting the financial services industry in 2016. It is typically spread through malicious spam emails, targets users' financial information, and acts as a malware dropper for other programs. Like many other pieces of malware, it can harvest credentials, spread laterally through a network, and conduct reconnaissance.[39] When Trickbot first burst onto the scene, the code looked a lot like Dyer's source code, though it was missing functionality in comparison. Like many pieces of financial malware, Trickbot's first iterations exclusively targeted financial institutions. It quickly expanded its focus from banks in Australia, the UK, and Canada to banks in Germany, as well. Within months of its first reported actions, Trickbot quickly expanded from banks to include US Credit Card Companies, wealth management services, and Customer Relationship Management providers. Further, Trickbot expanded its technical capabilities by adding a layer of encryption. Reportedly last seen in January 2019,[55] Trickbot has some new technical updates that include the ability to grab remote application credentials. Trickbot's authors are showing that they're still active, and companies should be aware that this malware is still a threat.

- **Dridex.** First seen in 2011, Dridex has had a longer evolutionary journey than most malwares and has survived through the years by obfuscating its main command-and-control (C&C) servers through proxies. Dridex's first appearances[40] in September 2011 came under the name Cidex. It caused destruction to banks until June 2014 when Dridex version 1.1 appeared in the wild. Dridex emerged almost exactly one month

after Operation Tovar's takedown of the Gameover ZeuS botnet, which also marked the end of Cidex attacks.[41] Dridex and Gameover ZeuS have many similarities in their code, and attribution for Dridex[42] is tied to a Russian-speaking gang that may be a spinoff from the "Business Club," an organized cybercrime gang that developed the Gameover ZeuS botnet. A number of arrests were made in September 2015, but that did little to stop Dridex. In February 2016, F5 labs published reports on the Dridex Botnet 220 campaign noting the evolution of the malware, and then in April 2016 noted that Dridex shifted focus from UK banks to US banks. In December 2018, researchers found connections between Dridex, Emotet, and Ursnif/Gozi malware.[56] It continues to evolve technically and remains an active threat.

- **DanaBot.** One of the newer banking trojans, DanaBot first emerged in mid-2018,[43] targeting Australian users. Since it first appeared in the wild, DanaBot has been seen targeting European banks and email providers. Like many other banking trojans, DanaBot has recently shifted focus away from exclusively targeting financial services institutions for a number of reasons. Since users often share passwords across platforms, compromising credentials is still useful for many cybercriminals. F5 Labs also published a notable link between DanaBot, Gozi, and Tinba web injection patterns, supporting the idea that a great deal of fraud business logic is now implemented in JavaScript and sold to malware authors.

- **Ramnit.** This unique banking trojan started out in 2010 as a worm and, sometime after the Zeus source code leak, acquired parts of the Zeus code and became a banking trojan.[44] Ramnit has continued to evolve in terms of sophistication, technique, and scope as a botnet since becoming a banking trojan. It remains active despite a shutdown of 300 command-and-control servers in February 2015.[45] After this setback, Ramnit reappeared in late 2015 and again in mid 2016.[46] In early 2017, F5 labs published a technical article breaking down Ramnit's new disappearing configuration file. Like many other banking trojans, Ramnit has broadened its scope in recent years. Over the 2017 holiday season, Ramnit's target list was 64% eCommerce retailers in addition to financial services institutions. In 2018, Ramnit continued to work quickly, infecting over 100,000 machines in two months.[47] Ramnit continues to be distributed via exploit kit and still runs active campaigns today, most recently returning back to target Italian financial institutions (/content/f5-labs-v2/en/labs/articles/threat-intelligence/ramnit-returns-to-its-banking-roots--just-in-time-for-italian-ta.html).

- **Panda.** Yet another Zeus variant, Panda was first discovered in Brazil in 2016, around the time of the Olympic games. Panda uses many of the traditional techniques from Zeus, including man-in-the-browser (MITB) attacks and keylogging, but sets itself apart through its advanced stealth capabilities. This has made analyzing the malware more difficult. As of 2017, Panda was able to detect 23 forensic analytic tools and it is possible that it now detects even more.[48] Like many other banking trojans, Panda has expanded its target list beyond just financial services institutions, and in 2018 was caught targeting cryptocurrency exchanges and social media websites. Moving to 2019, Panda continued to expand its scope. The March 2019 campaign (/content/f5-labs-v2/en/labs/articles/threat-intelligence/panda-malware--it-s-not-just-about-cryptocurrencies-anymore.html) exclusively targeted US-based companies, many of which are in the web services industry. Panda remains active; its stealth capabilities make it a unique malware family that continues to evade anti-virus software.

- **Backswap.** A variant on Tinba, Backswap was first observed in March 2018 targeting Polish banks and browsers. Backswap is written entirely in assembly language and is considered "position-independent code" (PIC), which means that it can be run from anywhere in memory. Its PIC status makes Backswap very different from other banking trojans. The Polish CERT published a comprehensive technical analysis on the code.[49] Backswap quickly expanded scope in April 2018, adding additional banks and techniques thoroughly detailed by F5 Labs. The evolution of techniques continued through August 2018 when Backswap also made a geographical shift away from Polish banks to exclusively target Spanish banks.[50] Through the latter part of 2018 and early 2019, Backswap continues to run campaigns, though its technical evolution has slowed.

Indications of Compromise for Users and Enterprises

While it can be difficult for the average user to detect that their device has been compromised, there are a number of clues to watch for. These clues can also be useful for security professionals managing user systems:

- Browsers that load web pages slowly and run sites slowly.
- Slow computer start-up and slow performance when nothing else on the system is running could be a sign of a virus or trojan.
- A fan that is constantly running or a hard drive that is always spinning could be a sign of an infection.
- Suspicious behavior such as a computer suddenly slowing down, opening programs that you didn't open, closing programs repeatedly.
- New or unexpected form elements in banking web pages, for example, fields that ask for credit card numbers or PINs.
- Failed login attempts the first time you attempt to log in despite the password being entered correctly.
- Unexpected pop-up windows are often a sign of an infection. Clicking on those pop-ups can install additional malware.
- Missing files or users noting that files are missing.
- Hijacked email or other accounts.
- Anti-virus solutions that stop working.
- Applications that take a long time to start or won't start at all.
- A computer that is actively doing something when no one is using it.

How Users Can Protect Against Banking Trojans

- Keep security, application, and utility software updated.
- Use two-actor authentication whenever the option is available.

- Only download apps and files from trusted sources.
- Use a browser that you trust when doing online shopping and banking.
- Use all security features that banks offer.
- Use a password manager. Most banking trojans can log keystrokes. By using a password manager to fill in passwords, you avoid physically typing in credentials, which essentially renders a keylogger useless.
- Compare your bank's login screen on your computer with the same login screen on someone else's to ensure they look the same.
- Use traffic filtering solutions to prevent data leakage.
- Take any security awareness training offered by your company or organization.
- Learn how to spot phishing emails and don't click on suspicious links. This is how most banking trojans are installed.
- Learn how to spot fake websites.

How Enterprises Can Protect Against Banking Trojans

Enterprises should consider implementing the following security controls based on their specific circumstances:
