Internet Security Threat Report

ISTR

Financial Threats Review 2017

An ISTR Special Report

Analyst: Candid Wueest

May 2017

Contents

Symantec

Contents

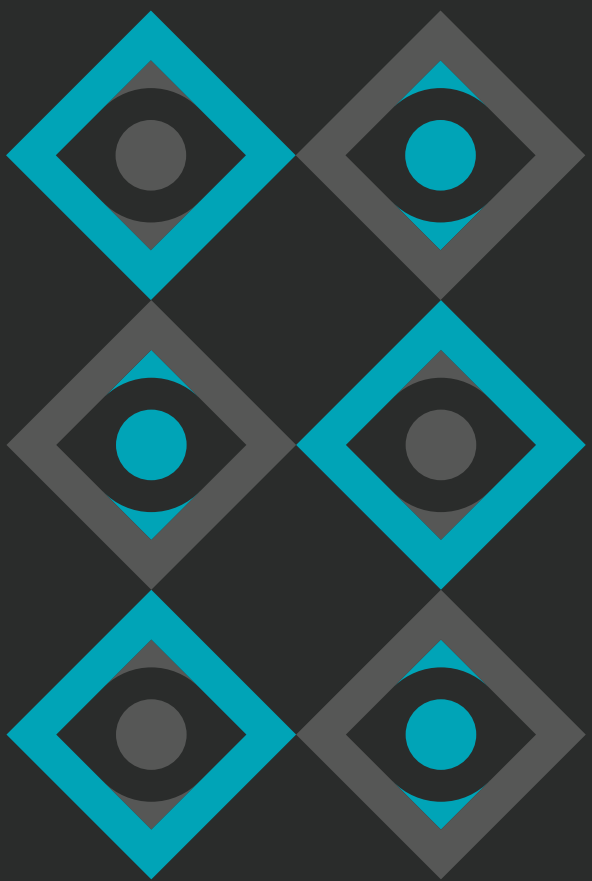
Graphics, Tables, and Charts

Symantec

Executive summary, key findings, and introduction

Section

00



Symantec

Executive summary

Financial threats are still profitable for cyber criminals and therefore continue to be an enduring part of the threat landscape. From financial Trojans that attack online banking, to attacks against ATMs and fraudulent interbank transactions, there are many different attack vectors utilized by criminals.

As we had predicted in 2015, we saw an increase in attacks against corporations and financial institutions themselves during 2016. This was evidenced with a series of high-value heists targeting Society for Worldwide Interbank Financial Telecommunication (SWIFT) customers. While there is no evidence of any such high value heists on SWIFT customers this year, the 2016 attacks saw several such institutions lose millions to cyber criminals and nation state supported attackers such as the Lazarus group.

On average, 38 percent of the financial threats we detected in 2016 were found in large business locations. Most of these infection attempts were not targeted attacks but were instead due to widespread email campaigns.

Although we have seen a 36 percent decrease in detection numbers for financial malware in 2016, this is mainly due to earlier detection in the attack chain and more focused attacks. With more than 1.2 million annual detections, the financial threat space is still 2.5 times bigger than that of ransomware. For example, the number of Ramnit (W32.Ramnit) detections approximately equaled all ransomware detections combined.

The financial Trojan threat landscape is dominated by three malware families: Ramnit, Bebloh (Trojan.Bebloh), and Zeus (Trojan.Zbot). These three families were responsible for 86 percent of all financial Trojan attack activity in 2016. However, due to arrests, takedowns, and regrouping, we have seen a lot of fluctuations over the last year. For example, Bebloh has all but vanished in 2017 after the Avalanche takedown. Many new variants of these families have appeared or re-appeared on the market, focusing on filling specific niches. The attackers mainly use scam email campaigns with little variation and simple attachments. For example, one single Bebloh sample was responsible for 55,000 global detections in 2016.

Japan was the main focus of financial Trojans Bebloh and Snifula (Trojan.Snifula) in 2016, with more than 90 percent of their activity focusing on the country. It is unclear why these two threats shifted their attention but there are indications that they use a shared resource for attacking similar targets. Globally, financial institutions in the U.S. were targeted the most by the samples analyzed by Symantec, followed by Poland and Japan.

We have also seen trends in financial malware attempting to hide configuration files from researchers as well as the move to redirection attacks or even manually logging into the system to issue large transactions if interesting financial software is detected.

This paper is an update to last year's paper (Financial threats 2015). While Symantec and other researchers have published various research focusing on individual threat families, this report will discuss the overall changes we have noticed in the financial threat landscape in more detail.

Key findings

- Cyber crime hit the big time in 2016, with high-profile victims and bigger than ever financial rewards. The Lazarus attacks that took place in 2016 were also the first time there was strong indications of state involvement in financial cyber crime.
- Ramnit was the most active financial Trojan in 2016, responsible for 38 percent of activity, followed by Bebloh (25 percent) and Zeus (23 percent).
- Three threat families were responsible for 86 percent of all financial threat attacks.
- Japan was the country with the most infections, followed by China and India.
- Financial institutions in the U.S. were targeted the most by the samples analyzed by Symantec, followed by Poland and Japan.
- The number of financial Trojan detections decreased by 36 percent in 2016 (73 percent in 2015).
- Malware authors are obfuscating the lists of attacked bank URLs, making it impossible to extract exact statistics for all threat families.
- Redirection attacks to fake sites have increased again.
- The phishing rate dropped to 1 in 9,138 emails in March 2017.
- The use of free self-service valid SSL certificates on malicious sites increased.
- Mobile banking malware targeted at least 170 apps for credential stealing.
- APT groups are using financial malware to blend in with more common attacks.
- One Bebloh sample alone was responsible for 55,000 global detections in 2016
- On average 62 percent of financial threat detections were on consumer computers.

Introduction

Financial threats, aimed at taking over customer transactions and online banking sessions, are still a force to be reckoned with. Although crypto-ransomware is becoming a common choice for cyber criminals when it comes to making a profit, we still see a significant amount of malware targeting financial organizations and their customers.

Financial institutions have increased security measures in their interactions with customers and also on their own infrastructure and backend systems. However, the cyber criminals have adapted their attacks and are mimicking customer behavior as closely as possible and attacking the institutions themselves.

Social engineering continues to play a major role in many attacks. As transaction authentication through mobile applications or text messages grows in popularity, we also see an increase in mobile malware trying to steal these credentials.

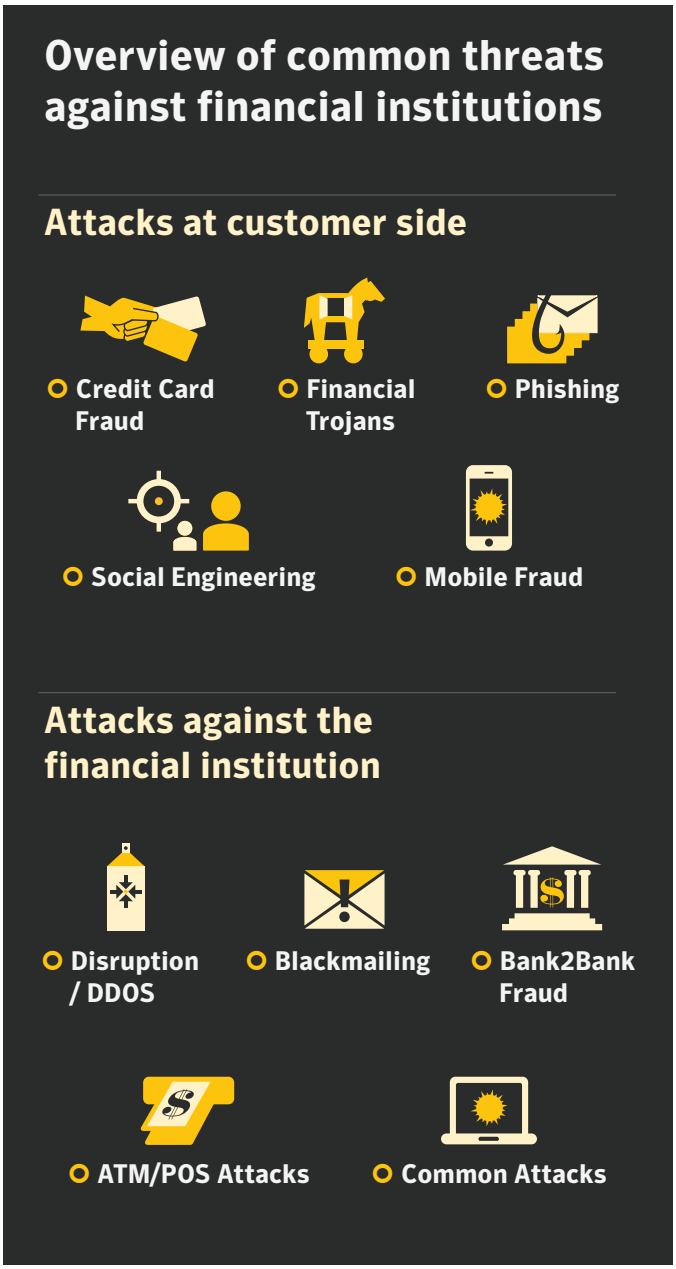
A simplified play book of common financial malware can be summarized with the following steps:

- The malware is installed on the target computer through any of the common infection vectors.
- The malware then waits until the user visits an interesting website and either steals the credentials, modifies the data inside the browser to its favor, or redirects the traffic to a remote server under the attackers' control to perform man-in-the-middle (MitM) attacks.
- Once the attackers have access to the online banking service, they will try to submit fraudulent transactions.
- Often the money is sent to so-called money mules, whose sole job is to withdraw the money and send it back to the criminals by other means.

The attacks are not only targeting the banks' customers. We have seen several attacks against the financial institutions themselves, with attackers attempting to transfer large sums in fraudulent interbank transactions.

Attacks against retail businesses and hotels, targeting point of sales (POS) terminals, continued in 2016. Even ATM threats are still active and evolving, although they often require physical access to the machine.

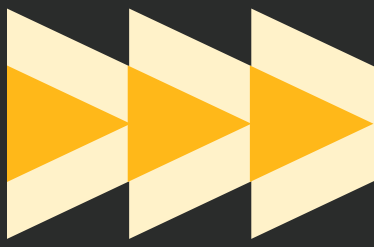
Financial institutions are confronted with attacks on multiple fronts. The main two types are attacks against their customers and attacks against their own infrastructure.



Targeted financial heists

Section

01



Symantec

Targeted financial heists

While the cyber crime threat landscape is typically dominated by indiscriminate, mass attacks, 2016 saw the emergence or re-emergence of a handful of sophisticated cyber crime groups going after financial institutions themselves instead of their customer base. Even though such sophisticated attacks take longer to conduct and have a lower success rate, when they are successful they can yield a high profit, making it more attractive to some groups. These criminals leverage techniques typically seen in advanced targeted attacks. The resources, knowledge, patience, and sheer bravado needed to execute these attacks demonstrates how cyber crime is potentially entering a new era.

There are quite a few groups who are after these big targets. For example, Dyre (Infostealer.Dyre) had a specialized team that targeted larger enterprise customers, trying to scam them out of transactions of $500,000 or more. The targets where hand-picked and infected using spear-phishing emails. Elaborate social engineering tactics with interactions by phone helped the criminal gang carry out successful fraudulent transactions.

Another example is the group behind Trojan.Redaman, which focused on remote banking systems in Russia. It is common for small and midsized companies to gather up payment transactions and issue them grouped together at the end of the month. Trojan.Redaman modifies the transaction batch files generated by enterprise accounting software before they are processed by the remote banking system tool. This allows the attackers to sneak in their own transactions unnoticed. All they have to do then is wait until the user submits the batch for processing. In some of the attacks the attackers installed a modified version of the remote access tool VNC, allowing them to connect to the compromised computer and explore further options for issuing transactions.

Another typical example is the Buhtrap group, which uses a first stage loader to analyze the target and identify if there are tools related to financial transactions installed. If the target is of interest, a specific payload will be deployed. Of course this also means that most sandboxes will not receive the actual final payload due to the absence of any financial software. The group is believed to have successfully stolen more than $25 million from banks in Russia and Ukraine.

In some cases, attacks against financial institutions do not lead to fraudulent transactions. In these cases, attackers can still attempt to profit from the break-ins by selling stolen information, profiting from insider trading on gained information or blackmailing the banks. For example, in November 2016 newspapers reported on a case of a bank in Lichtenstein where cyber criminals had breached the bank's security measures and extracted the account information of various customers. Subsequently the customers received a blackmail notice demanding they pay 10 percent of their account balance or risk having their information published online.

These incidents, along with past activity of the Carbanak, Calcium (Fin7) and Metel groups indicate that many attackers are increasingly focusing on corporate targets. Attack groups are either going after the financial departments of corporations or directly attacking the financial institutions.

Two widely discussed groups targeted the inner workings of the international financial system in 2016, hinting at how financial institutions would be facing a much different kind of threat in 2017.

Lazarus

A cyber heist on the Bangladesh central bank in early 2016 was one of the most audacious bank heists of its kind. The criminals got away with US$81 million and, were it not for a typo and the suspicions of eagle-eyed bank officials, could have made off with $1 billion.

The criminals exploited weaknesses in the Bangladesh bank's security to infiltrate its system and gain access to computers with access to the SWIFT network. The attackers were able to steal the bank's operator credentials, which allowed them to make the fraudulent transactions on the messaging interface connected to the SWIFT network. This was not due to a vulnerability in the SWIFT network, as the attackers simply took control of a trusted computer to orchestrate the fraudulent transactions. The criminals then used malware to cover their tracks. The malware was able to doctor the bank's printed transaction confirmation messages in order to delay discovery of the transactions. The attackers also carried out the attack at the start of a long weekend in Bangladesh, further reducing the chances of the theft being discovered.

The criminals made several transfer requests to the Federal Reserve Bank of New York for it to transfer the Bangladesh bank's money, primarily to locations in the Philippines and Sri Lanka. Four requests to transfer $81 million to entities in the Philippines successfully went through but a request to transfer $20 million to a non-profit foundation in Sri Lanka raised suspicions because the word foundation was spelled incorrectly. This led to the transfers being suspended and clarification being sought from Bangladesh, which was how the fraud was uncovered. However, by then the $81 million had disappeared, primarily into accounts related to casinos in the Philippines.

Most of that $81 million remains unrecovered; however, $15 million was returned by a casino in the Philippines to the Bangladesh central bank in November 2016.

The methods used in this attack, in particular the in-depth knowledge of the bank's SWIFT systems and the steps taken to cover the attacker's tracks, are indicative of a highly proficient actor. This was an incredibly audacious hack, and was also the first time strong indications of nation-state involvement in financial cyber crime had been observed, with the attack being linked to nation-state actors in North Korea.

Symantec's analysis of the malware (Trojan.Banswift) used in the attack on the Bangladesh bank found evidence of code sharing between this malware and tools used by Lazarus—a group the FBI claims has links to the North Korean government. This same group was also linked to two earlier heists targeting banks that make transfers using the SWIFT network, though the SWIFT network itself was not compromised in any of these attacks. Vietnam's Tien Phong Bank revealed that it had intercepted fraudulent transfers totaling more than $1 million in the fourth quarter of 2015, while research by Symantec also uncovered evidence that another bank was targeted by the same group in October 2015.

A third bank, Banco del Austro in Ecuador, was also reported to have lost $12 million to attackers using fraudulent SWIFT transactions, although no definitive link could be made between that fraud and the attacks in Asia.

At the end of 2016, more than 100 institutions in 31 countries, mostly in the financial sector, were targeted by a focused watering hole attack. With 25 targets, the main focus of the campaign was Poland, followed by the U.S. and Mexico. Analysis of the malware used in this attack (Downloader.Ratankba) revealed many similarities to the Lazarus group.

Odinaff

A campaign involving malware called Trojan.Odinaff was discovered to be targeting financial organizations worldwide in 2016. The attacks leveraging Odinaff were sophisticated and clearly carried out by a professional cyber criminal gang. While also targeting users of the SWIFT messaging service, there is no evidence linking these attacks with the Banswift attacks. In the Odinaff campaign the attackers again exploited weaknesses in banks' security to infiltrate their internal networks and compromise their operators and applications connected to the SWIFT network – however the SWIFT network itself was not exploited or compromised in any of these attacks.

Symantec research indicates that campaigns using Odinaff began in January 2016 and were focused on organizations in the banking, securities, trading, and payroll sectors. The Odinaff Trojan was typically deployed in the first stage of an attack to gain a foothold on the network.

Attacks involving Odinaff were highly sophisticated, requiring a large amount of hands-on involvement, with methodical deployment of a range of lightweight backdoors and purpose-built tools onto computers of specific interest.

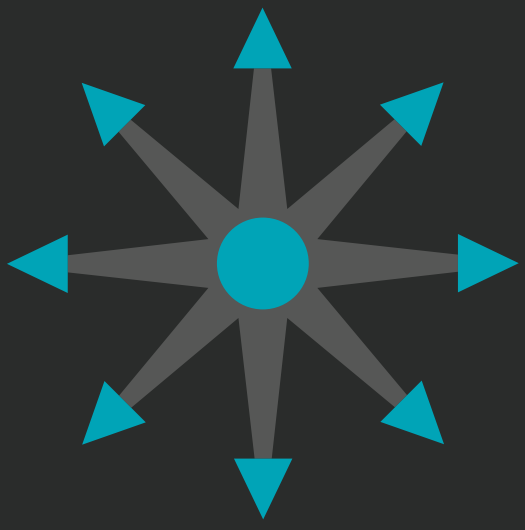
The Trojan was most commonly deployed in documents containing malicious macros, while botnets were also used to deploy it. The attacks were carefully managed, with the threat actors maintaining a low profile on the targeted organization's network, only downloading and installing new tools when necessary.

Tools used in the Odinaff attacks bear the hallmarks of the infamous Carbanak group, which has been targeting the financial sector since 2013.

Carbanak's activities were discovered in late 2014 and the group is believed to have targeted hundreds of banks in multiple countries, with estimates from some in the cyber security community of the money it has stolen ranging up to $1 billion. Symantec discovered multiple links between Carbanak and the Odinaff attackers; however, the infrastructure crossover is atypical, meaning it could be a similar or cooperating group if the Odinaff attackers are not part of the wider organization.

The Odinaff and Banswift attacks demonstrated that, while in 2016 many attackers moved back to utilizing existing tools and techniques such as spear phishing to target victims, there are still cohorts of extremely sophisticated cyber criminals deploying advanced campaigns for big financial rewards.

Infection, prevalence, and distribution



Section

02

Symantec

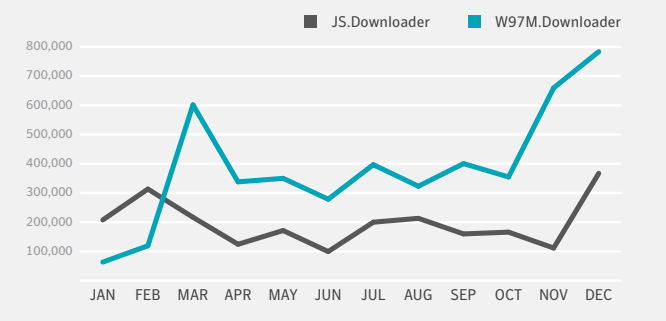
Infection, prevalence, and distribution

Infection vectors

Infection vectors for financial Trojans haven't changed much in the past year and are still identical to other common Trojans. Distribution mainly relies on spam email with malicious droppers attached and web exploit toolkits.

The use of scam emails was the most prevalent method of distribution for financial Trojans in 2016. The already well-known Office document attachment with malicious macros continued to be widely used. However, Microsoft Visual Basic Scripting (VBS) and JavaScript (JS) files in various attachment forms have also been used in massive spam runs to distribute malware. We have also seen Office documents without macros, and instead with embedded OLE objects and instructions for the user to double click the payload. The Necurs botnet (Backdoor.Necurs), which sent out more than 1.8 million JS downloaders on one day alone in November 2016, highlights the magnitude of some of these campaigns.

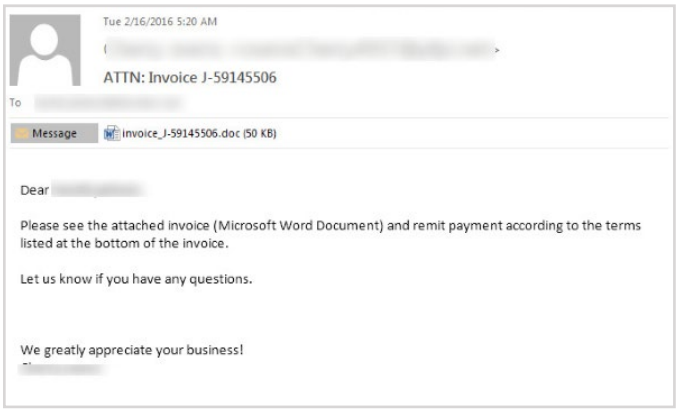
Document macro and JS downloader detections per month in 2016



Some of the groups are fast to adopt new exploits, for example on April 10, 2017 Dridex (W32.Cridex) used a just recently discovered zero-day vulnerability in Microsoft Word to infect thousands of users. Large waves of infected emails were sent out and opening the document infected the computer with a Dridex variant.

Other groups focus on the social engineering. We have seen phishing emails personalized using names and other information obtained from data breaches. Some of the scam emails were even sent out by legitimate well-known email service providers (ESP) offering email marketing and transactional email services. As pointed out by GovCERT Switzerland, this can increase the chances of such emails reaching the user's inbox. In the case of Dridex, the spam email was constructed very convincingly and lead to a malicious JS downloader.

Typical lure email with malicious document attachment



Phishing emails, where the victim is lured to fake websites that trick them into revealing their account details, decreased to just 1 in 9,138 emails in March 2017. In 2016, the average number of phishing emails was slightly higher than 1 in 3,000 emails. Simple phishing no longer works against most banks and financial institutions, as they rarely rely on static passwords alone. However, phishing attacks can still be successful in stealing online retail account credentials and credit card details.

Web exploit toolkits varied a lot over the year. Angler was the most active exploit toolkit in January 2016. Then, in March, Spartan took the crown, only to be once again overtaken by Angler in May. July was the month where Neutrino was the most active exploit toolkit and the rest of the year belonged to RIG. In March 2017 RIG was responsible for 13.6 percent of all exploit toolkit activity, a slight decrease from 25 percent of all activity in February, but still leading the group ahead of SundDown and Magnitude. In March 2017 we blocked 584,000 web attacks per day, most of them related to financial Trojan and ransomware droppers. The number of malvertising campaigns, where infected web ads are used to redirect the user to a web exploit toolkit landing page, increased slightly in 2016.

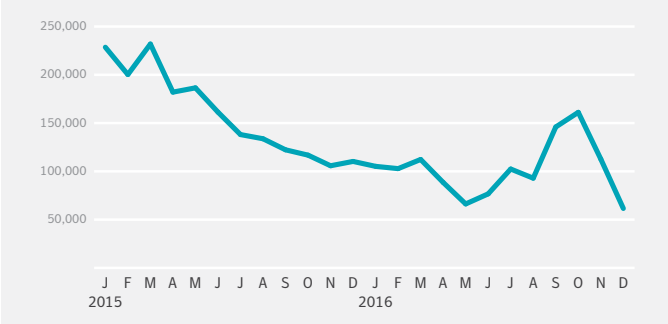
If you want to learn more about these infection vectors, we recommend reading last year's whitepaper—Financial Threats 2015—which highlights the different techniques used by attackers to distribute financial threats. For many of the threat families there are dedicated research papers available from us or our research colleagues.

Prevalence

The financial Trojan landscape is in constant development and we see changes over time due to takedowns or shifts to newer versions. The most active threat families in 2016 were Ramnit, Bebloh, Snifula, and Zeus variants. The global number

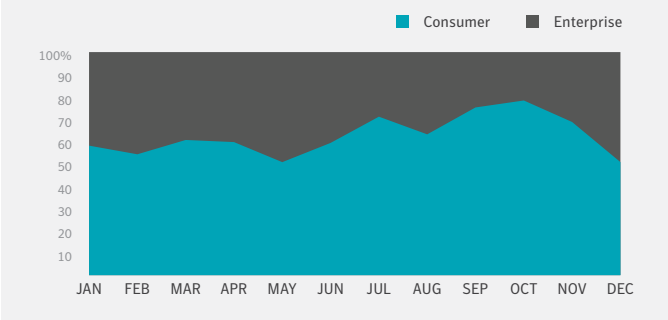
of attempted infections by financial Trojans continued to drop last year. We saw 36 percent less detections on endpoints in 2016 compared to 2015. And in 2015 we observed a 73 percent drop over the previous year. One of the explanations behind this decline is that security companies are becoming better at blocking the threats earlier in their cyber kill chain and more efficient in blocking spam runs. The successful detection of the dropper malware diminishes the infection numbers for the corresponding financial Trojan. Therefore the real number of malware that is spammed out to end users is larger than what actually makes it to the endpoint. The increase in detections around September and October 2016 was mainly due to an increase in Trojan.Bebloh activity in Japan.

Banking Trojan detections on the computer, 2016 and 2015



On average, 38 percent of all financial malware detections came from corporate computers. At the end of 2016 this increased to a high point of 49 percent. Of course many of these infection attempts are simply collateral damage due to the wide net cast by many spam campaigns. But, as elaborated earlier, we have also seen an increase of targeted attempts to specifically infect enterprise customers with financial threats in order to defraud them of large sums of money.

Distribution of financial malware detections



Threat family distribution

Ramnit and Zeus, and its variants, continued to lose their market share in 2016, whereas other threats like Bebloh gained traction towards the end of the year. The publicly available Zeus source code has also lead to many spinoff projects over the years, resulting in a large number of groups using some variation of the original threat.

After a takedown operation against Ramnit in February 2015 the threat went dormant but then reappeared in 2016 and went on to dominate the financial Trojan landscape. Ramnit was detected at a high rate consistently for the whole year. Interestingly, as Ramnit was often distributed via the Angler exploit kit in the past, it did not show any drop in activity following the disappearance of Angler in the middle of the year. This indicates the actors behind the threat adjusted their infection techniques—for example there were reports of Ramnit being spread via email in the UK during this time.

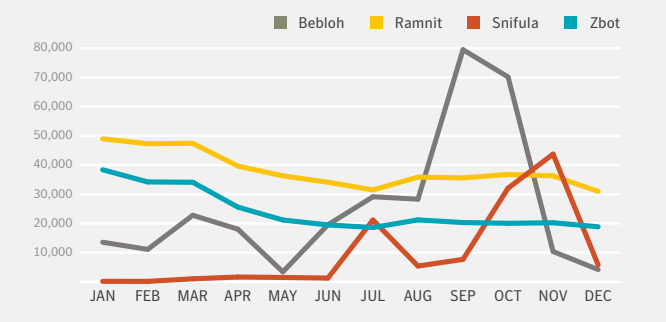
It should also be noted that some variants of Ramnit self-replicate, infecting executables and HTML files, which contribute to its prevalence. Some of these older infected files might have been dormant, but are still contagious and can start to spread again. For example in July 2016 a huge spike in Ramnit infections was reported in China. This was assumed to be related to older infected files being propagated once more. We have seen similar cases contributing to the infection numbers in Japan.

Number of financial threat detections in 2016 and 2015

Threat	Compromised computers in 2016	Compromised computers in 2015
Ramnit/Gootkit	~460,000	~779,000
Bebloh	~310,000	~13,000
Zeus/Citadel & variants	~292,000	~960,000
Snifula/Vawtrak	~122,000	~4,500
Dridex/Cridex	~23,000	~62,000
Dyre	~4,500	~55,000
Shylock	~4,500	~14,000
Pandemiya	~3,500	~600
Shifu	~2,000	~200
SpyEye	~1,500	~3,500

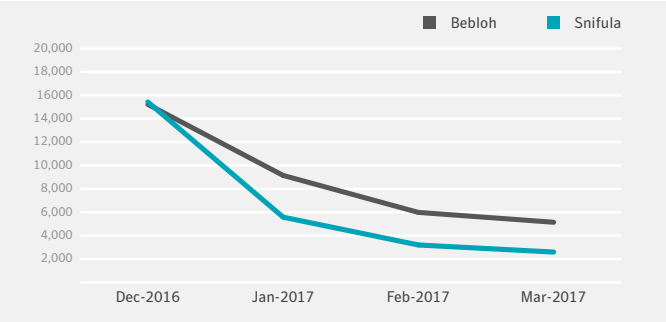
Bebloh, which occupies second place in the top financial Trojans list, was aggressively spread which lead to an increase of over 23 times the detection count over the whole year. In September and October we saw large spikes caused by Bebloh infections, particularly with email campaigns focused on Japan.

Monthly detection count for top four threats in 2016



As previously mentioned, takedowns can change the threat landscape tremendously, as can be seen by the near disappearance of the Dyre and Shylock (Trojan.Shylock) Trojans in 2016. The dismantling of the Avalanche malware-hosting network at the end of 2016, which was also used by Bebloh, resulted in a sharp drop in Bebloh activity beginning in November. After the arrest of the alleged author behind Trojan.Snifula in January 2017, we saw a drop in detections of Snifula as well. Both of these events lead to the dropping of detection numbers, for Bebloh by 66 percent from December 2016 to March 2017, and for Snifula numbers dropped by 83 percent in the same time frame. Now these threats appear to have almost vanished.

Detection numbers for Snifula and Bebloh in Q1 2017

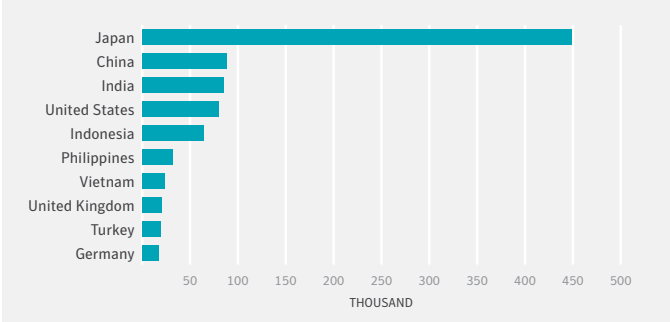


Geographical distribution

As discussed, the quantitative detection rates for each country heavily depend on the threat group and the time period of the group activity. Some of the threats have a very narrow geographical focus and are not distributed around the globe while other groups move from country to country in waves.

There are two notable trends that stand out when analyzing the financial threat distribution per country. For one, there is a large increase of detections in Japan. There was a more than 11-fold increase in the detection count for Japan in 2016, making it the most attacked country globally. The other noticeable trend was that attacks in the U.S. decreased by 26 percent, dropping the country to the fourth most attacked country globally.

Computers compromised with banking Trojans, by country 2016



Of course it should be clear that financial threats are a global problem and no country is really safe from them. Smaller countries may not make it to the top 10 list in terms of total detection numbers, but relative to the connected population, the risk can still be substantial. For example IBM reported in September 2016 on Dridex attack waves that, among other countries, focused on Latvia, a country which in the past has not been a priority for financial threat gangs.

Countries ranked by percentage of global detections seen per year

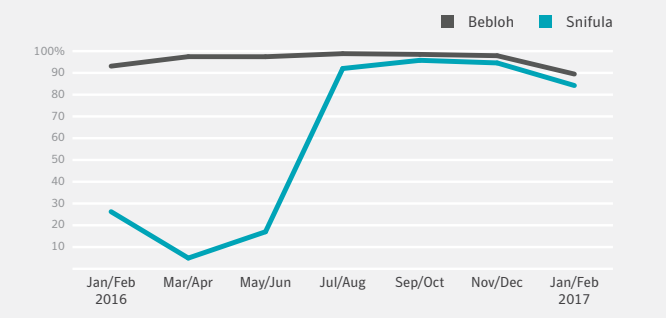
Region	Percentage of global detections 2016	Percentage of global detections 2015
Japan	36.69%	3.21%
China	6.92%	4.69%
India	6.37%	6.31%
United States	6.30%	8.54%
Indonesia	4.78%	6.31%

Japan in focus

In our Financial Threats 2015 paper we had already seen a spike in attacks against Japan and correctly predicted more would follow. We have seen a large increase in financial Trojan detections in Asia with Japan, China, India, the Philippines, and Vietnam all gaining places in the top 10 list. This shows that the attackers are trying to expand to less saturated regions, which may also be less protected.

We have seen Bebloh and Snifula specifically focusing on financial targets in Japan, which helped drive up the infection count for this country. More than 90 percent of the Bebloh detections seen globally where in Japan. In January 2016, 30 percent of Snifula detections were in the U.S., however, it shifted focus in the second half of the year when more than 90 percent of the detections for this threat were in Japan. It is unclear what motivated the shift.

Detections in Japan as a percentage of global detections, grouped by two months in 2016.



At least 19 financial institutions in Japan have been targeted by Snifula and Bebloh. As has been noted by others as well, it is interesting to see that both threat families seem to be using the same webinjects and target almost the same list of URLs. This could likely be an indication that both groups are using the same service for creating webinjects.

If we look at the individual samples, one Bebloh sample alone was responsible for 47 percent of all global detections in January 2016. The five most active Bebloh samples together represented 93 percent of all global detections in January 2016. These five samples also make up 90 percent of all detections in Japan for this period. In December 2016, the same five samples were still responsible for 0.6 percent of all global detections. This shows the attackers did not change the sample very often and did not deploy sophisticated polymorphic runtime packers for their final payload.

All these samples were spammed out in simple emails disguised as documents from a scanner with one of the following double extension file names:

- scan(2).doc.2016.01.20.PDF.exe
- scan01_doc_2015~jpeg.jpeg.exe
- IMAGE(1).15_02_2016_PDF_PNG.PDF.EXE
- image_n_(1) 20160217_PNG,PDF.png.exe

A similar situation can be found with Snifula, where the top five samples in December 2016 made up 94 percent of all global detections. Remarkably similar to Bebloh, these samples were spammed out in email waves with one of the following double extension file names:

- MX_20161031_1530380.JPG.exe
- 43894370932861.html.exe
- IMG_20161020_095456~1.jpg.exe
- ID654093871066.PDF.EXE

As previously discussed, both Bebloh and Snifula declined considerably at the beginning of 2017 following disruptions by law enforcement.

Distribution in relation to configuration

While analyzing three Dridex samples, which had the same configuration file and most likely came from the same spam run, we noticed something interesting: they each target the same 16 financial URLs in Germany and 10 in Austria. Looking at the top five countries where we have seen these samples reveals an interesting pattern. As expected, they have all been seen in Germany and Austria but these two countries were found to be the most prevalent locations for only one of the three samples. The samples were also observed in the U.S., which could be explained by a VPN or internet provider using IP addresses in that country. However, it is questionable if that explanation can be used to explain the infections in Israel and the Philippines. All that can be said is that, likely due to the

chosen distribution pattern of spam email, the attacks are not as well targeted as we would have expected. Of course three samples is not a representative set for the thousands of spam runs, but we have found that this holds true for many of the samples that we looked at. This highlights how far the samples are spread really depends on the threat family and the criminal group behind it. As we have seen, some Bebloh variant detections and targets may be nearly all in Japan, whereas the discussed Dridex samples have a wider distribution.

Regional distribution of the three Dridex samples discussed

	Sample 1	Sample 2	Sample 3
United States	42.7%	8.7%	89.4%
Germany	22.9%	26.1%	2.1%
Austria	16.7%	34.8%	3.4%
France	7.3%	17.4%	3.9%
Israel	10.4%	0.0%	0.0%
Philippines	0.0%	13.0%	0.0%
China	0.0%	0.0%	1.3%

Analysis of targeted institutions

In 2016, we observed many attack groups focusing on specific geographical locations. Therefore some of the threats might not play a significant role on a global level but can be very active in smaller markets.

We analyzed 684 samples from four threat families: Dridex, Snifula, Panda Banker (Trojan.Exedapan), and Trickbot (Trojan.Trickybot). This revealed 301 unique URL patterns from 132 institutions in 17 countries that the malware was monitoring for. If we focus on countries that are common to all the samples analyzed, 79 percent attacked at least one financial institution in the U.S., making it the most targeted country by institutions, followed by Poland and Japan. On average, each sample targeted 37 different institutions.

Most targeted countries based on URLs in webinject configuration

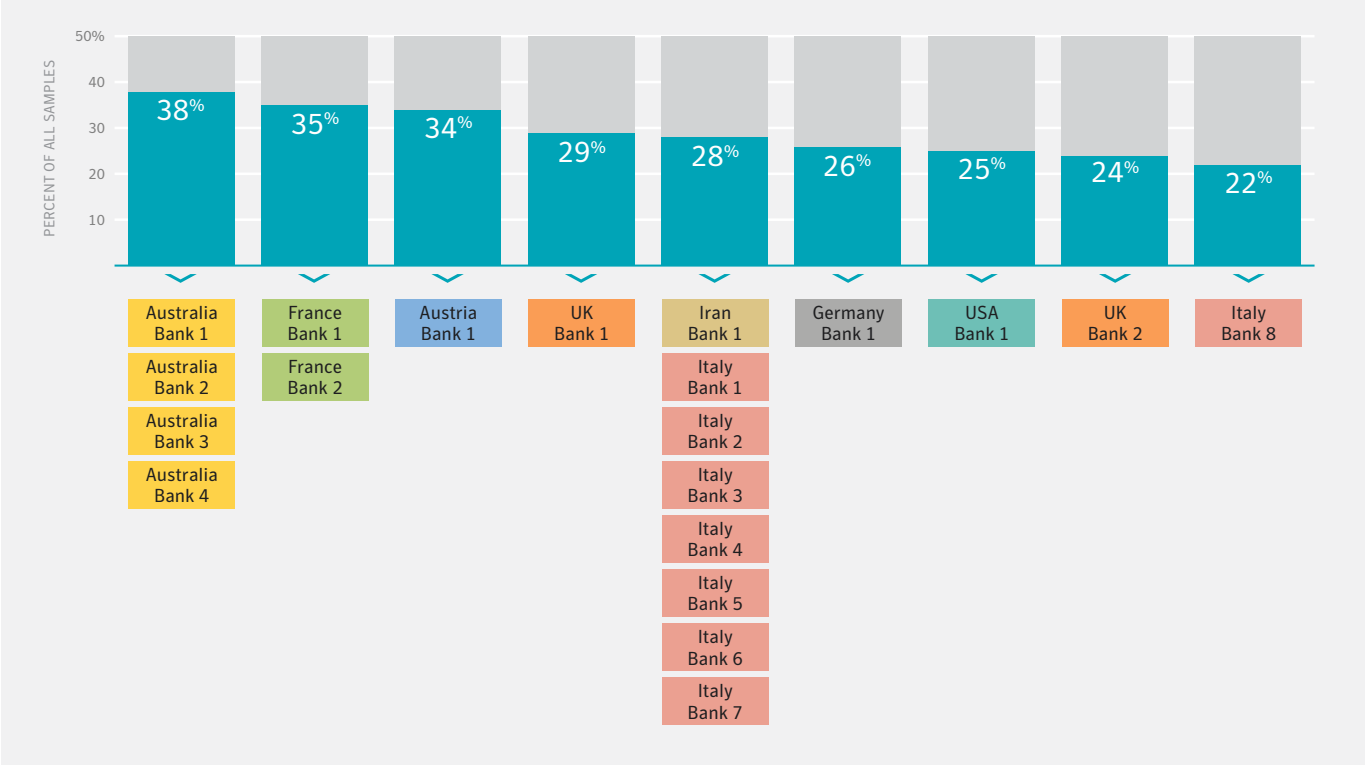
Rank	Country
1	United States
2	Poland
3	Japan
4	Australia
5	New Zealand
6	Germany
7	Austria
8	United Kingdom
9	Canada
10	Italy
11	Iran
12	China
13	Spain
14	Tonga
15	France

Unfortunately the list of targeted banks and countries is very dependent on the individual spam runs of the cyber criminals. A country can be ranked on top one month and disappear from the top 20 the next month. For instance, we have seen attack waves where criminals switched overnight from attacking Australia and New Zealand to attacking Germany and the UK.

Furthermore, as we will discuss later, we have noticed a trend for threats to redirect traffic completely or to use dynamic injects from a remote server. These samples will redirect traffic from any visited website that contains the word "bank" in the URL. This means the malware will not download the full configuration file to the client, keeping this information from researchers. In addition to this we have seen some malware authors hiding their implants completely. Previously configuration files of financial Trojans always contained a list of URLs of interest stored in an encrypted file. However, we have seen new variants of Blackmoon (Infostealer.Boyapki.E) that only store the SHA1 hash of the URL, concatenated with a unique salt value. This makes it almost impossible to reconstruct a complete list of targeted URLs.

Nevertheless, if we take all the samples we analyzed and weight them according to their prevalence, then we see that four banks headquartered in Australia were in 38 percent of all the samples, making them to most attacked financial institutions in our sample group.

Top targeted financial institutions in sample group



Top 10 countries targeted by Android.Fakebank.B

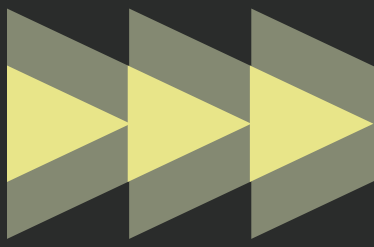
Rank	Country	Percentage
1	United States	17.16
2	Turkey	11.24
3	France	10.65
4	Germany	9.47
5	Australia	7.10
6	Thailand	5.92
7	United Kingdom	5.92
8	Poland	5.33
9	Austria	4.73
10	Russia	3.55

The country distribution is slightly different for the mobile threat landscape. The analyzed samples of mobile malware Android.Fakebank.B target 169 different mobile applications from 24 different countries. With 29 targeted institutions based in the U.S., this country is targeted the most, followed by Turkey and France.

Tactics, techniques, and procedures

Section

03



Symantec

Tactics, techniques, and procedures

Most financial threats deploy a general set of modules for various tasks such as taking screenshots or videos, keylogging, form grabbing, or installing SOCKS proxies and remote access tools like hidden VNC servers. Many attackers use free SSL certificates to protect their infrastructure. Some variants of Snifula (aka Vawtrak) now even implement SSL pinning for their command and control (C&C) infrastructure, making them more difficult to monitor.

Modern malware often deploys various anti-debugging tricks in an attempt to make analysis more difficult. Process hollowing and injecting into system processes is still a very common tactic used by malware authors to try and remain hidden on infected computers. The use of dynamic API resolution and checking for user land hooks as methods to attempt to bypass security tools has increased as well.

Source code merging

The financial malware ecosystem is constantly evolving. Besides the availability of financial malware as a service, which is helping to lower the entry barrier for aspiring cyber criminals, there are also quite a few new families being created. Since the source code of many threat families has been leaked in the past it is easy for attackers to modify or even combine them to create new malware families. Examples of this include Goznym (Trojan.Nymaim.B), a crossbreed of Nymaim and Gozi ISFB, and Floki Bot (Trojan.Flokibot), which is based on Zeus code. Unfortunately this uncontrolled growth makes it difficult to clearly distinguish between threat families as new variants could be a simple evolution or an entirely new branch utilized by a new group.

Sandbox evasion

Malware authors are wary of their creations being analyzed with automated analysis tools. Hence virtual machine (VM) and sandbox detection have become a standard feature among malware. We have reported in the past on the various methods used for detecting and bypassing sandboxes. In 2016, 20 percent of malware was able to detect and identify the presence of a VM environment, an increase from 16 percent in 2015. Some threat families, such as Zeus and Dridex, are more cautious in virtual environments than others, unlike Snifula, which rarely stops executing on VMs.

Percentage of VM aware samples in 2016 per family

Threat family	Percentage of samples that are VM aware
Ramnit/Gootkit	5.97
Bebloh	6.82
Zeus & variants	39.65
Snifula	1.59
Dridex/Cridex	34.27

Most script downloaders, even the ones in Office macros, are able to detect sandboxes through delays and environmental checks and deny execution if needed. Of course, bypassing a sandbox is not the same as detecting a virtual environment. Goznym checks the current date, which has to be close to the real date of the infection campaign. This ensures that only fresh samples execute and hinders later attempts at analysis.

If the threat manages to bypass the gateway and execute on the computer it will often attempt to kill any process related to security tools. Some even try to sabotage the update process or add themselves to the exclusion list, as recently observed in a Dridex variant. However, these methods do not work against Symantec's products.

Remote desktop access

A popular method used by attackers to carry out fraudulent transactions is to open a remote session to the compromised computer. Some attackers simply enable the Windows Remote Desktop Protocol (RDP) allowing them to connect to the compromised computer. Other threats, such as Dridex and Ramnit, have the capability to deploy a virtual network computing (VNC) module that gives the attackers full remote control over the compromised computer. While VNC on its own is not malicious and is often used by system administrators for legitimate purposes, it gives criminals access to a hidden virtual desktop so that their activities go unnoticed by the user.

This attack method works well against device fingerprinting protection, as the attackers are using the victim's computer to carry out the fraudulent transactions. Hence the only chance for the anti-fraud team to notice the attack is by analyzing the transfer patterns and transaction history.

The same method can also be applied if the compromised computer belongs to the finance department of a company. Dridex and other families check for the presence of interesting software tools that may signal the computer is of interest and will assign a manual scam operator if this is the case. This approach will be discussed in more detail in the Targeted financial heists section.

Diversion

Cyber criminals can also combine attack methods to create a diversion. In last year's white paper we discussed how attackers are using distributed denial of service (DDoS) attacks to keep the banks busy, while the criminals empty customers' bank accounts. Other groups, like Dyre, block access to the bank's online banking website with a DDoS attack so that customers are unable to verify if their account has been hacked. In some cases this is paired with a phone denial of service (DoS) attack against the support hotline.

Recent leaked documents published by Wikileaks suggest that nation-state attackers were using the Carberp malware source code to create their own modified malware variants. As mentioned in last year's white paper, we have seen APT groups using Trojan.Zbot in their attacks for similar reasons. These cyber crime toolkits are quite sophisticated and therefore it makes sense to copy them. At the same time the use of common malware allows the attackers to blend in with the masses without raising suspicion should the attack be detected—most organizations do not investigate further if common threats such as Zbot or Carberp are detected.

Webinjects

Webinjects allow malware to modify data in the browser before it is displayed to the user and before it is sent to the service provider. In the past, JavaScript-based webinject commands were stored encrypted on the local computer and would start when a specific URL was triggered. Most modern webinjects can load the final payload from a remote server, which allows for dynamic adaptation for the specific target. The accounts of the money mules are loaded in real time when needed and replaced with fresh ones if any are blocked. Any encountered errors are sent back to the malware authors, who quickly adapt the injected scripts to handle any new defense measures implemented by the financial institutions.

The injected scripts can also mimic the user's behavior and add delays between filling out forms and submitting them, making it more difficult to spot the scam on the backend.

Redirection method

Since an increasing number of security tools monitor and block any injection into a web browser, quite a few financial Trojans have changed their behavior in an attempt to evade local detection. Instead of injecting into the browser they try to redirect network traffic to a website they control. While this type of traffic redirection was a trick deployed by banking Trojans in the early days, it is now experiencing a comeback. In 2014, Dyre was one of the first groups to start focusing on redirection again.

Some variants of Ramnit have started to create their own local proxy in order to redirect web traffic through it. The threat still needs to inject a module into the browser in order to be able to redirect the traffic but that uses different APIs. The threat also hooks the certification validation API in crypt32.dll, enabling it to listen into SSL communications as well and suppressing error messages from the user.

Another popular method is to change the DNS server—sometimes referred to as pharming. This simple method is widely used in Latin America. As an example, Infostealer.Banprox.B modifies the default DNS server and also installs a rogue root certificate in order to suppress SSL warnings.

Blackmoon, which is mainly active in South Korea, can modify the local hosts file, redirecting specific domains to a remote server under the control of the attacker. This malware also sets new DNS servers and flushes any cached DNS resolver pairs. The idea of using the hosts file as a redirector is definitely not new, but we have seen an upward trend in the use of these old-school methods. Some Dridex variants poison the local DNS cache by adding a malicious entry for certain domains, resulting in the same effect.

Other variants of Blackmoon have used Proxy Auto-Config (PAC) configuration in order to automatically modify the browser's proxy settings for certain URLs. While others use PowerShell scripts to modify the system and browser proxy and DNS settings.

It's not just since the rampage of the Mirai IoT botnet that attackers have known that routers are an easy target. Instead of using compromised routers as a DDoS attack weapon, some attackers simply switch the DNS server in order to perform MitM attacks. For example, we blogged about such attacks against routers in Mexico back in 2008.

Sometimes the attackers get lucky and hijack whole DNS servers, such as in October 2016 when a Brazilian bank lost control of all of its online presence for five hours, allowing attackers to redirect customers to fraudulent websites.

The redirection is not always limited to a small set of targeted URLs. In June 2016 we saw Trojan.Retefe attacking UK customers. Besides a dozen hardcoded URLs, the threat also redirected any connection to a .com or .co.uk domain to the malicious proxy. Allowing the attackers to expand their reach significantly.

All of the above mentioned redirection methods will lead to the user ending up at a fake website created by the attacker or a transparent proxy that can modify the traffic in both directions. This also means that the logic of the webinjects rests on

the remote server and therefore is more difficult for security researchers to analyze.

Of course, keeping a collection of fake websites updated is a lot of work for attackers, but it pays off. One of the big disadvantages for attackers is that the traffic to the bank is now coming from a different IP address (unless it's a local proxy), and too much traffic from the same address can raise suspicion.

Session hijacking

Some online services solely rely on session tokens or cookies once the initial authentication is made. Some threats will steal valid tokens and send them back to the C&C server. An automated script can then use the token to log into the bank and issue transactions. In order to mimic the user's browser as best as possible the attacker can clone the browser user agent and other identification attributes like screen resolution. However, the IP address will still be different and can be picked up by anti-fraud backend systems. In order to bypass such checks, attackers can use a hidden instance of the same browser on the compromised computer or install a proxy and bounce the transaction through the victim's computer.

Fileless load points

Following the trend of leaving less obvious traces on compromised systems, we have seen financial Trojans beginning to use fileless load points. For example, some Ramnit variants make use of hidden load points by using a Group Policy Object (GPO). Older versions registered a scheduled task to load the watch dog DLL every minute or created a Windows service entry with a randomized name.

In early 2016, some variants of Ramnit used their loader DLL to download the actual payload from the internet over SSL. This on its own is nothing new, as SSL has been used to add another layer of obfuscation for some time now. The interesting part is that the downloaded payload is stored as an XOR encrypted blob inside the Windows registry. The loader thread, which typically runs inside explorer.exe, can then decrypt the payload from the registry and inject it into the process.

Overlay forms

Some minor threats have been experimenting with window overlays. In this technique the Trojan waits for the user to visit a specific online banking service or open a dedicated banking application. It then creates a fake window which is placed on top of the original form. With this, the user is asked to enter their account credentials, which are then stolen. As the threat does not need to hook the browser or get notified about the URLs, it doesn't ring any anti-hooking alarms. Although not commonly used by desktop-based threats, this method is widely used by mobile threats.

AtomBombing injection

At the beginning of 2017, Dridex started to distribute a new version (version number 4).

One of the most notable changes was that the threat started using so-called AtomBombing to inject malicious code into the target process. This method has been known for some time but it is the first time we have seen it used by a financial Trojan. As this method has generated much discourse, we will discuss it here in more detail. AtomBombing relies on Windows atom tables, or more specifically on the NtQueueApcThread and NtSetContextThread APIs.

Commonly a threat would use the VirtualAllocEx API to allocate a buffer in the remote target process. It would then copy the payload with the WriteProcessMemory API to the allocated buffer. Finally, the payload is executed with a call to CreateRemoteThread.

With this method the threat can write the payload to the Windows atom table with GlobalAddAtomW and then use, for example, the NtQueueApcThread API to have the remote process call GlobalGetAtomW to load the payload from the table and write to its own memory. This allows for indirect writing to the target memory space.

Next step is to remotely execute the written payload (Dridex uses NtProtectVirtualMemory to achieve this). Another method, which was described in detail by enSilo in 2016, is to use an ROP chain to allocate an RWX memory region and copy the payload there before jumping to the RWX memory and executing the code.

Other threats like Shifu (Infostealer.Shifu) make use of atoms to check if an instance is already running, instead of the more common method of using mutexes.

Symantec's behavioral detection engine has been monitoring these calls for many years and is able to block AtomBombing injections (detected as SONAR.ProcHijack). The use of this new technique is another sign that security products are protecting against the usual process injection methods and attackers are scrambling to find new tactics.

Social engineering attacks

Social engineering plays a large role in most financially motivated attacks, either during the infection phase or when overcoming multi-factor authentication. There are also some types of attacks that do not require any malware and rely solely on social engineering. We have discussed business email compromise (BEC) attacks in the past, where scammers send convincing emails to the finance department trying to convince them into transferring money.

The social engineering tactics used in BEC scams continue to evolve. For example, there has been an increase in attacks where email servers are being compromised or scammers are registering similar looking domain names to those used by targeted organizations. The scammers then wait until the time of the month when the target organization sends out its invoices and then either switches the account number on the fly or sends a second email from a lookalike domain with a slightly modified invoice and a note that the account number has changed. As the customer is expecting an invoice from the organization, the scam is even more convincing. We expect these low tech scams to keep evolving.

What are they stealing?

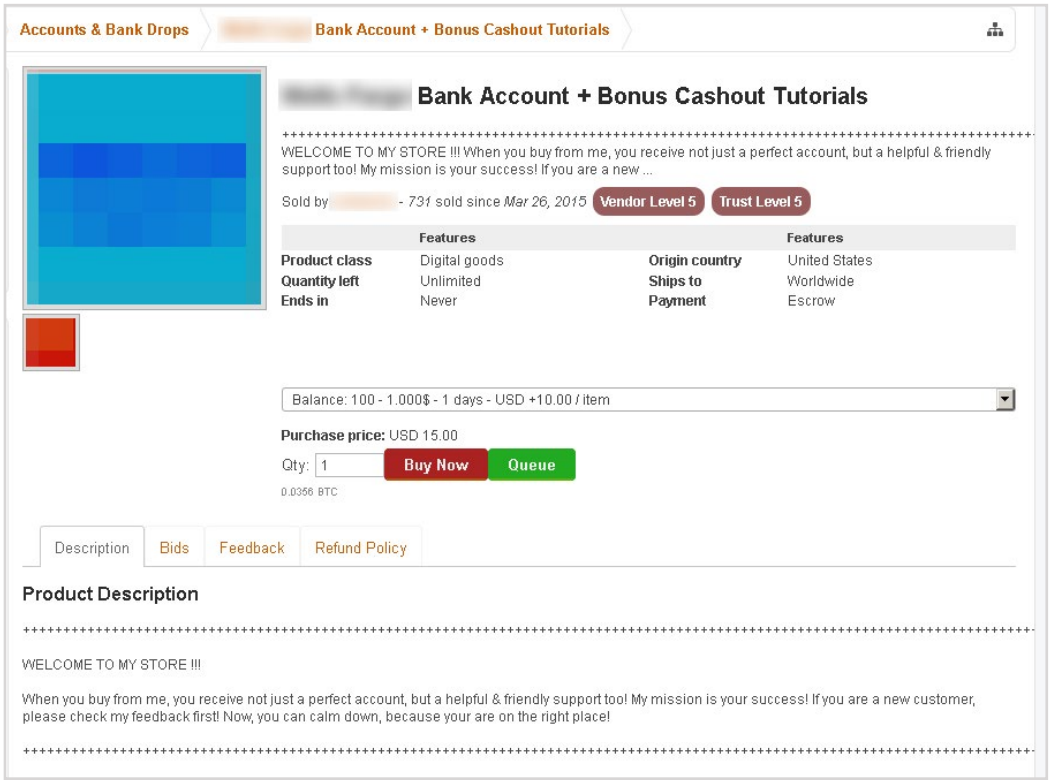
Once a financial threat has compromised a computer it will steal any credentials that will help the malware operators maximize their profits. Besides stealing online banking credentials, they may search for other passwords as well.

It is common for financial threats to steal any other account information that they can find on a compromised computer. After all, the attackers want to make profits and stolen accounts could help spread their malware further or be sold on underground forums. Ramnit, for example, steals account credentials for various administration tools and FTP clients. Crypto currencies such as Bitcoin are commonly targeted as well. We have also seen several samples stealing online retail access, auction platform account credentials, online game credentials, and login data for music and video streaming services. This is also reflected in popular underground markets where we have seen an increase in such account credentials being offered for sale.

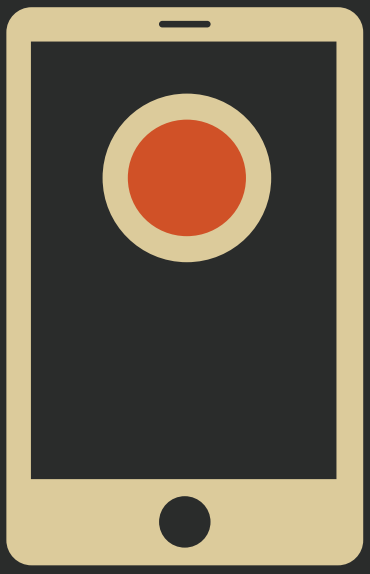
The majority of digital goods offered on publicly accessible underground forums and dark web TOR sites remained stable since last year. Credit card details are still the most sold digital goods on underground forums. Bank account access information is priced according to the account balance. For example, an account with $1,000 in it can be sold for $10. An account with a greater balance will be on sale for a larger sum.

Symantec observed an increase in offers for money transfer services, which were being sold for around 10 percent of their value—for example pay $100 in bitcoins for a money transfer of $1,000. This indicates that the process of cashing out the stolen money is still the most difficult step in the chain for cyber criminals.

Underground advert for bank account logins



Attacks against ATM, POS, and mobile



Section

04

Symantec

Attacks against ATM, POS, and mobile

ATM and POS

ATM and point of sales (POS) attacks continued to increase in 2016. ATM malware has been around for 10 years but is still effective. With the increase of targeted attacks aimed at banks, we also saw an increase in attacks against ATMs from within the financial network. There are many active ATM and POS threat families, such as Ploutus (Backdoor.Ploutus), Flokibot, Trojan.Skimer, FastPOS (Infostealer.Fastpos), Infostealer.Poslit, Infostealer.Donpos, Infostealer.Jackpos, Infostealer.Scanpos, and Backdoor.Pralice to name just a few. Since the adoption of Chip & PIN has begun to spread outside of Europe, we have seen a decrease of classic memory scraping threats, as they are no longer efficient for the attackers.

There are various degrees of sophistication seen in the wild when it comes to ATM attacks. For some attacks the criminals need physical access to the ATM computer and they get this by opening the cover with a stolen key or picking the lock. Once they have access to a USB port or the CD-ROM they can install malware and attach a keyboard to issue commands (the Ploutus malware uses this attack vector).

Similar attacks have been reported in hotels where attackers used the often exposed USB ports on the backside of the check-in computers to install malware. Or in retail stores where the attackers added their sniffer to an exposed network port inside the shop. This allows them to compromise any attached POS device and scrape the memory for payment card information.

With physical access to the ATM another attack vector is possible. As reported in April 2017, some attackers discovered they could drill a hole into the ATM casing in order to access to the internal bus system. Once access is obtained, a cheap microcomputer is all that is needed to send commands to the bus in order to make the ATM dispense its cash.

Physical access is not required for all ATM and POS attacks. In November 2016, the FBI warned about the Buhtrap group breaking into financial institutions' internal networks and issuing ATM commands that lead to the dispensing of money, all without physically tampering with the ATMs. The Taipei police estimates that the cyber attacks may have led to $300 million in losses. In another case, attackers were able to install the ATMitch malware on multiple ATMs, and cash out at least $800,000.

The same applies for POS attacks, which can also be carried out remotely. For example, Trojan.Flokibot was going after POS computers which process payment card transactions. Attackers compromised computers using spear-phishing emails and then used TeamViewer and Ammyy Admin software to remotely control the compromised computers and progress with their attack.

In August 2016, the website of a POS software vendor was compromised. According to reports, the stolen information could have provided the attackers with remote access to POS systems in use at various retailers. The revelation lead to the vendor issuing a password reset for support accounts on all affected systems.

Android financial threats

Since the introduction of mobile banking apps and two factor authentication (2FA), cyber criminals have had to look for ways to either bypass 2FA using social engineering or by attacking the mobile platform. For the past few years financial threats on Android phones have become increasingly common, but the infection numbers and variety of families is still much smaller compared to the Windows threat landscape.

The detection numbers for mobile malware in general increased by 29 percent to 7.2 million in 2016. More than half of mobile malware detections are related to downloader threats, such as Android.MalDownloader. Besides generic detections, mobile financial threats is the third most common threat category, behind premium text message sending apps and ransomware. Most mobile threats do not require root permissions, but some download privilege escalation exploits, which allow the threat to steal cached passwords from the browser and other applications. A common tactic is to show the "Device Admin activation dialog" over and over again until the user grants admin permission to the app. At more than 20 percent, the rate of runtime packer usage in mobile threats more than doubled between January and December 2016, showing an increasing use of obfuscation.

The infection vector commonly involves social engineering and a spammed out link to the threat masquerading as a legitimate app. The attackers are Trojanizing legitimate tools and advertise them for download. Another avenue for distribution is on compromised websites where the malware poses as a movie player that needs to be installed to view content. The user is typically tricked into ignoring any security warnings and voluntarily installing the malicious app themselves. Attentively reading the requested permissions in the installation dialog is still one of the most effective protection methods and some apps have started to delay the request for permissions to a later point, where more social engineering can be applied.

Malicious apps is not only a problem found on third-party app stores. We still see infected apps appear on the official Google Play Store now and then. For example, in February 2017 an Android.Fakebank.B variant disguised itself as a weather

application called “Good Weather” on the official Google Play Store and was downloaded by approximately 5,000 users.

With the constantly evolving Android operating system we also see a constant change in the methods and tactics used by attackers. The main methods employed by financial mobile threats include SMS and call forwarding, fake form overlays, information stealing, and fake mobile banking apps.

Using fake form overlays is still a common tactic, although Android 6.0 made it more difficult for malware authors to use this method. Similar to their desktop counterparts, mobile threats can dynamically download an overlay from the C&C server that corresponds to the app that is launched or the website visited by the user. This overlay mask can then steal the login credentials or ask for additional information such as credit card details.

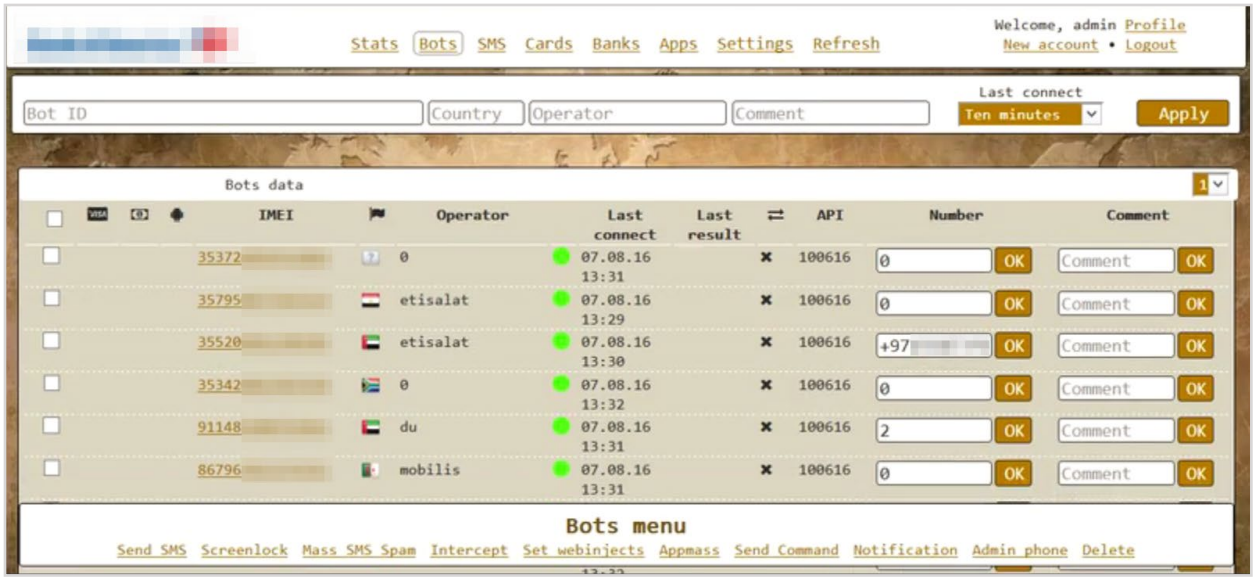
Mobile threats also target non-financial applications like social media apps or chat applications. We have seen some Android.Fakebank.B variants, also known as Marcher, targeting over 125 different institutions. In some campaigns the attackers spoof a text message from the bank asking the user to verify a fraudulent transaction, which serves to create some urgency and tricks the user into logging into the financial application right away.

Another tactic used by Android.Fakebank.B is adding itself to the Battery Optimizations exceptions whitelist so that the new doze feature in Android 6.0 does not stop the Trojan when it goes into battery saving mode. This allows the threat to stay connected to its C&C server. The same malware family was also seen in March utilizing call-barring functionality. This meant that the malware could block any outgoing call to a predefined list of customer service numbers (in this case numbers related to Russian and South Korean banks). This feature makes it more difficult for the user to verify or cancel suspicious transactions with the financial institute. This functionality is similar to a tactic used by the Windows malware Shylock, which replaced the bank’s customer support telephone numbers when a user visited the bank’s website with on an infected computer.

Sometimes attackers use simple tricks to achieve their goals. At the beginning of 2016, Android.Bankosy added a simple trick to intercept voice 2FA tokens (when the bank calls the customer and a synthetic voice reads the 2FA code to the user). The Trojan added call forwarding using the special service code *21*[DESTINATION NUMBER]#, which is supported by many telephone carriers. Once activated, the call back from the bank would end up at the VOIP number controlled by the attacker and they would have the 2FA code needed to carry out fraudulent transactions.

The crimeware-as-a-service model is also available for mobile malware. For example, a Trojan called Exo Android Bot was heavily advertised in forums in 2016. For $400 per week or $3,000 per year the author promised Android malware that could intercept SMS, use screen overlays, and had 24/7 support. The focus of the threat was clearly financial applications.

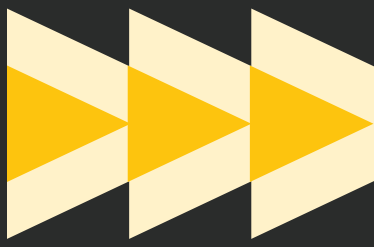
Control panel for a rentable mobile Trojan



Disruptions and takedowns

Section

05



Disruptions and takedowns

With increased collaboration between researchers and law enforcement agencies around the globe, there were a number of significant disruptions in the past year including several high-profile takedowns. These efforts not only helped put a dent in financial malware activity but also served as a warning to cyber criminals involved in this type of crime.

Dyre

One of the major takedown stories to break in early 2016 surrounded the Dyre financial fraud Trojan.

Reports emerged in February that a Russian law enforcement operation in November 2015 coincided with a major drop in activity from the financial Trojan. This is also reflected in the 92 percent drop in detection numbers for Dyre in 2016.

Dyre had grown to be one of the most active financial fraud tools in 2015. Dyre spam campaigns contained a malicious attachment that, if opened, would install the Upatre downloader (Downloader.Upatre) on a victim's computer. Detections of Upatre hit a high of more than a quarter of a million in July 2015. Detections of both Upatre and Dyre dropped sharply after the November 2015 takedown.

The circumstances surrounding the Dyre takedown are unclear, with no definitive evidence emerging about who or how many people were arrested. Reports in late 2016 claimed that new banking Trojan Trickbot was a rewrite of Dyre.

Avalanche

The Avalanche takedown dealt a severe blow to the cyber criminal community following the seizure of infrastructure used by multiple malware families. The takedown was a combined effort by multiple international law enforcement agencies, public prosecutors, and security and IT organizations, including Symantec. It resulted in the seizure of 39 servers and several hundred thousand domains that were being used by the criminal organization behind the Avalanche network.

Symantec's research into the Avalanche network began in 2012 when it published research on ransomware that was predominantly targeting German speakers in Germany, Austria, and parts of Switzerland. At the same time, German police were carrying out an investigation into the Bebloh malware, which featured in Symantec research. Symantec researchers provided technical assistance to the police during the investigation, and these combined efforts eventually led to the discovery of the Avalanche botnet. Avalanche was a massive operation responsible for controlling a large number of compromised computers around the world.

The investigation culminated on November 30, 2016, and resulted in the takedown of infrastructure providing support for at least 17 different malware families, as well as the arrests of multiple individuals suspected to be participating in the activity.

Arrests

In addition to takedown initiatives, there have been various arrests made in the past year. Russian security forces cracked down on the Lurk banking group in June 2016, arresting 50 people in Moscow and in January 2017, the suspected author behind Trojan.Snifula was arrested in Spain resulting in Snifula nearly disappearing completely. The Lurk banking Trojan targeted Russian financial institutions and the group behind it is believed to have stolen more than $25 million.

These arrests coincided with a drop in activity from a number of threat groups including Locky (Ransom.Locky), Dridex, and the Angler exploit kit. However, while Locky and Dridex experienced a surge in activity again in the second half of 2016, Angler did not. This led to speculation that the same people were behind both the Lurk banking Trojan (Trojan.Filurkes) and the Angler exploit kit. Since the Lurk arrests, Angler has disappeared from the threat landscape.

Conclusion

Section

06

Conclusion

Although the detection count for financial malware decreased in 2016 by 36 percent, this threat category is still very much active and relevant despite several takedown operations and arrests. The three major players for 2016 were Ramnit (aka Gootkit), Bebloh, and Zbot (aka Zeus), together responsible for 86 percent of all financial threat related activity. Surprisingly, most of this prevalence was achieved by a handful of samples. For example, one Bebloh sample accounted for 47 percent of all global detections in January 2016. This is a result of large spam campaigns with millions of malicious emails being spammed out. The infection vectors for financial threats are the same as for other common malware such as ransomware and we have seen many groups share the same spam botnets or exploit toolkits.

Japan was hit with 37 percent of all financial malware attacks in 2016, which demonstrates that attackers are fast in adapting to new markets when current targets become saturated, too well protected, or are no longer easily defrauded.

Sandbox evasion and anti-debugging tricks did not change in 2016. However, there was an increase in the use of redirection attacks—where victims are redirected to a remote site which will then perform the inline attack. This can make it more difficult to block the attack on the user's computer.

Another noticeable trend is the increase in attacks against corporations and financial institutions themselves. On average, 38 percent of all financial threat detections were in corporations. Once such an infection is identified by attackers, they will log in remotely and, over time, learn how transactions are conducted. Depending on the opportunities presented they may attempt to inject fraudulent transactions into the monthly invoice payment orders or, in the case of a bank, try and submit their own interbank transfers. Even though such attacks are harder to carry out and take longer to prepare, they yield a much higher profit. With the Lazarus group being linked to some high-profile bank attacks, it is the first time that a possible nation-state actor has been identified performing these types of financially motivated attacks.

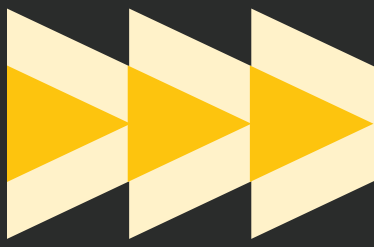
Mobile threats on Android are mainly focusing on form overlay attacks or fake online banking apps. We have seen more than 170 mobile apps targeted by mobile malware. Mobile threats are still relevant as many financial institutions have deployed two-factor authentication through mobile phone applications. As it has become more difficult to conduct such attacks on the latest Android OS, we have seen attackers reverting to social engineering attacks, where they trick victims into authorizing fraudulent transactions. The end user still remains the weakest link in the chain during an online transaction, which means even the strongest technologies are susceptible to social engineering attacks.

We expect financial threats to remain a problem for end users in the future, but attackers will likely increase their focus on corporate finance departments and using social engineering against them.

Protection

Section

07



Symantec

Protection

Adopting a multilayered approach to security minimizes the chance of infection. Symantec has a strategy that protects against malware, including financial threats, in three stages:

01 **Prevent:** Block the incursion or infection and prevent the damage from occurring

02 **Contain:** Limit the spread of an attack in the event of a successful infection

03 **Respond:** Have an incident response process, learn from the attack and improve the defenses

Preventing infection is by far the best outcome so it pays to pay attention to how infection can be prevented. Email and infected websites are the most common infection vectors for malware. Adopting a robust defense against both these infection vectors will help reduce the risk of infection.

Advanced Antivirus Engine

Symantec uses an array of detection engines including an advanced signature-based antivirus engine with heuristics, just-in-time (JIT) memory scanning, emulator, advanced machine-learning engines and reputation based detection. This allows the blocking of sophisticated threats, including directly in memory executed threats, at various layers.

SONAR Behavior Engine

SONAR is Symantec's real-time behavior-based protection that blocks potentially malicious applications from running on the computer. It detects malware without requiring any specific detection signatures. SONAR uses heuristics, reputation data, and behavioral policies to detect emerging and unknown threats. SONAR can detect malicious behaviors common to lateral movement and block them.

Email Security

Email-filtering services such as Symantec Email Security .cloud can stop malicious emails before they reach users. Symantec Messaging Gateway's Disarm technology can also protect computers from email based threats by removing malicious content from attached documents before they even reach the user. Email.cloud technology includes Real Time Link Following (RTLF) which processes URLs present in attachments, not just in the body of emails. In addition to this, Email.cloud has advanced capabilities to detect and block malicious script contained within emails through code analysis and emulation.

Sandbox

Sandboxes such as the Symantec Malware Analysis sandbox technology have the capability to analyze and block malicious content. It can work its way through multiple layers of obfuscation and detect suspicious behavior.

Network security

Monitor and block malicious traffic on the endpoint with Symantec Endpoint Protection or in the network with Symantec Secure Web gateway.

System Hardening

Symantec's memory exploit mitigation can protect against typical exploit techniques with an exploit agnostic approach. In addition, Symantec's system hardening solution called Symantec Data Center Security can secure physical and virtual servers and monitor the compliance posture of server systems for on-premise, public, and private cloud data centers.

Best Practice

In addition, users should adhere to the following advice to reduce the risk of cyber attacks:

- Exercise caution when conducting online banking sessions, in particular if the behavior or appearance of your bank's website changes
- Exercise caution when receiving unsolicited, unexpected, or suspicious emails
- Keep security software and operating systems up to date
- Enable advanced account security features, like 2FA and login notification, if available
- Use strong passwords for all your accounts
- Always log out of your session when done
- Monitor bank statements regularly
- Notify your financial institution of any strange behavior while using their service
- Be wary of Microsoft Office attachments that prompt users to enable macros

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure.

Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

More Information

Symantec Worldwide: http://www.symantec.com

ISTR and Symantec Intelligence Resources: https://www.symantec.com/security-center/threat-report

Symantec Security Center: https://www.symantec.com/security-center

Norton Security Center: https://us.norton.com/security-center

Symantec

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043
United Stated of America

+1 650 527–8000
+1 800 721–3934

Symantec.com

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745 6054.

05/17