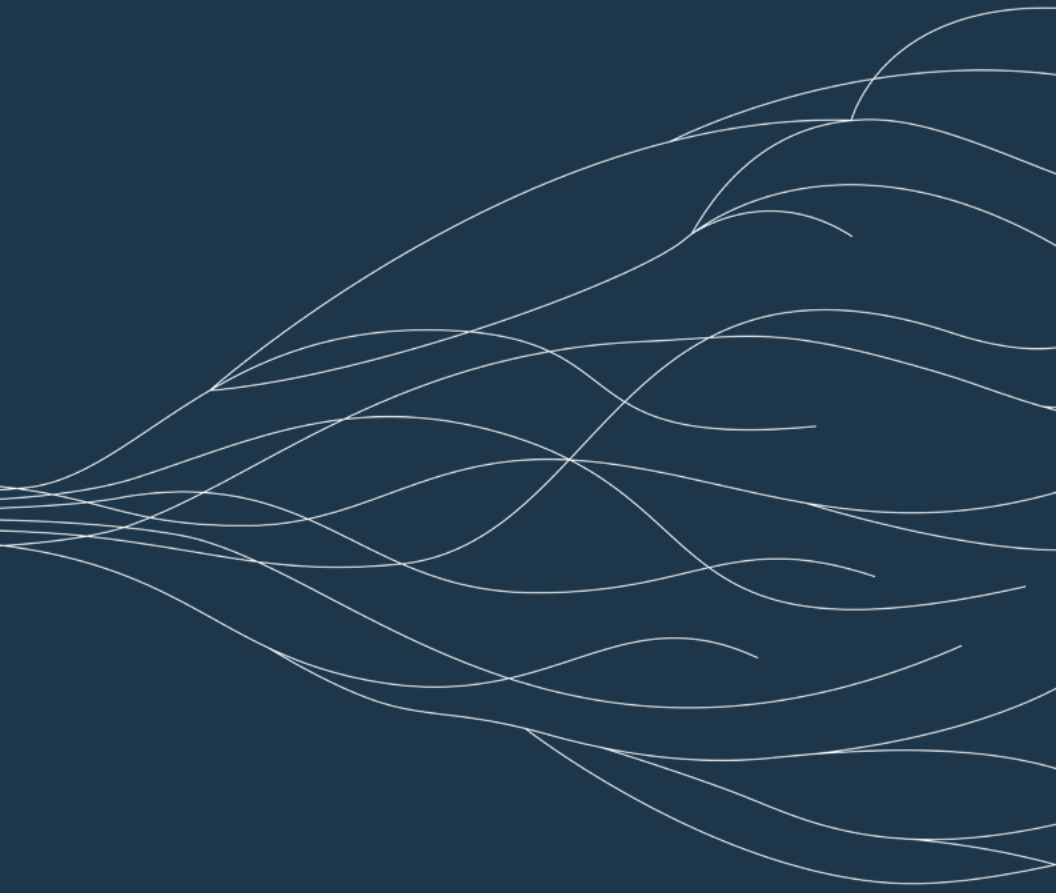


IBM Security

Financial malware shifts of 2017 and a look ahead

IBM X-Force Research – IBM Trusteer

IBM

Click here to start ►

Contents

Overview

Losses to cybercrime are a growing issue to banks and service providers across the globe. Numbers forecasted by different research firms quote Juniper Research expecting $2.1 trillion in losses by 2019, and up to $6 trillion by 2021 may be the global price tag, according Cybersecurity Ventures. These amounts are attention-grabbing and naturally urge organizations to take heed and plan for protecting their assets and customers.

A large part of the overall losses to cybercrime is generated by financial fraud and financially motivated attacks. Within that domain, banking Trojan-driven attacks have gradually turned into the playing field of organized crime groups – a trend that has become quite pronounced in the past three years.

IBM® X-Force® research tracks this type of cybercrime activity and indicates that, nowadays, when it comes to encountering new financial malware, most often it will feature sophisticated source codes, high-value targets, and grand-larceny capabilities that paint the picture of an organized operation rather than a small team or lone actor.

About X-Force

The IBM X-Force research team studies and monitors the latest threat trends including vulnerabilities, exploits, active attacks, viruses and other malware, spam, phishing, and malicious web content. In addition to advising customers and the general public about emerging and critical threats, IBM X-Force also delivers security content to help protect IBM customers from these threats. Threat intelligence content is delivered directly via the IBM X-Force Exchange collaborative platform, available at xforce.ibmcloud.com

Contents

As an example, groups operating the Dridex or TrickBot Trojans can easily include dozens of people in different roles and need-to-know levels. Other malware groups, like the operators of Gozi, for example, are considered crime-as-a-service operations, and can have links to an even larger number of actors in different geographical hubs. While it would appear that the financial crimeware arena has reached a somewhat predictable form, shifts that shaped 2017, and will likely affect 2018, show that it is still an evolving landscape. The following are notable observations from the 2017 financial malware arena:

- Gozi (Ursnif) topples Zeus from its number one position as most active financial malware.
- New financial malware emerges: IcedID and Ursnif V3, appear and remain limited in scope. Client Maximus rises in Brazil.
- Once notorious financial Trojans, Shifu, Neverquest, and GozNym, saw their demise, proving that only the fittest survive.
- Malware infection vehicles shift: the fall of the Andromeda botnet and continued rise of the Necurs botnet.

2017's most active financial malware families

Looking back at the most active financial Trojans in 2017 cybercrime shows that, for the first time, Zeus Trojan variants placed lower than Gozi in terms of activity for the year. This change provides another proof that cybercrime has moved on from the commercial and fly-by-night malware operators, and organized, business-like gangs are taking the lead in 2018.

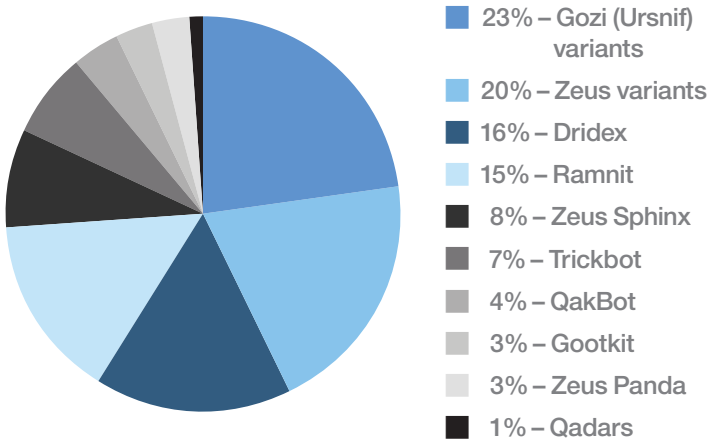


Figure 1. Top most prevalent financial malware families – 2017 (Source: IBM X-Force)

Contents

2017's newcomers

Since financial malware is only the tip of the iceberg in the organized cybercrime supply chain, it is not very often that new gangs arise. Most years will see one or two new malware codes at most, and that was case in 2017 as well with a new Trojan, IcedID, in the US and UK, and a new Ursnif (Gozi) iteration in Australia. Aside from those two global malware codes, Brazilian developers have been working to improve and spread the Client Maximus Trojan. More on each of these in the following sections.

IcedID emerges in US and UK

In September 2017, X-Force research discovered and analyzed a new banking Trojan that emerged in the wild. The malware was coined IcedID, and while the testing period started in September, actual infection campaigns did not take place until October 2017. Our researchers noted that IcedID features a modular malicious code with modern banking Trojan capabilities comparable to malware such as the Zeus Trojan.

IcedID targets banks, payment card providers, mobile services providers, payroll, webmail and e-commerce sites in the US. Two major banks in the UK are also on the target list the malware fetches.

One notable finding about IcedID is that it spreads via another Trojan: the Emotet malware. Emotet was originally a banking Trojan itself, derived from the Bugat source code, which is also the core of the Dridex Trojan.

X-Force research believes that a threat actor or a small cybergang has been operating Emotet as a distribution operation for banking Trojans, especially serving the cybercrime elite in Eastern Europe. Emotet's most prominent attack zone is the US. To a lesser extent, it also targets users in the UK and other parts of the world.

Emotet has been one of the notable Trojan distribution methods in 2017, linked with groups operating QakBot and Dridex, both of which favor targeting business banking. It has added IcedID and Zeus Panda as new payload drops in late 2017.

When it comes to tactics, techniques and procedures (TTPs), IcedID has a few tricks up its sleeve. The malware features a network propagation module to allow it to spread to multiple users and terminal servers that share the same LAN/WAN connection.

The malware monitors victims' online activity by setting up a local proxy for traffic tunneling, which is a concept used by the GootKit Trojan. Its fraud attack tactics include both web-injection attacks

Contents

and sophisticated redirection attacks similar to the schemes used by Dridex and TrickBot.

After publishing information about IcedID, it appears the group operating it has taken a step back and reduced its activity. Will IcedID be launched into wider campaigns? That is doubtful at this time since this malware started out in targeted fashion, electing the Emotet group as distributors, which makes it inherently much less aggressive in terms of attack scope.

Ursnif (aka Gozi) V3 emerges in Australia

Starting in the summer of 2017, IBM X-Force research started detecting a new variation of the Ursnif Trojan which was being tested in the wild. Per X-Force's analysis, the malware is entirely based on the same malcode of the original Ursnif Trojan (aka Gozi ISFB), but features some modifications on the code injection level and the fraud attack tactics.

Beyond the material modifications, the malware's developer also switched the internal build version, which now shows as v3 increments. The existing Ursnif variants are v2 builds, which would make this iteration new, and an upgrade of sorts that was most likely undertaken by a different malware developer and a different group.

Ursnif v3 first appeared in Australia, and the notable thing about it is that it featured some web-injection attacks, but had separate configurations with redirection attacks created to target business and corporate banking services in Oz. Redirection attacks are a sophisticated tactic currently used by cybergangs such as Dridex, GootKit, TrickBot, and IcedID.

Ursnif v3 only emerged in late-2017, and for now, X-Force research is only seeing its activity in Australia and New Zealand. The malware may spread to other parts of the globe, but that would depend on its operators' resources and plans to expand if ever.

Client Maximus emerges, thrives in Brazil

In a niche of its own, another malware code that emerged in 2017, has been growing and upgrading its capabilities in Brazil.

Unlike the plethora of Delphi-based malware in the region, Client Maximus caught X-Force's attention for its relative sophistication, stealthy delivery tactics, and ongoing code development. The purpose of the Client Maximus malware is financial fraud, and as such, its code aspires to create the capabilities that most banking Trojans have: to allow attackers to monitor the

Contents

victim's web navigation, and to take control of the online banking session at will.

To do that, Client Maximus monitors open Internet tabs, and if it matches them with a target on its list, is operator can launch real-time device takeover using a remote access tool to ride the authenticated banking session. The attacker displays premade fake overlay screens to the user to keep them engaged and have them provide transaction authorization codes which can ultimately allow the attacker to complete fraudulent transactions from that trusted device.

X-Force research notes that unlike other codes in Brazil, Client Maximus has been consistently evolving to evade anti-virus detection and update the code's capabilities. Moreover, the malware has been spreading in a rising number of campaigns in Brazil. Both these observations suggest that Client Maximus is a commercial offering being developed and sold to other criminals by its creators.

Overall In 2017, IBM X-Force is seeing an ongoing escalation of malware codes in Brazil. After seeing trending collaboration with external parties, it appears that there has been a permanent step-up in sophistication of malware codes that target online banking users in the country.

2017's goners

Although 2017 was definitely an active year for malware activity, some cybercrime groups—new and old—departed from the scene for different reasons, while others greatly reduced their activity volumes and scope.

Some of those codes are the Shifu Trojan, GozNym, Neverquest, and URLZone.

Goodbye Shifu?

The Shifu Trojan's story is actually quite an unusual one in the cybercrime arena. Shifu emerged in Japan in 2015, and from the get-go its code was considered to be quite sophisticated based on X-Force's analysis. More than just a hybrid code, Shifu took best-of-breed parts of several banking Trojan codes in a way that could only be crafted by a malware-savvy developer who knew those codes and had access to them.

The group behind Shifu launched its operation with modular and multi-purpose code, and they also developed the toolset and infrastructure to attack Japanese banks, setting up spamming and infection vectors, configurations and web-injections. Shifu thus opened the floodgates to other malware gangs from Eastern Europe, like Rovnix, URLZone, and Gozi, that promptly followed in its footsteps.

X-Force monitoring of Shifu's activity showed it was quite active in 2016, leveraging the Angler exploit kit to spread around during the period following its release. Within a month from the Japan launch, attacks spread to the UK, intermittently targeting banks in each territory.

But Shifu rarely attacked in both countries at once, and it did not spread to other countries. Overall, it seemed that Shifu was not really lifting off in spite of its highly sophisticated DNA.

In mid-2016, X-Force research noted that Shifu was using web-injections bought from Shifu's underground vendors that supplied them to other malware gangs. This was rather significant, because it meant that the group did not have their own developers and had to outsource some of their needs. This may have been the first sign of trouble for Shifu. By September 2016, X-Force saw a very sharp drop in Shifu activity and a dying-out trend since.

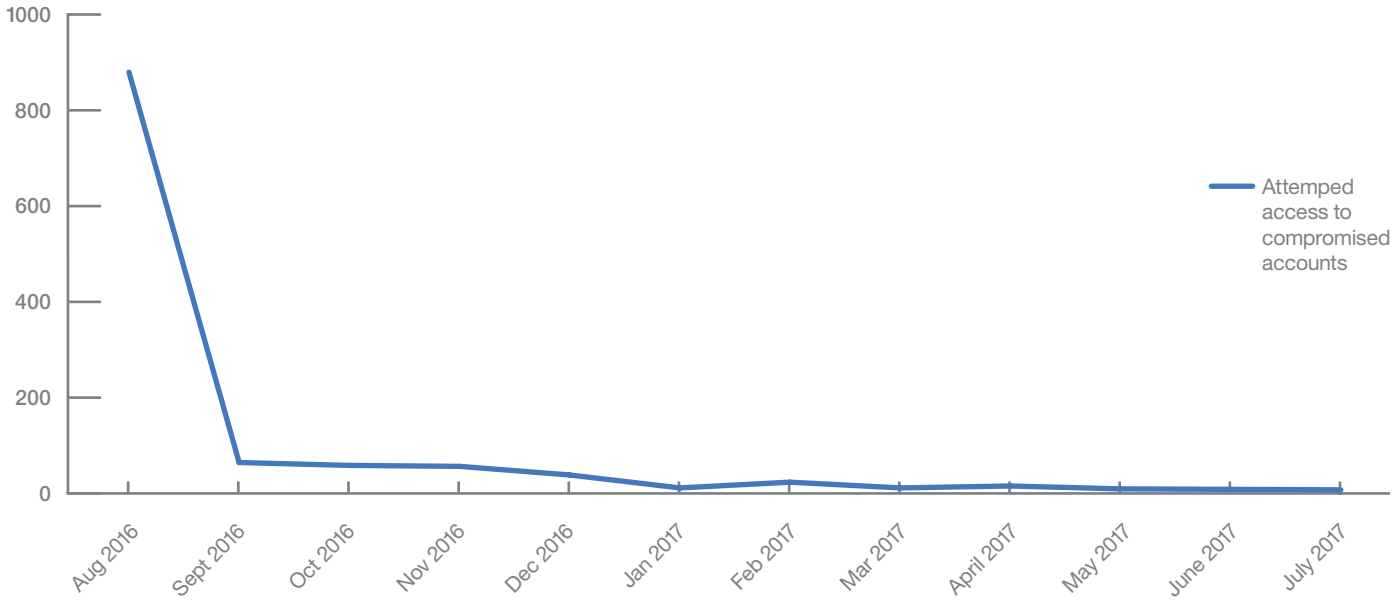


Figure 2. Shifu trend of attempted illicit access on infected endpoints – Source: IBM X-Force

What happened to Shifu? None but its own operators may know the reason, but the speculation is that the gang was simply not connected enough to operate globally and eventually disbanded. Shifu is still one of the most professional Trojan codes out there, and it could be one that we will see in the future if another group takes over.

Neverquest's 2017 exit

A very significant exit this year featured the Neverquest Trojan—a cybercrime-as-a-service gang that has been part of the crimeware arena since 2013. The malware was sourced from the Gozi ISFB code, but evolved separately to feature its own modules and capabilities.

At its prime, Neverquest, aka Vawtrak, was a vast operation that touched many parts of the globe. Through their years of operation, Neverquest operators enabled their accomplices to target business banking accounts, allowing them to rob organizations of hundreds of millions of dollars every month. The operation was considered sophisticated and robust, and in cybercrime terms, it was also long standing. According to X-Force research, Neverquest held on to the top ranks on the global malware chart since 2014.

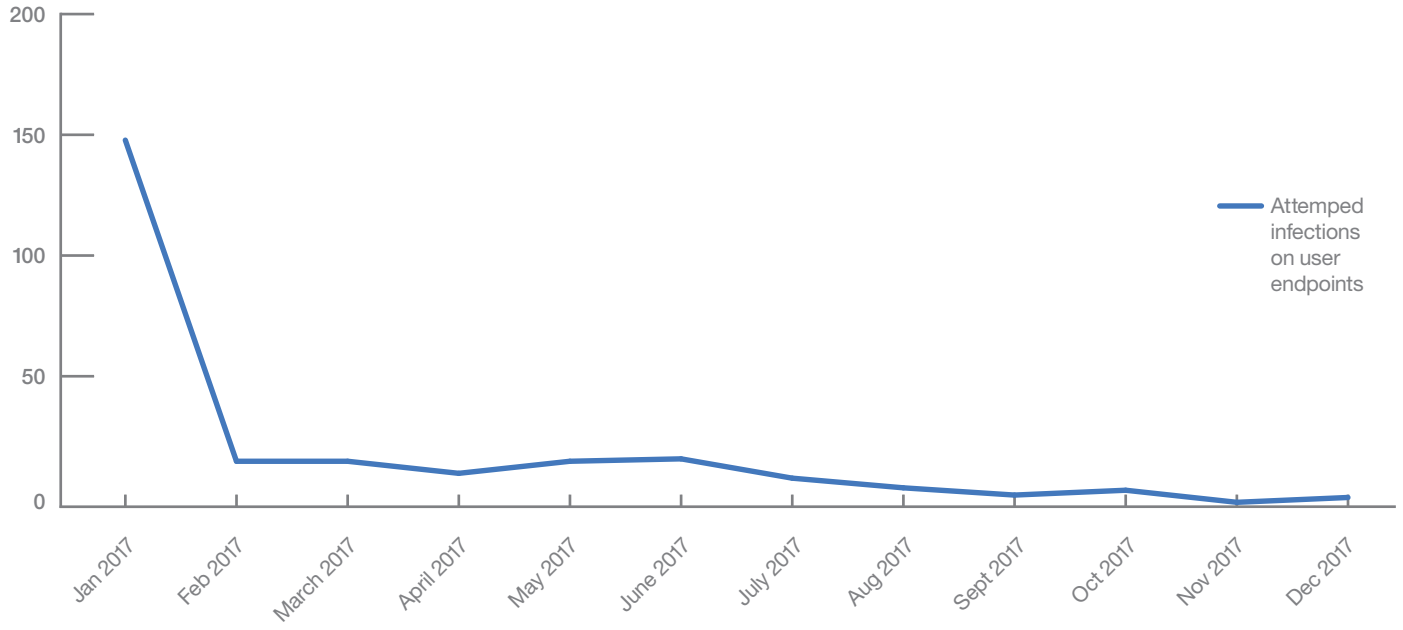


Figure 3. Neverquest monthly infection attempts–Source: IBM X-Force

Contents

Ending its successful run, Neverquest's exit was approaching, and its demise would come from the intervention of law enforcement that captured one of its key players.

In late 2016, the group hit a road-bump that shook it enough to disband. One of its key members, the person who was suspected as the malware's author, was arrested in Spain.

By January 2017, as the news became public, Neverquest's crime collaborators saw law enforcement reach one of their trusted parties and likely realized the FBI was already too close.

Neverquest campaigns brusquely halted, and the attack pattern died out gradually.

The Neverquest Trojan's exit in 2017 was one of the more meaningful occurrences of the year, and was likely affected by the Europol's takedown of the Avalanche cybercrime infrastructure in a multi-national law enforcement effort.

GozNym's deadly hit

The GozNym Trojan is another cybercrime exit that took place in 2017.

GozNym emerged in April 2016 as a hybrid of two existing malware codes: Nymaim and Gozi ISFB. GozNym was likely partly owned by the same group that still operates the Nymaim infector to this very day.

On the attack landscape, GozNym was highly active from the get-go, and by summer of 2016, a mere four months after its launch, it was a rising threat in the cybercrime arena. The actors operating GozNym targeted banks in Europe and North America, focusing on businesses and robbing millions in fraudulent wires. They were aggressive and fast to spread the malware to different countries, which quickly got the attention of law enforcement, especially in the US, after banks there suffered ongoing losses to GozNym attacks.

The GozNym group likely realized trouble was underway by summer of 2016, as the upcoming takedown of Avalanche, one of the largest

and longest standing bulletproof cybercrime operations, was approaching. Avalanche just happened to also serve GozNym attacks, and the law enforcement operation designed to dismantle it was not only about domain takedown, it was also about taking down Avalanche's criminal customers.

The Europol released notice about the takedown on December 1, 2016. On December 12, 2016, the American DoJ released a notice on the arrest of a Bulgarian national charged with operating GozNym attacks against US residents.

Similar to Neverquest, GozNym's operators were likely shaken by the arrest as the group apparently disbanded. In November 2016, X-Force research was still observing some GozNym campaigns in the US and in Germany, but those quickly died out, as did GozNym activity which has remained silent ever since.

So long Andromeda, hello Necurs

Dedicated to spreading malware to millions of users across the globe, the Andromeda botnet was a cybercrime operation associated with as many as 80 malware families. According to the Europol, it was detected or blocked on an average of over 1 million machines per month in the second half 2017 alone. Andromeda had ties to the Avalanche infrastructure which was host to similar activity.

Insights gained during the Avalanche case by investigating German law enforcement entities were shared, via Europol, with the FBI, and those findings supported investigations that led to the demise of the Andromeda botnet in late November 2017.

Similar to the GozNym case, the takedown also resulted in the arrest of a 33-year-old Belarusian named Sergey Jarets, who was named the mastermind behind the Andromeda operation.

With Avalanche and Andromeda both gone, the biggest malware distributor that still regularly spews banking Trojans and ransomware is the Necurs botnet that commands about six million endpoints and continues to be active across the globe.

Contents

Notable or rising activity

Aside from the moving parts of the cybercrime arena in 2017, some of the existing constituents held steady, showing continued and rising activity. The top three in this category were Ursnif for its activity volume, TrickBot for its consistent activity bouts, and the QakBot Trojan for re-emerging and targeting businesses.

Ursnif v2 (AKA Gozi)

By order of activity volume, X-Force research notes that Ursnif v2, a long-standing cybercrime group, has been 2017's most active operation in a few measures:

- Number of campaigns
- Code updates
- Geographic reach
- Actual attack volume

Aside from its usual targeting patterns, starting the third quarter in 2017, X-Force has been seeing Ursnif step up its focus on Japanese banks, making activity in Japan, which was previously sporadic, more consistent. Ursnif targets Japanese banks and credit providers as well as e-commerce and popular cryptocurrency exchanges.

TrickBot

TrickBot has been the most consistent group this year in terms of code updates and campaigns. During the summer months, when other malware groups went into a slower period, TrickBot stood out as the one cyber gang that did not reduce volumes, continuing to distribute the malware through the Necurs botnet and via fake domains registered in order to target UK banks. TrickBot was second only to Gozi in terms of code updates and campaigns.

Overall in 2017, TrickBot continued developing its global reach and building additional redirection attacks for many of its targeted entities. It regularly tests online banking procedures and continues to spruce up target lists, adding business banking, payment cards, and cryptocurrency exchange platforms to those lists, which have reached the hefty size of over 1,000 URLs each.

QakBot (AKA QBot)

QakBot is an old financial Trojan that sort of came out of the woodwork in 2017. This gang-owned code has been around since 2009, at which point it was one of the only cybercrime operations that focused solely on US business banking accounts.

Contents

Qakbot activity has been on and off through the years, but it came back in 2017, with the same focus on North American business banking, and with its modular, multithread code that's designed to enable network propagation, security evasion, online banking fraud, and data exfiltration.

QakBot works in limited scope: it is delivered in a targeted way by Emotet, into already infected endpoints. In 2017, our research team observed QakBot in what might have been an operational glitch, causing mass Active Directory lockouts on compromised networks in its attempt to spread to other endpoints in the organization. Sporadic QakBot campaigns continue to target US financial entities.

Zeus Panda, CoreBot, URLZone

In the fourth quarter of 2017, X-Force has seen some sporadic Zeus Panda and CoreBot activity in Canada, rising only toward the end of the year as other malware was ramping up for the seasonal rush of the holidays.

URLZone, which has been rather inactive in 2017, rose in small campaigns in Japan.

What to expect in 2018?

The financial cybercrime arena is not expected to slow down in 2018. Even with some groups gone, the ones that remain are those who manage complex operations that include the entire supply chain linked with financial crime, especially its money laundering aspects.

Some of the trends to look out for in 2018 are:

Trojan codes will be exclusive to elite cybercrime syndicates

Commercial codes are not likely to make it far in the 2018 security landscape. With rising awareness and bank controls, online fraud is becoming somewhat of a profession and malware authors that work to sell their codes are not going to keep up with evolving security, machine learning, and artificial intelligence controls.

Nation-state-grade weaponization

The WannaCry and NotPetya attacks, that pestered organizations with destructive ransom-worms, gave the world a glimpse into what attackers can achieve with exploits stolen from nation-state agencies. It was not long after that the TrickBot Trojan adopted network propagation based on SMB, drawing inspiration from those attacks.

Contents

In 2018, we are bound to see more widespread vulnerabilities and non-civilian exploits make it into malware that targets civilian organizations, including banking Trojan developers who can adopt them just as other malware authors do.

A focus on businesses

Financial malware will be focused on businesses, leaving most of the consumer base to the smaller cybercrime groups and to mobile malware operators, who will be picking up the fraud slack in 2018.

Carbanak-style bank heists

Groups that carry out attacks against banks' internal systems have not only remained at large after major heists in 2015 and 2016, they also continued their activity in 2017.

We expect to see more of those attacks in 2018, that will prey on banks' internal systems and processes, as well as continue their focus on automated payment relays and ATMs used by the banking industry.

Mobile malware to drive rise in fraud

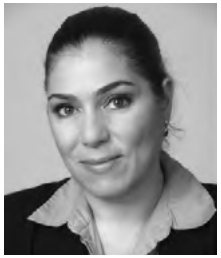
In 2017, mobile malware became a cross-channel fraud enabler. With the increasing use of mobile payments, shopping apps, and mobile banking, cybercrime is ready to take on the consumer market and fraud cases are expected to increase via that channel in 2018.

Android banking Trojans have been spreading across the globe, and reminiscent of the Zeus malware's spread, most of them are based on the same leaked source codes of malware like GM Bot and BankBot. That does not stop these codes from making it into official app stores, and ultimately compromising user devices to take over their financial accounts.

Keep up to date on threat intelligence

We know that keeping a keen eye on the threat landscape is part of our readers' jobs. The content of this report and the insights shared are fruit of ongoing threat intelligence work delivered by X-Force year-round. To keep up to date about the cybercrime arena, please join X-Force Exchange, and check out securityintelligence.com often for news from our research teams.

Contents



About the author

Limor Kessem, Executive Security Advisor, is one of the top cyber intelligence experts at IBM Security. She is a seasoned security advocate, public speaker and a regular blogger on the cutting-edge IBM Security Intelligence blog.

Limor is considered an authority on emerging cybercrime threats. She participated as a highly appreciated speaker on live InfraGard New York webcasts (an FBI collaboration), conducts live webinars on all things fraud and cybercrime, and writes a large variety of threat intelligence publications. With her unique position at the intersection of multiple research teams at IBM, and her fingers on the pulse of current day threats, Limor covers the full spectrum of trends affecting consumers, corporations and the industry as a whole.

For more information

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

For more information on IBM X-Force Research, visit: ibm.com/security/xforce

Contents

IBM Security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2018

IBM