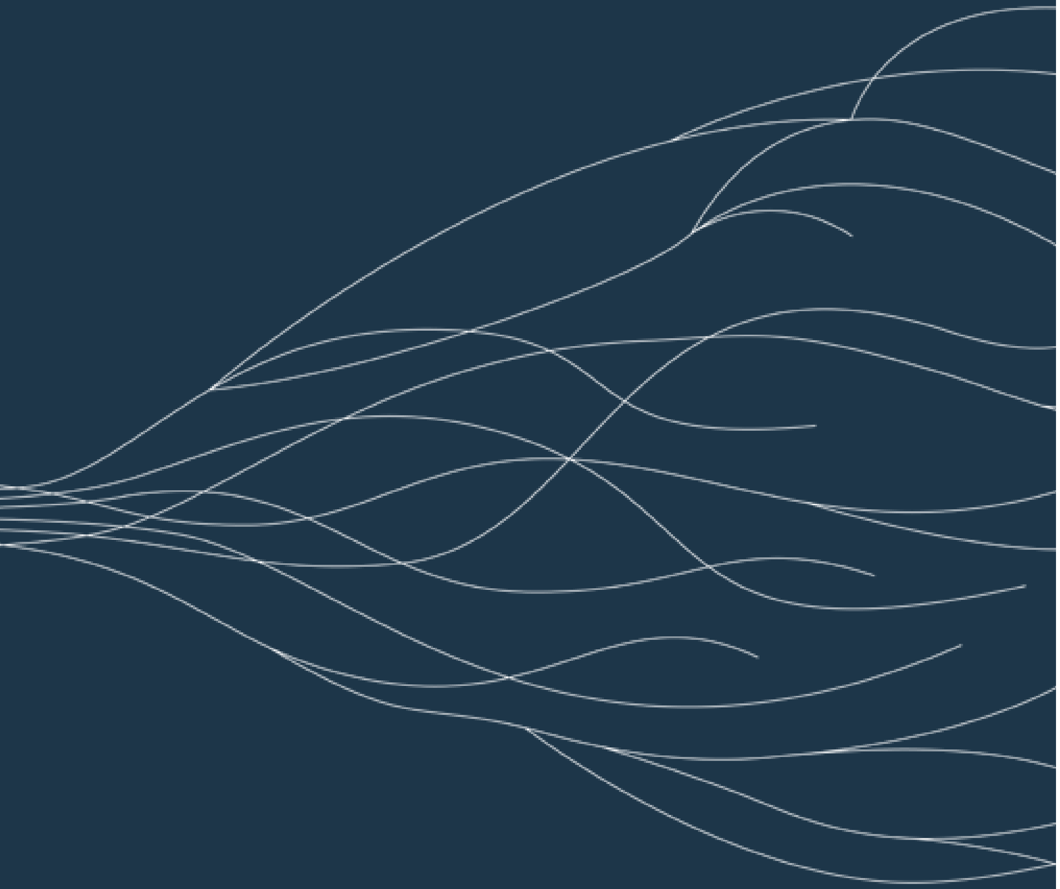
IBM Security



The shifting panorama of global financial cybercrime

A survey of attacks and attackers around the world

IBM X-Force® Research

Click here to start ▶

◄ Previous Next ►

Contents

Executive overview

In the global panorama of financial cybercrime, one year might bring little change, with the same types of malware continuing to target the same geographies, while the next can be very active. That was certainly the case 2016, with some countries seeing a marked rise in the attention of cybercriminals.

The IBM X-Force researchers, who monitor almost three hundred million protected endpoints across the globe, have been seeing some shifts in the usual undercurrents of the cybercrime arena. Those developments are the subject of this report.

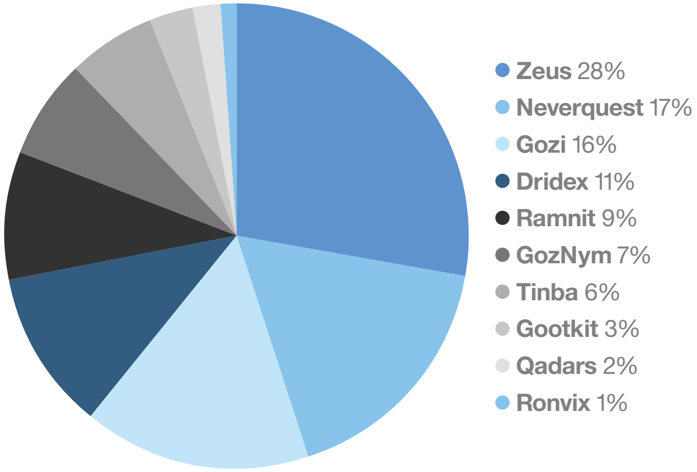


Figure 1. The most prevalent financial malware families globally in 2016 (Source: IBM Trusteer)

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

◄ Previous Next ►

Japan: Organized cybercrime proliferates

In 2016, we saw cybercrime take meaningful strides in Japan, both on the malware front and in yet another ATM heist that probably drew on support from local organized crime.

For many years Japan remained relatively isolated on the global cybercrime scene due to the scarcity of attack tools in its complex language. That changed and cybercriminals' focus on Japanese targets began to accelerate once the Shifu Trojan emerged in late 2015, laying the foundation for further attacks.

The top most active financial malware in Japan, per attack volume, includes:

1. Gozi
2. URLZone
3. Rovnix
4. Shifu

Rovnix

The expanding malware trend in Japan kicked off with the new Rovnix malware campaigns that emerged between end of 2015 and January 2016. The attacks were meticulously planned, with well-crafted Japanese-language email spam and a hefty configuration file, replete with web injections designed to fully and uniquely attack banks in Japan. Unsurprisingly, Rovnix's developers seemed to draw on Shifu's existing attack schemes and web injections, derived either by analyzing them and then applying additional elements or by buying them directly from the Shifu gang.

URLZone

By February 2016, the well-known Eastern European cyber gang, URLZone, had set its sights on Japan and launched infection campaigns targeting local banks. That launch marked an increasingly evident evolution of the fraud infrastructure in Japan, encompassing spam and infection, malware adaptation, effective web injections for social engineering, money mule recruitment and the eventual cash-out and laundering of stolen funds.

◄ Previous Next ►

Gozi

Next up, in March 2016, X-Force researchers saw that the Gozi Trojan developers started stepping up attacks in Japan, investing more resources into studying local banks by deploying video grabbers that activate on access to Japanese bank URLs. Gozi was already targeting banks in English-speaking countries like the US, UK, Canada and Australia, but Japan became one of its top targets in 2016 when it launched recurring campaigns there throughout the year. Gozi appears to be operated by an organized cyber gang based in Eastern Europe, and according to its configuration files, Japan is the only known non-English-speaking country on its attack roster. The malware receives frequent incremental updates to the code and its evasion mechanisms. IBM X-Force research shows that Gozi ranks first on a list of the most active malware projects in terms of the code change cycles applied to its mechanisms.

As it's used in Gozi, video grabbing is a module implemented into the works of banking Trojans in which the attacker has the malware record a video of the desktop activity. This recording can be set up to begin when the user takes a specific action, such as accessing a predetermined URL. Using video grabbers, malware developers and cybercriminals have been able to record online banking sessions and learn from actual users how to perform transactions with each bank.

Canada on the map

In global cybercrime it's typical for countries to be targeted along with their neighboring geographies, often because they share some bank brands across borders. Australia and New Zealand, for example, are frequently targeted in tandem. It would make sense, then, to see Canada and the US targeted together, but historically that hasn't been the case. Canada has escaped the high attack activity typical in the United States.

Until 2016, that is—it seems to have been the year organized cybercrime realized Canada could be a lucrative target, and X-Force researchers started seeing Canadian banks in a variety of configuration files of both commercial banking Trojans and cyber gang-operated ones.

In terms of attack volume, the top five Trojans regularly featuring Canadian bank targets in 2016 were:

1. Gozi v2
2. Ramnit
3. Qadars
4. TrickBot
5. Zeus Sphinx

Each malware has a different approach to the Canadian financial sector. Some target the national banks, others target credit unions, and TrickBot even dedicated redirection attacks to the major banks in Canada.

Gozi

Gozi is known to regularly target English-speaking countries with strong economies. Its configurations typically include targets in the US, the UK, Canada and Australia. Although Gozi ISFB's source code was leaked in 2010, one consistently active variant appears to be operated by a closed cyber gang targeting these English-speaking countries throughout the year.

Gozi activity in Canada was detected throughout 2016, but peaked towards year's end, corresponding with the rise in attacks across all online threat categories during the holiday season (see Figure 2).

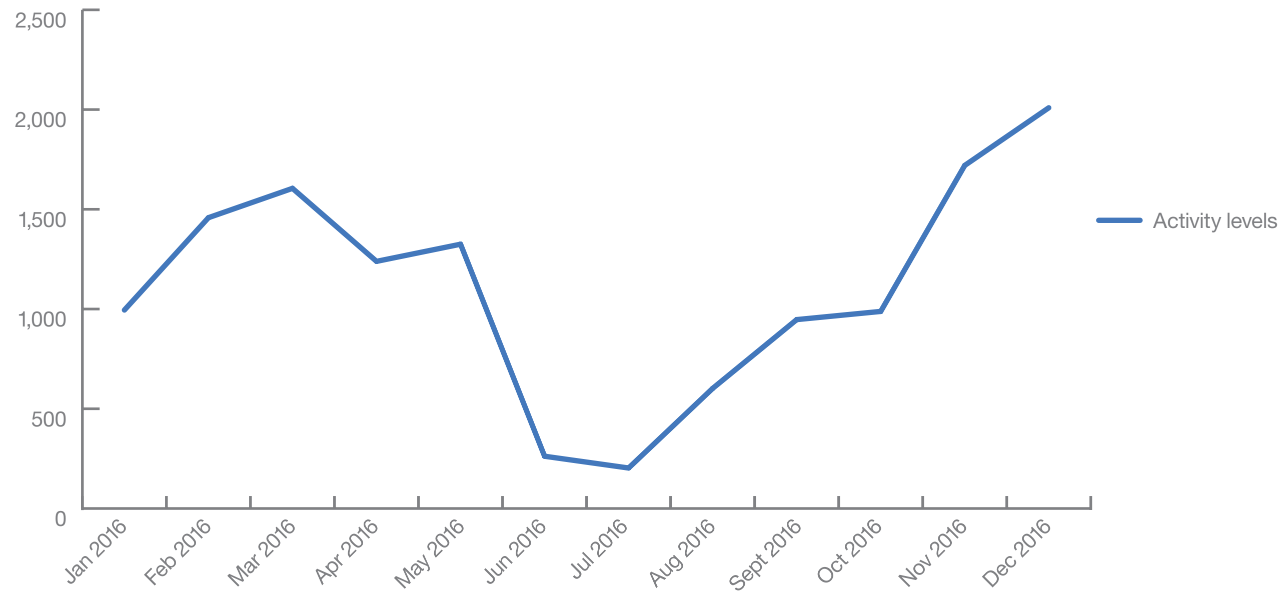


Figure 2. Gozi's activity trend line in Canada during 2016 (Source: IBM Trusteer)

Ramnit

Another frequent visitor to Canada is Ramnit. Discovered in the wild in 2010, at first it was used as a worm that leveraged removable drives and network shares to spread to new endpoints. In 2011 its developers borrowed some code from the leaked Zeus Trojan source code and turned it from a worm into a banking Trojan.

Known for its extensive mule-recruitment campaigns, Ramnit gained momentum quickly, and resurfaced after a European law enforcement shutdown to become intermittently active in the cybercrime arena. Its most recent campaigns targeted banks in Canada, the UK and Australia. Figure 3 shows Ramnit's ramped-up Canadian activity late in 2016.

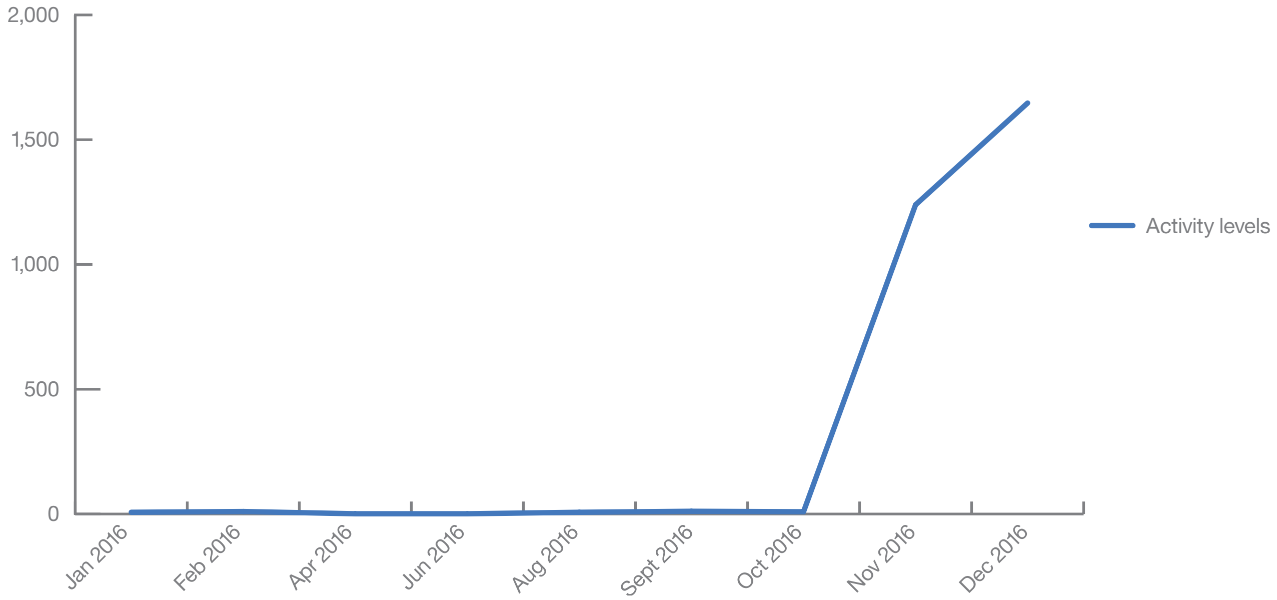


Figure 3. Ramnit's activity trend line in Canada during 2016 (Source: IBM Trusteer)

Qadars

The Qadars Trojan always had its sights on Canada, and according to X-Force research data its configuration files included Canadian banks since 2013. Our data shows that Qadars' operators stepped up their attacks in Canada between 2015 and 2016 and added other countries to the mix, among them Australia, the US, Germany, Poland and the Netherlands.

In the third quarter of 2016 Qadars' operators released an updated version of the malware and populated its target lists with banks in the UK. X-Force researchers believe that Qadars is privately-owned code operated by a closed cyber gang that targets Western countries.

TrickBot

The TrickBot Trojan emerged quite aggressively in Canada very soon after its launch in the wild.

IBM X-Force research reported TrickBot's launch in November 2016. Although the malware had only just become operational, it proved to be technically advanced with the capability to dynamically fetch web injections from its command and control server and use redirection attacks on its targets, abilities matched only by Dridex and GozNym.

TrickBot started its onslaught with banks in the UK, but less than two weeks later it had spread its reach to Canada with redirection attacks before doing the same in Germany. Ten days later, it showed how well funded and connected it is by starting to target banks in Singapore and other parts of Asia. By December of 2016, TrickBot's redirection attacks already covered Australia, New Zealand, Singapore, India and Malaysia[1].

Redirection attacks are considered an advanced modus operandi because they bypass bank security measures, hijacking victims before they ever reach the bank's site and redirecting them to a malicious website. These attacks can therefore be very effective in tricking bank customers and elevating online banking fraud success rates.

Zeus Sphinx

Last on this list is the most recent contender, Zeus Sphinx. Sphinx's Canadian tour began in late 2016 when its operators prepared a 33-bank brand configuration to steal the credentials of credit union customers. According to configuration data analyzed by X-Force research, 80 percent of the target URLs on Sphinx's list belong to credit unions and regional banks, with only 20 percent belonging to major Canadian banks[2].

Interestingly, it looks as if Sphinx's operators are testing the waters in Canada, deploying very small rates of infection in the field and checking their malware's operation. Given that pattern of activity, IBM X-Force believes that in 2017 Canada is likely to experience more widespread Sphinx campaigns. According to X-Force researchers, Sphinx used the same attack servers that facilitated the Zeus Citadel attacks early in 2016 and the Ramnit attacks in the fourth quarter. The web injections used by the malware share familiar code patterns with other banking Trojans, indicating that the attackers probably bought them from an injection-writing service.

The lands down under: Australia and New Zealand

X-Force research data on malware campaigns in 2016 ranks Australia fourth among the geographies most targeted by banking Trojan attacks, following the UK, the US and Canada.

Australian financial institutions are often targeted in tandem with banks in New Zealand, though the malware groups responsible still show less interest in New Zealand banks. The list of Trojans most prolific in Australia and New Zealand features four top contenders:

1. Ramnit
2. Gozi
3. Dridex
4. TrickBot

Ramnit

Globally, the Ramnit Trojan ranks fifth among the most active banking Trojan families. In Australia it's the most active malware in terms of campaign numbers, mostly because it simultaneously targets Australia, the UK and Canada.

X-Force research data shows that Ramnit has targeted a small number of large Australian banks, using web-injection attacks on four or five URLs in each case and mostly targeting personal banking services[3].

Gozi

Gozi ranks third on the global financial malware chart, and its campaigns are the second most prolific in Australia. Typically Australian banks are targeted alongside others, mostly in the UK and US.

The malware has a variety of attack techniques in the configuration, using them to adapt to the security features in each geography targeted. Gozi attacks can include redirection to a remote transaction orchestration panel, SOCKS proxy, VNC activation and video grabbing. All have been deployed in Australia[4]: VNC, web injections, redirection to a transaction panel which supplies the malware with on-the-fly web injections, mule account details, and transaction parameters to match the victim's account balances, or video grabbing.

Dridex

Dridex has been targeting Australian and New Zealand banks, following in the footsteps of the late Dyre Trojan. Its favored target is business and corporate banking[5], and to find the right victims its operators craft relevant phishing emails to deliver their payload to users in Australia and New Zealand. Dridex is known for diverse target lists, and its recent Australian infection campaigns were launched alongside campaigns in the UK, France and Ireland. Dridex appears to take an interest in credit unions, and deploys click-shot attacks on those banks in Australia. In such attacks, click shots are taken every time the infected user taps the left mouse button on a link inside the bank's website. Used in place of the heavier video-grabbing modules, the tactic allows attackers to familiarize themselves with a legitimate flow of events on the bank's site.

TrickBot

TrickBot is the most recent organized cyber gang to arrive in Australia, bringing the bells and whistles of redirection attacks to the land down under in November 2016, at the same time it started attacking banks in the UK. The malware targets Australian banks alongside their New Zealand neighbors, focusing on the larger local banks in the region[6] with a mix of financial institution types.

Much like Dyre and Dridex before it, TrickBot prefers business and corporate bank accounts and targets the web portals of these services with redirection attacks.

Banks in Australia and neighboring New Zeland are often targets of the same attacks and attackers.

Brazil: Technical sophistication changes the game

Cybercrime in Brazil is beyond doubt one of the country's greatest challenges, and unlike elsewhere in the world, most attacks there are the work of local criminals using tools adapted into the Portuguese language and sold on Brazilian forums and social networking pages. In the past, the malware employed by Brazilian cybercriminals has tended to operate at lower sophistication levels than most malware made in Eastern Europe, but on that front 2016 saw a shift toward greater technical savvy. The shift gained momentum towards year's end, bringing the Brazilian threat landscape more closely into line with other parts of the world. Behind it are local criminals increasingly collaborating with Russian-speaking cybercrime actors to buy and market malware or plan more effective attacks.

The new face of phishing

Phishing is one of the oldest threats in the cybercrime book, but while this online menace has existed for decades, it is still effective in preying on people's emotions and psychological reactions.

Globally, phishing increased in 2016. Brazil, where attack kits are traded freely in underground forums and sometimes even on social media, sustained more phishing attacks in 2016 than any other country in the world. X-Force researchers following underground sources report that attack kits can be quite unsophisticated, but it might not matter. Emails from "Nigerian princes" are still abundant in Brazilian email spam folders because they may still work.

Although cybercriminals are in no hurry to "fix something that's not broken," October of 2016 saw a notably sophisticated twist on the old phishing attack kit: live, interactive phishing attacks uncovered by IBM X-Force researchers.

This particular method is designed to emulate the social engineering element used by banking Trojans to extract information from victims in real time. The attack takes place over a web session between the attacker and the victim, on a website that closely mimics the look and feel of the original bank's site. The attacker uses Ajax-powered screens to switch up the messages the victims see on their end, asking them to provide critical identification and transaction authorization elements in the guise of messages from their bank.

The flow of events is controlled from a web-based admin interface that allows the attacker to automate the choice of screens shown to the victims or even to craft their own message to the victim in order to further personalize it.

This was the first time our researchers witnessed this type of attack in Brazil. They consider it advanced since it makes the process much more believable to the victim and therefore more likely to result in successful data theft.

Since this sort of phishing attack can enable criminals to access victims' accounts and defraud them with illicit transactions, one of the best ways to detect it is by using a solution that identifies account takeover (ATO) attacks.

Browsing hygiene guidance is just as important as technology in helping users avoid even an advanced attack like interactive man-in-the-middle (MitM) phishing. Use these tips for mitigating malware to reduce risks, and check out the IBM X-Force Report "The Perils of Phishing" for additional recommendations.

Zeus ushered into Brazil

The Zeus Trojan is an old foe, but was not often seen in Brazil until 2016, probably because local cybercriminals generally didn't have the high levels of technical savvy to maintain the code functionality that operation of this sort of botnet requires.

In 2016, however, Zeus found its way into the local cybercrime arena just in time for the international sporting games. Zeus's code was the basis of two commercial malware iterations, Zeus Panda and Zeus Sphinx, which were adapted to target Brazilian banks and payment platforms. The latest Zeus-based offspring, FlockiBot, showed up in December 2016. Significantly, its author is suspected to be of Brazilian origin.

Bringing Zeus into a territory that operates Delphi-based malcode and overlay-screen-type malware is a sophisticated game changer, much less visible to victims in the infection phase and trickier to prepare for, or visually detect, in the attack stage.

Zeus Panda and Zeus Sphinx were both sold in underground fraud-themed forums and could have been purchased along with technical support and a user guide by actors from inside Brazil, then deployed against financial institutions in the country.

Fresh actors, fresh code

Another sign of the times is the maturing Brazilian malware-writing community, a trend that's becoming more evident as new malcode appears in attacks in the country.

One of the notable examples studied by IBM X-Force researchers featured a remote overlay malware designed to take over victims' endpoints in real time and enable the attacker to perform a fraudulent transaction from their device. The attacker uses overlay screens shown to the victim to ask them to divulge authentication codes and finalize the transaction.

Our X-Force researchers were interested to see a new level of sophistication in Brazil, with malware that was ushered in by a proper AV-disabling loader in driver form, as well as new malcode they named Client Maximus. They believe they'll be seeing further escalation in 2017.

Old tricks in a new territory

Brazilian cybercriminals' increasing technical capability is also evident in TeamXRat. In this instance, a cybercrime faction in Brazil wrote a cryptographic ransomware variant and leveraged it in attacks against organizations in the country, holding them up for ransom.

The scheme itself was previously used in Western countries against healthcare organizations, and the Brazil-based crew also went after hospitals, penetrating their infrastructure with RDP brute force attacks reminiscent of the SAMAS group's modus operandi. Unlike earlier Brazilian-made ransomware, XRat was authored by an organized cyber gang with technically advanced actors on its team that launched targeted attacks on the organizations it preyed upon. That was a first in Brazil.

It's virtually inevitable that such operations will proliferate and escalate over time. In fact, cyber extortion of this type is expected to be one of the most prominent threats in Brazil in 2017.

Organized cybercrime targets Germany

Germany in 2016 saw the emergence of two sophisticated cybercrime gangs. Interestingly, both used malware codes that were new at the time and appeared in Germany shortly after their arrival in the global cybercrime arena.

GozNym

The GozNym banking malware, a Trojan hybrid discovered by IBM X-Force in early April 2016, began targeting banks in Germany in August 2016 with redirection attacks on 13 banks and their local subsidiaries. These new redirection schemes came in addition to web-injection-based attacks for all the targeted brands, showing GozNym's investment in German-language attack capabilities.

GozNym's Europe-focused attack faction was intensifying its activity across the region at the time, showing a very sharp activity peak in August 2016—in numbers, a 3,550 percent hike since July 2016, and a 526 percent increase compared to the total number of attacks since the rise of the GozNym hybrid in April to July 2016. The malware continues to target banks in Germany, using both web injection and redirection attacks.

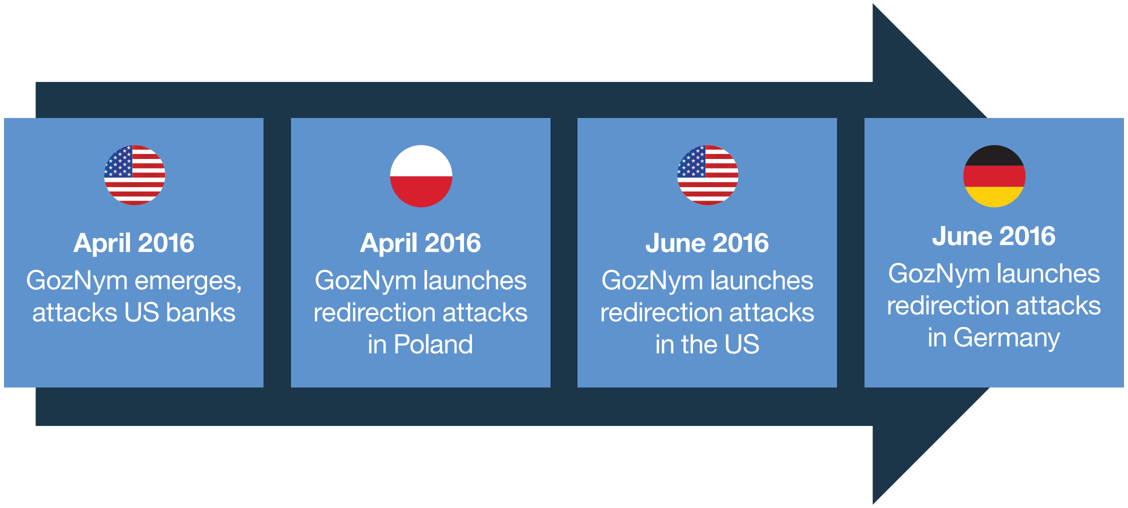

April 2016
GozNym emerges, attacks US banks
April 2016
GozNym launches redirection attacks in Poland
June 2016
GozNym launches redirection attacks in the US
June 2016
GozNym launches redirection attacks in Germany

Figure 4. Evolution of the GozNym malware (Source: IBM X-Force)

TrickBot

A second organized crime group that set its sights on German banks in 2016 was the crew operating TrickBot. TrickBot emerged in August 2016 and was launched into a testing and development period to turn it into a banking Trojan. By October 2016 the malware, which resembles the Dyre Trojan in some ways, was fully operational and detected in infection attempts leveraging the RIG exploit kit or the Godzilla loader.

By December 2016 X-Force research detected TrickBot in Germany, fully equipped with web injections and redirection attacks to target local banks[7] after launching similar attacks in the UK, Australia, New Zealand and Canada.

The malware's technical capabilities, its ongoing development and its links to other cybercrime groups make TrickBot one to watch in 2017 along with Trojans like Dridex, Gozi, and GozNym.

UK and USA: Business as usual

According to X-Force data, the UK and the US continue to be the countries most targeted by banking Trojans. In 2016 the financial sector in these geographies suffered intense attention from cybercrime groups of all grades.

Figure 5 shows the malware families that were active throughout 2016 in the UK.

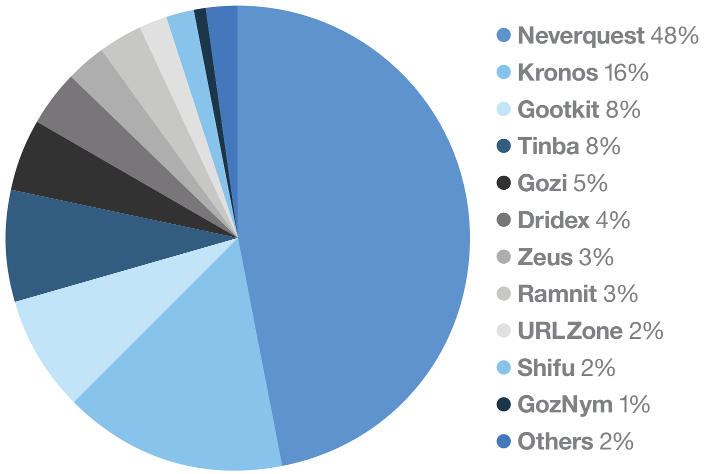


Figure 5. Top most active financial malware families in the UK per attack volume (Source: IBM Trusteer, 2016)

Neverquest was the most active Trojan in the UK during 2016, presenting a major activity peak in June (see Figure 6).

The reason behind Neverquest's June activity peak is unclear, but this malware gang operates in collaboration with a number of professional cybercrime factions, and it's possible that May-June peaks across the board in the UK are linked to tax season spam campaigns conducted just after the tax year ended in April.

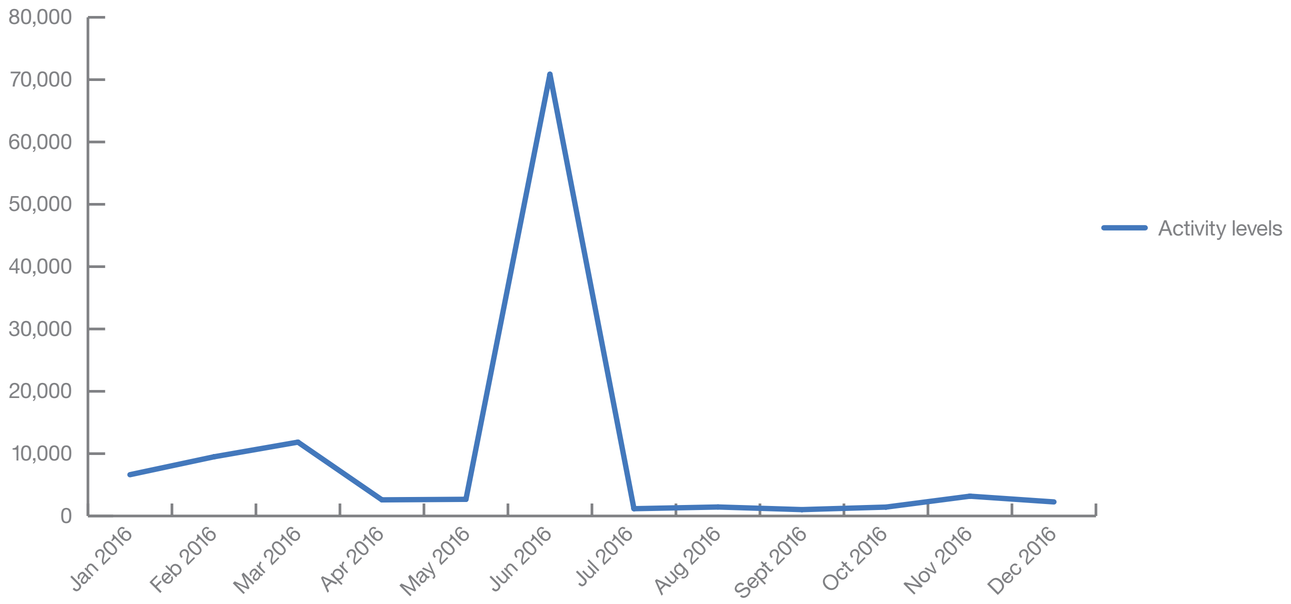


Figure 6. Neverquest activity trend line in the UK during 2016 (Source: IBM Trusteer)

Kronos arose in the UK in October 2015 and became one of the most active malware families to affect banks in the country during 2016 (see Figure 7).

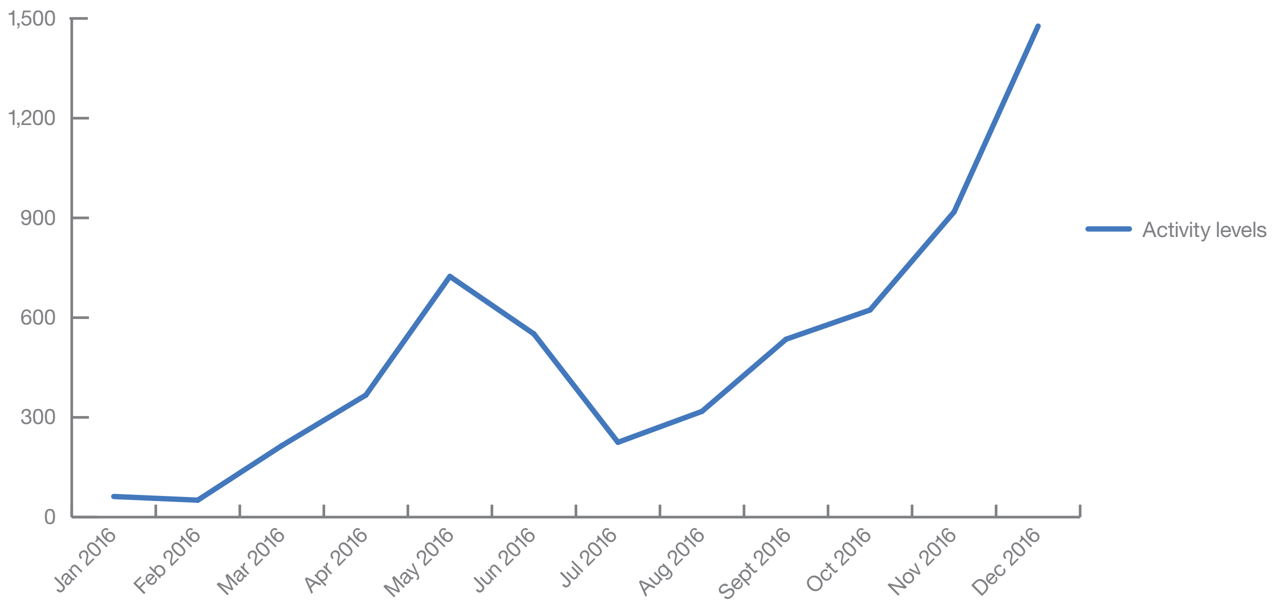


Figure 7. Kronos activity trend line in the UK during 2016 (Source: IBM Trusteer)

Dridex activity was constant throughout 2016 in the UK (see Figure 8).

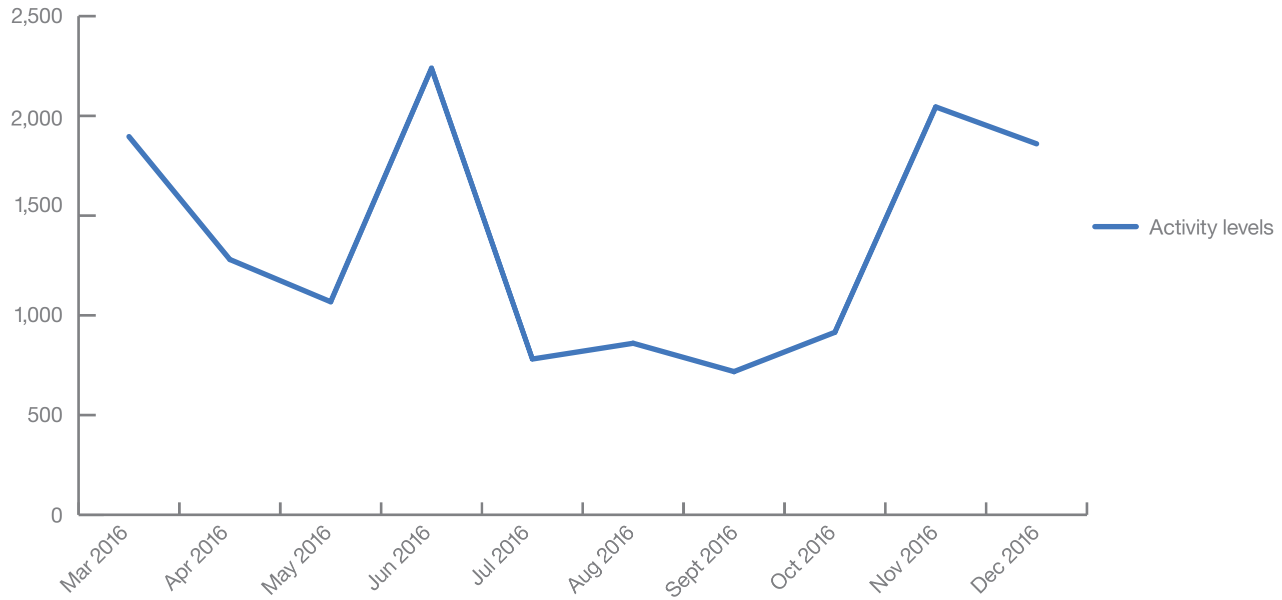


Figure 8. Dridex activity trend line in the UK during 2016 (Source: IBM Trusteer)

Shifu spread in the UK in September 2015 and became one of the stealthier Trojans to target banks in the country. Shifu's campaigns have become minimal but constant throughout the year in both the UK (see Figure 9) and Japan.

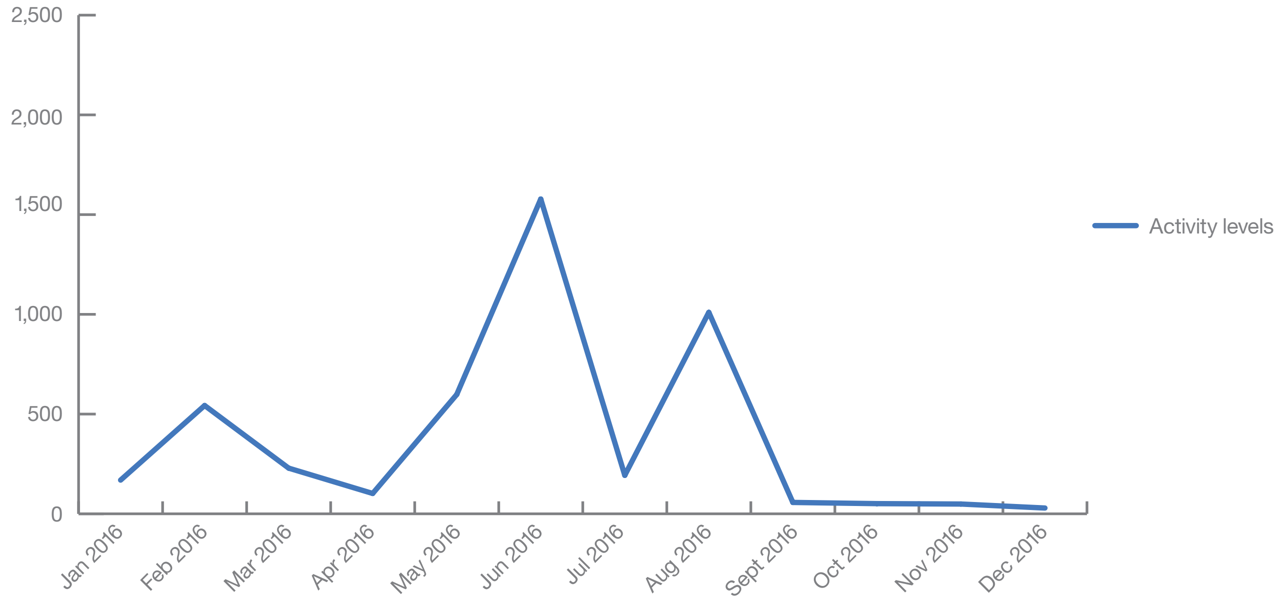


Figure 9. Shifu activity trend line in the UK during 2016 (Source: IBM Trusteer)

◄ Previous Next ►

Contents

GootKit was discovered in the summer of 2014 and is considered to be one of the most sophisticated banking Trojans active in the wild. GootKit is used in online banking fraud attacks on consumer and business bank accounts, mostly in the UK and other parts of Europe. GootKit was quite active in attacks against UK banks through 2016, with a sharp peak in March (see Figure 10). The UK was also targeted by mobile malware like Marcher and SpyLocker.

In the United States, the malware families shown in Figure 11 continued to be active throughout the year.

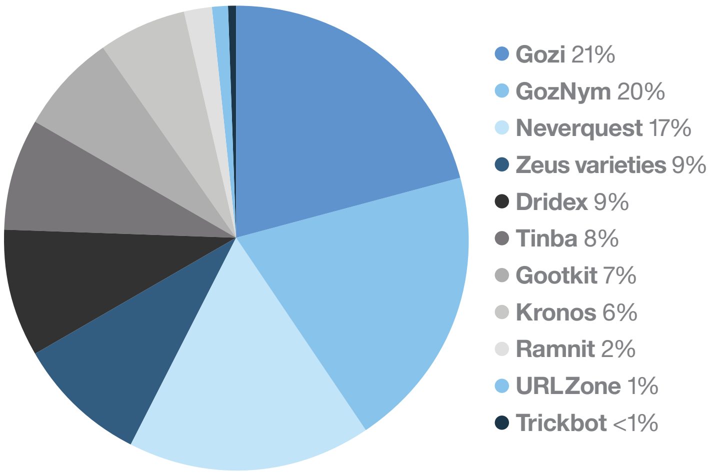


Figure 11. Top most active financial malware families in the US (Source: IBM Trusteer, 2016)

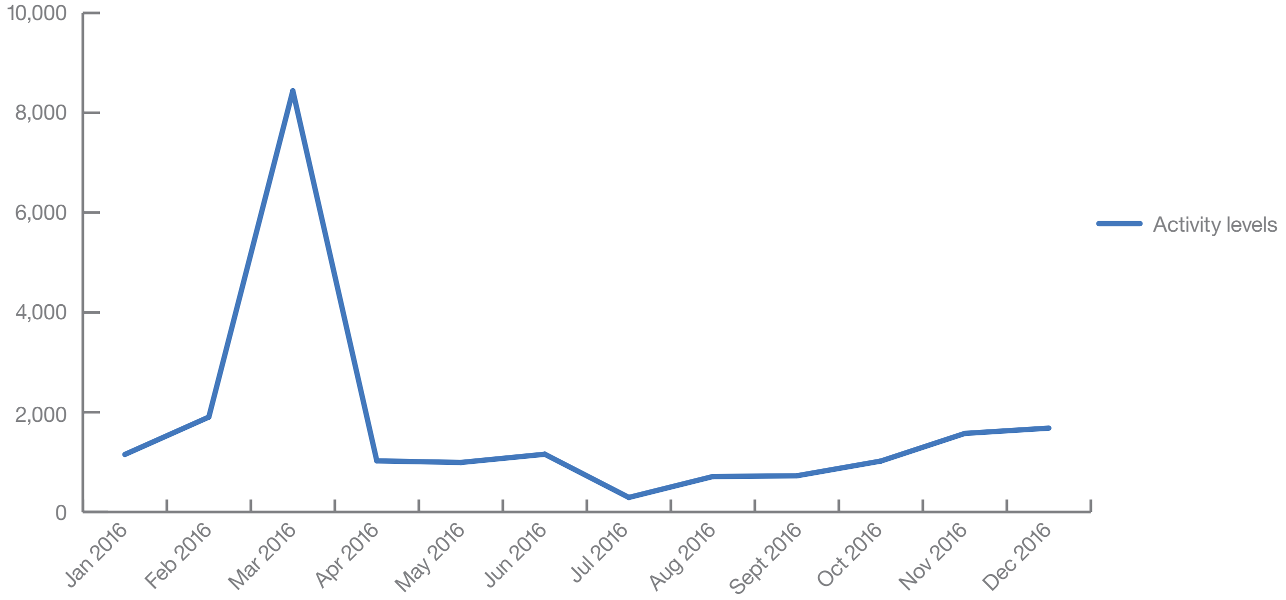


Figure 10. GootKit activity trend line in the UK during 2016 (Source: IBM Trusteer)

Dridex activity was fairly constant throughout 2016 in the US, peaking in March and December (see Figure 12).

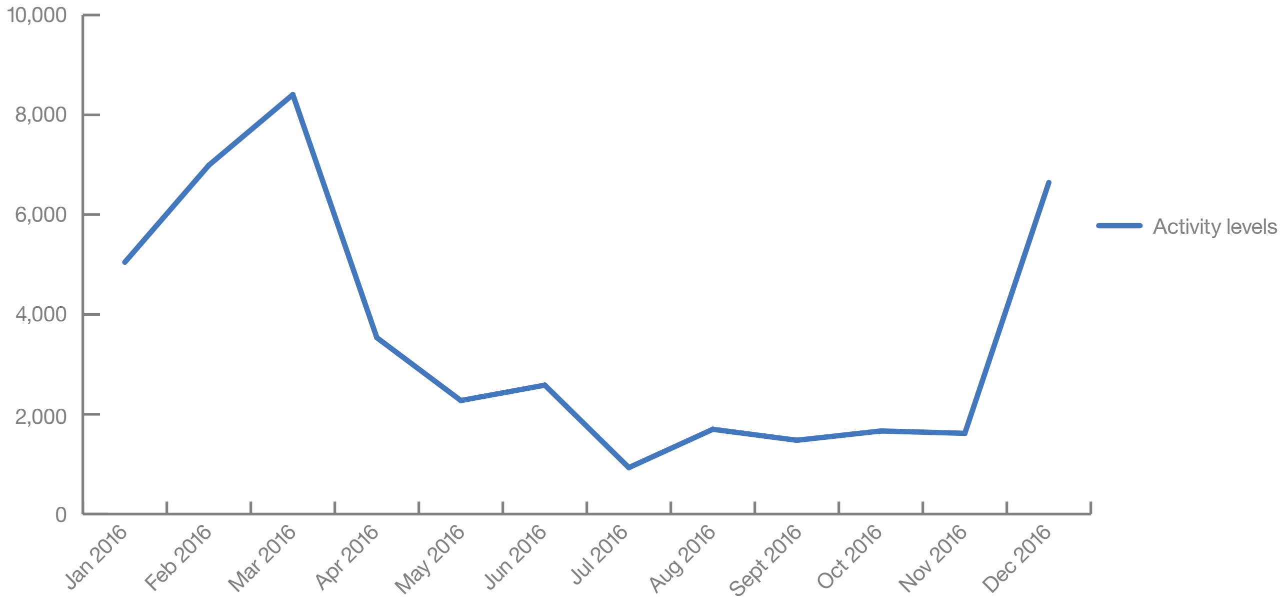


Figure 12. Dridex activity trend line in the US during 2016 (Source: IBM Trusteer)

◄ Previous Next ►

The **GozNym** gang has been focused on US banks since its emergence in April 2016. Its activity was notable through the rest of 2016 in the US, resulting in the arrest of some of one of its operating members in December 2016 (see Figure 13).

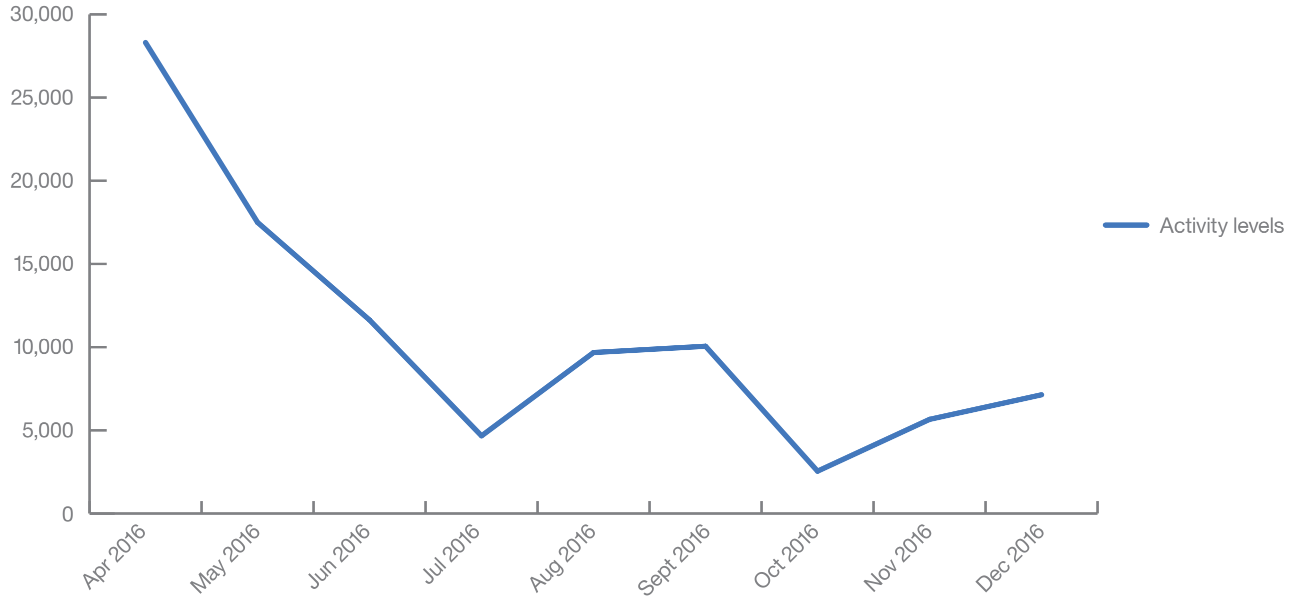


Figure 13. GozNym activity trend line in the US during 2016 (Source: IBM Trusteer)

According to X-Force data, **Neverquest** was the third most active malware in the US in 2016, with activity peaks in March, November and December 2016 (see Figure 14).

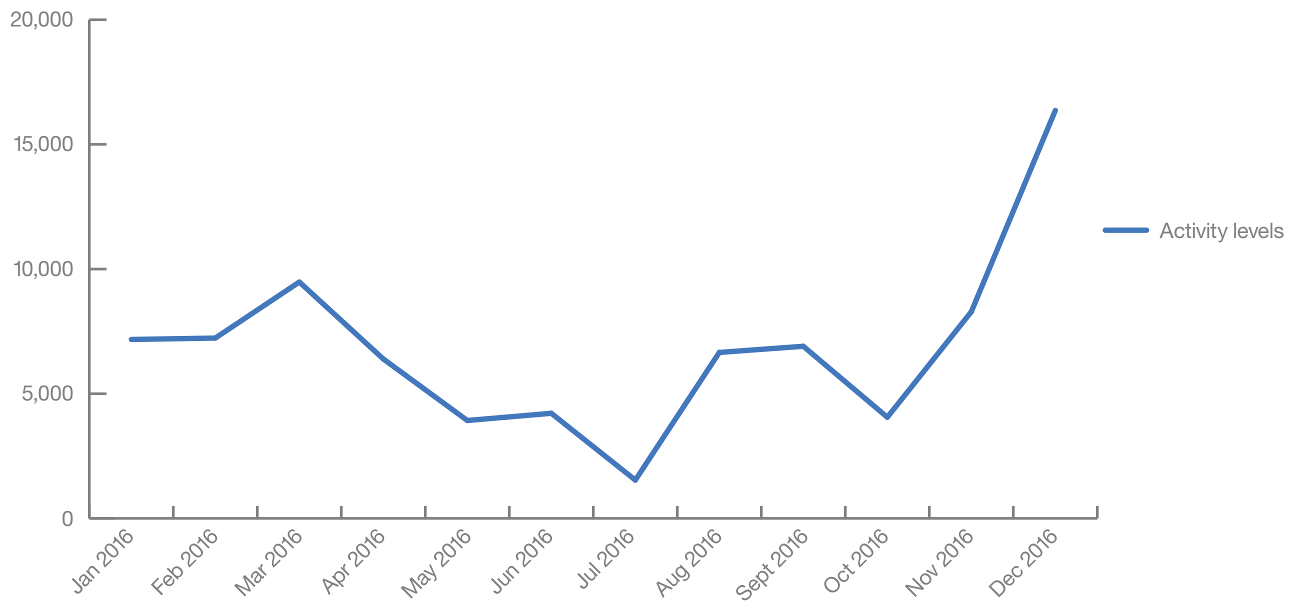


Figure 14. Neverquest activity trend line in the US during 2016 (Source: IBM Trusteer)

A trip to Asia

Asia, which has seen previous interest from malware like Dyre and Dridex, continued to attract organized cybercrime groups in 2016.

Two of the most prominent threats relevant to Asian countries are Dridex and TrickBot, both of which are operated by organized cyber gangs. Singapore is especially heavily targeted, but it's not the only country where these Trojans seek to attack; X-Force research analysis of configuration data shows that most malware families have targets in other parts of Asia such as Indonesia, India and Malaysia.

Dridex

Dridex has been targeting banks in Asia since 2015, mostly going after the credentials of business and corporate banking users. The locales most frequently featured in configurations are Singapore, Thailand, Hong Kong, China, Vietnam and Indonesia.[8]

TrickBot

TrickBot's appearance in Asia in the fourth quarter of 2016 was not very surprising, given its established resemblance to Dyre. If the two are indeed connected, target lists are among the first things they would share. TrickBot's configurations include redirection attacks on corporate banking in Singapore, Malaysia and India[9].

Rising interest in the UAE

Another geography increasingly present on Trojan configurations is the United Arab Emirates (UAE). X-Force data shows that organized gangs like the Dridex and the TrickBot crews are including more UAE banks on their target lists, as did Dyre before them.

This is notable because the UAE resembles Singapore in a sense: it is a global center of business, and its population is considered to have above average wealth. Also, businesses and individuals in the region tend to operate in both English and their local languages, allowing malware operators to employ their existing English-language attack tools.

Beyond the basics of infecting victims and stealing funds, it's possible that organized gangs from Eastern Europe are in contact with local crime groups—much like the modus operandi they use in Asia. Per X-Force data, the Emirates in the UAE most often targeted by organized malware gangs are Dubai and Abu Dhabi. Other targeted countries in the surrounding regions are Saudi Arabia, Qatar and Kuwait. Although it's not part of the UAE, Egypt sometimes shows up on the same list of targets.

Contents

Cybercrime in 2017 and beyond

Year-by-year shifts in the cybercrime arena do not necessarily mean that much is changing in the way online fraud works or the tools cybercrime gangs are using to work it. In 2017, cybercrime will probably present some new whats and wheres, but less likely show fundamental transformations.

The real change has to come from the defenders' side. The cybercriminal lifecycle has to be shortened to render it less and less lucrative over time. The faster we react to cybercrime findings and share them across the entire community, the less time each malware variant will realize successful fraud attacks. With increased vigilance, stronger detection and quicker reaction times, criminal operations can become much less financially viable for attackers. Fraudsters will be forced to abandon the field for lack of profit.

How IBM can help

IBM Trusteer® products help detect and prevent the full range of attack vectors responsible for the majority of online, mobile and cross-channel fraud. IBM Trusteer solutions deliver a holistic, integrated cybercrime fraud prevention platform designed to help prevent the root cause of fraud, improve the customer experience, reduce operational impact and utilize the global IBM X-Force threat intelligence service. IBM Trusteer Pinpoint™ Detect now incorporates behavioral biometrics, patented analytics and machine learning for real-time cognitive fraud detection. To learn more about how to protect your enterprise from evolving threats and cybercrime, visit IBM Trusteer Advanced Fraud Protection.

Defenders who respond quickly to attacks are the key to shortening the cybercrime lifecycle.

◄ Previous Next ►

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

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

[1] Configuration MD5 sampled: 9875438e51fad8286059405516d7268e

[2] Configuration MD5 sampled: C5ADC8EC369941CDF3DFC6B4E8BC799C

[3] Configuration MD5 sampled: 9ec4be5f422b1e26ff6150e2fd3415af

[4] Configuration MD5 sampled: 5e3e12b62c997d7df8693bea43084a90

[5] Configuration MD5 sampled: 5fbe0cb166d08c6890b7bda83bb2fdeb

[6] Configuration MD5 sampled: 533153fc63c009cfeaef61761e326868

[7] Configuration MD5 sampled: 66e693e7f8ef4e973ad4c29faa2ec657

[8] Configuration MD5 sampled: 7db9d1fbc438c44841be6aa322f08d2c

[9] Configuration MD5 sampled: 5596e9972bc1122ab8eb7e3f3b0f36ab

◄ Previous Next ►

Contents

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.