Customer Notification:

Zeus Panda Begins Targeting EU, NA Banks, Uses Web-Injections and ATS

Released July 13, 2016

PLEASE NOTE: This alert notifies affected customers about increased risk due to current attacks on their web applications, specifically where new advanced malware variants are involved.

Insights from IBM Trusteer Research

IBM Security Trusteer researchers report new **Zeus 'Panda'** (alias: Panda Banker) variants currently focused on targeting banks in Europe and North America. This is an advanced notice about the malware's modus operandi, as detected and analyzed by Trusteer research.

What's New Here?

A new Zeus v2 variant knowns as "Panda" is targeting the URLs of personal online banking services of banks in Europe and North America. The malware uses web-injection tactics, which include both technical changes and social engineering, to steal user credentials, take over victim accounts, and initiate fraudulent money transfers.

Target Geographies

Zeus Panda configurations target bank, payments, card services, airlines, and online betting brands in Europe and North America.

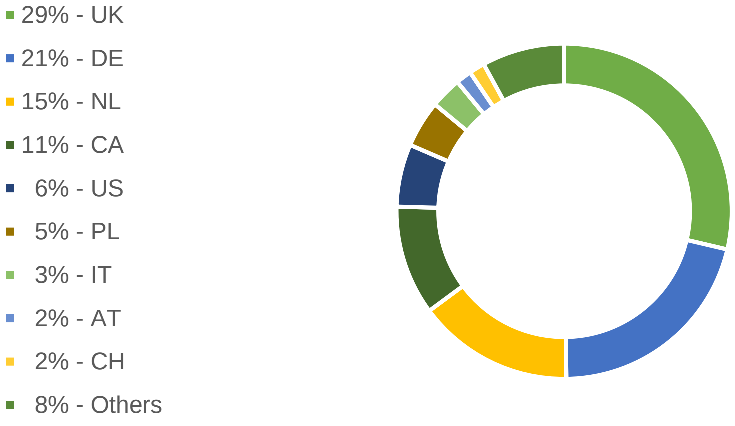


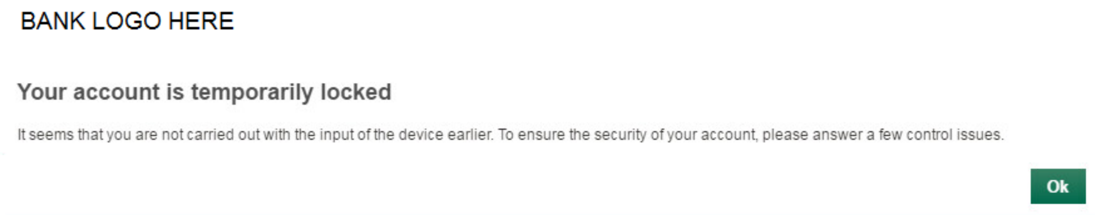
Figure 1: Zeus Panda's Geo Targets per Number of Brands in Each Country

Attack Details

The current attacks have been observed to actively deploy against European banking customers. The logical stages of the attack are described in this section, followed by further information about the Zeus "Panda" variation.

1. Zeus Panda's operators opt to infect users via drive-by downloads and poisoned email attachments using popular crime-as-a-service exploit kits (Angler/Nuclear/Neutrino). Campaign targets are filtered by geography, similar to the way the GozNym Trojan keeps irrelevant endpoints out of country-specific campaigns.
2. The malware attack begins as soon as the infected victim attempts browsing to a targeted web application. The malware hides the bank's genuine page using a CSS, and then sends a request to its command and control server requesting an external script.
3. The external script from the C&C is designed to replace the bank's original **Login** button with a malicious one, and then reveal the altered page to the victim.
4. When the victim enters their login credentials into the designated fields, and then click "Login", the malware changes the page's content and displays a fake message to the victim, claiming that their account has been locked.
5. Next, the malware pulls up other social engineering pop-up windows. When a victim goes through the process of supposedly 'unlocking' their account, the malware runs them through a different screens where it requires they key in a list of personally identifying information and payment card details according to each bank's authentication scheme.

Figures 2 through 4 show Zeus Panda's web-injections as they appear on the bank's website:

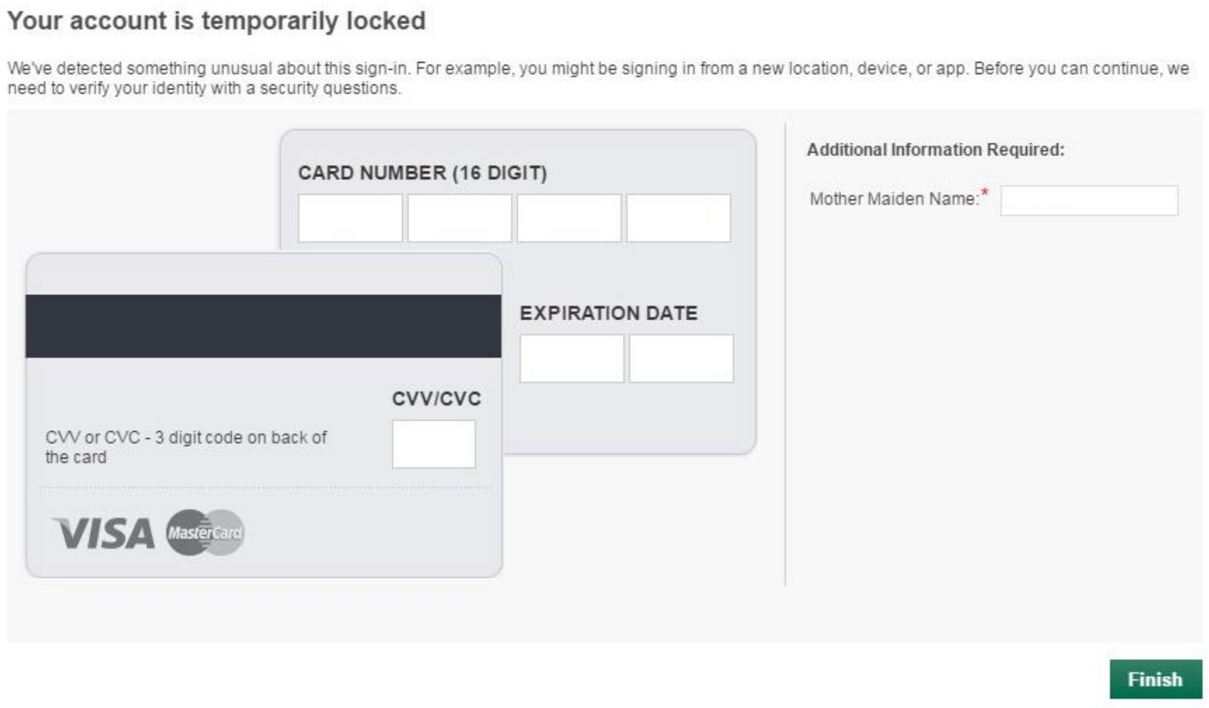


BANK LOGO HERE

Your account is temporarily locked

It seems that you are not carried out with the input of the device earlier. To ensure the security of your account, please answer a few control issues.

Figure 2: Zeus Panda Web-Injections Falsely Informing Victims Their Account is Locked



Your account is temporarily locked

We've detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity with a security questions.

CARD NUMBER (16 DIGIT)

EXPIRATION DATE

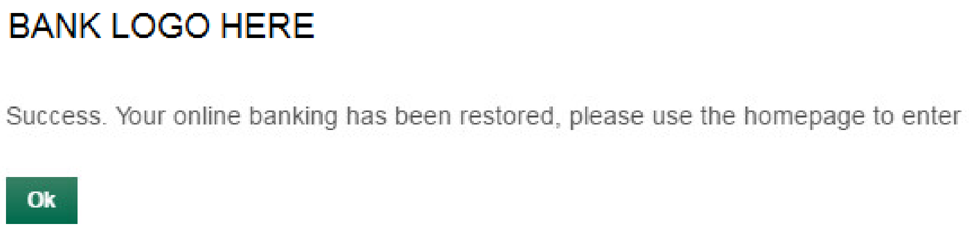
CVV/CVC

CVV or CVC - 3 digit code on back of the card

Additional Information Required:

Mother Maiden Name:*

Figure 3: Zeus Panda Web-Injections Requesting Victim Payment Card Details and PII



BANK LOGO HERE

Success. Your online banking has been restored, please use the homepage to enter

Figure 4: Zeus Panda Web-Injections Indicating the False Update Process is Complete

Throughout the web-injection process, the malware sends the stolen information to the C&C server at the completion of each separate page.

Upon consequent access to the bank’s website from the same infected machine, the login page still contains the malicious button and trigger web-injections. However, the botnet recognizes endpoints that already went through the process, and after the first time the victim enters their information into the malicious pop-ups, external scripts sent from the C&C will only remove the CSS hiding the bank’s genuine page and allow the victim to see the original content.

The actual fraud attempt will take place from a separate endpoint the fraudster controls.

About Zeus Panda

The variation dubbed Zeus “Panda”/Panda Banker emerged in early 2016. The malware is based on the Zeus VM code base, however, does not contain the virtual machine feature. The payload is typically ushered in by a malware downloader infection, and email spam campaigns related with Panda show that its operators target company employees rather than send indiscriminate spam to webmail addresses.

Zeus Panda’s deployment includes hooking the popular Internet browsers by implementing two sets of patches:

- One set is for IE and the Microsoft Edge browsers
- Another set is for Firefox and Google Chrome

To define its attack targets and injection choices, Panda’s modular structure fetches three separate configuration chunks:

The bot’s *initial configuration* arrives with its dropper, but web-injections, malware modules, and advanced configuration options are downloaded from C&C in separate configuration files; the latter can also be removed by the C&C per the botmaster’s choice.

Zeus Panda stores its malicious modules in encrypted form inside the Windows Registry. The web-injection configuration file is stored in an encrypted file on disk. Paths specifying the location of all malware files and Registry keys are stored inside the bot’s initial configuration chunk.

Notably, the botnet communicates over a fast flux network to obfuscate Panda’s actual infrastructure’s IP address(es). The malware checks for connectivity by browsing to the Russian Yandex.ru search engine, which could be a hint to its operators’ origins or whereabouts.

On top of its web-injection schemes, which are based on Zeus v2’s code, the Zeus Panda variant at hand further orchestrates fraudulent transactions through a web-injection control panel (ATS). The web-based panel provides its malicious operators with a Jabber-based instant notification interface to alert the fraudster when new transactions are underway.

Malware IOCs

Relevant Sample MD5

- e9dd9705409df3739183fb16583686dd
- a181627930c77fcf17efaf69081e3194
- b83fe966bda5918e31df6d15b4330367
- c4b31419e90c4e83d265096304408d41
- e9dd9705409df3739183fb16583686dd

AV Detection Aliases

Anti-virus engines take a while to detect Zeus Panda, and in most cases do not detect it accurately. Some of the aliases by top AV engines for this variant are:

- Trojan-FIDB!E9DD9705409D
- Trojan:Win32/Dynamer!ac
- Trojan-Spy.Win32.Panda.d

Global Perspective

The chart in Figure 5 lists the most prolific banking malware families globally, in 2016 YTD. Zeus variations rank third on the top ten list, with different cybercrime factions operating Trojans based on the leaked Zeus v2 code. Zeus Panda joins various Zeus VM, Zeus Maple, Citadel, and Atmos builds, to name a few.

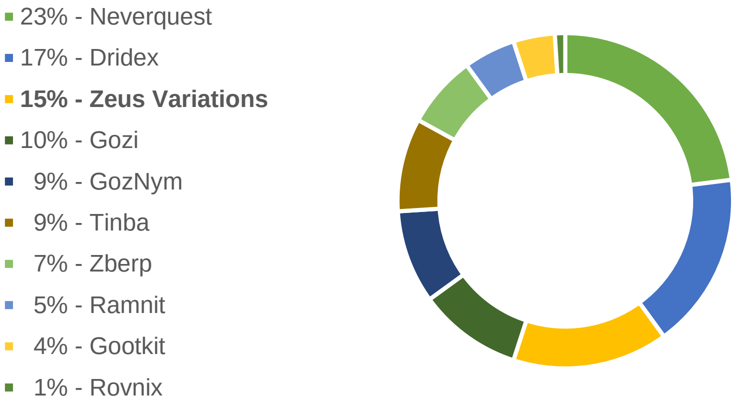


Figure 5: Top Most Prevalent Financial Malware Families (1H2016)

Current Protection Status for This Threat

IBM® Security Trusteer Rapport® – Updated to prevent Zeus Panda fraud on customer endpoints.

IBM® Security Trusteer Pinpoint™ Detect – Active detection and Passive in some customer deployments.

All IBM Trusteer products versions are updated in real time and able to detect and stop Zeus Panda's malicious activity in the web browser, on endpoints, and ATO facilitated by Zeus Panda, providing customers with effective protection against this threat.

For more information about Pinpoint™ Detect protection mechanisms, anti-fraud rules, and fraud intelligence that make for the detection of account takeover fraud, please contact our Enterprise Support team at: enterprise.support@trusteer.ibm.com

About IBM® Security Trusteer® Solutions

With IBM® Security Trusteer® solutions, financial organizations gain access to a real-time malware intelligence network that provides insight into fraudster techniques and capabilities. This global threat intelligence serves as the foundation for IBM Security Trusteer automated threat protection capabilities, and is used by IBM Security experts to help develop and deliver new protections for organizations like yours.

At IBM, a research and development (R&D) team of security experts scrutinizes threat intelligence as it arrives from both Trusteer-protected endpoints, as well as underground cybercrime venues. IBM Security Trusteer solutions use this intelligence to deliver flexible protection layers that can be rapidly configured and updated by IBM R&D staff. As a result, as soon as new threats emerge or mutate, new countermeasures are automatically deployed back into Trusteer software without any intervention by bank security staff and without any noticeable impact to banking customers.

If you have any questions, contact our Enterprise Support team at:
enterprise.support@trusteer.ibm.com