# Panda Malware Broadens Targets to Cryptocurrency Exchanges and Social Media

By Authors & ContributorsDoron Voolf (Author)Malware Analyst, F5About DoroncloseAll Articles

Archived: 2026-04-05 18:29:10 UTC

Seven years after it first appeared, the Zeus banking trojan is still active through its latest spin-off: Panda. Panda, first discovered in early 2016 by Fox IT and later analyzed by Proofpoint,[1] spreads through phishing attacks and targets Windows operating systems (OS). Its main attack techniques include web injects, screen shots of user activity (up to 100 per mouse click), logging of keyboard input, Clipboard pastes (to grab passwords and paste them into form fields), and exploits to the Virtual Network Computing (VNC) desktop sharing system. All of these attack methods are supported by ATSEngine,[2] which Ramnit, another prolific banking trojan, also used in its 2017 holiday campaign.

- Panda is primarily focused on financial services organizations, but it is expanding its industry targets with each new campaign.
- Panda was heavily focused on cryptocurrency sites in February.
- Panda is currently targeting Facebook and Twitter in all three campaigns active in May.
- There are different C&Cs for each campaign, three of which are connected through a known threat actor network in Russia, the fourth is hosted in China.

We analyzed four campaigns that were active between February and May of 2018. The three May campaigns are still active at the time of this writing. Two of the four campaigns are acting from the same botnet version but have different targets and different command and control (C&C) servers.

Panda is still primarily focused on targeting global financial services, but following the worldwide cryptocurrency hype, it has expanded its targets to online cryptocurrency exchanges and brokerage services. Social media, search, email, and adult sites are also being targeted by Panda.

*Figure 1: Panda campaign targets by industry*

The campaigns that targeted Italian, US, and Canadian financial organizations were the same ones that targeted cryptocurrency sites. The campaign that focused on Japanese financial organizations had the broadest set of industry targets. Across all campaigns in May, the same social media, search, email, ecommerce, and tech providers were targeted.

*Figure 2: Panda industry targets by campaign*

Adult sites were also targeted by Panda in May. We have been seeing an expansion of banking trojan targets into other industries that collect payment information and other forms of personally identifiable information (PII), so

this behavior is not surprising given the size of the adult industry and potential revenue generation for fraudsters.

## February Campaign - Botnet “Onore2” Targets Italian Financial Services and Cryptocurrency Sites Equally

The Panda configuration we analyzed from February was marked as botnet “onore2.” This campaign leverage the same attack techniques as previously described, and it is able to keylog popular web browsers and VNC in order to hijack user interaction session and steal personal information.

*Figure 3: Italian campaign, botnet Onore2 dynamic configuration*

The Onore2 campaign targeted two industries: financial services and cryptocurrency sites. The majority of the targets were financial services sites in Italy at 51%, followed closely by cryptocurrency targets used worldwide at 49%.

*Figure 4: The February Panda Onore2 campaign targeted Italian financial services and cryptocurrency sites*

The cryptocurrency sites Panda focused on in February were primarily targeted through screenshots versus the typical web inject. We assume this was to document and spy on user interaction at cryptocurrency accounts, side by side to the web injection list. The list of cryptocurrency sites targeted includes but is not limited to:

- Anycoindirect.eu
- Btcc.com
- Bitstamp.net
- Bethumb.com
- Bitpanda
- Bitbey.net
- Bity.com
- Blockchain.info
- Cex.io
- Coinbase.com
- Coinsbank.com
- Cryptocompare.com
- Exmo.com
- Gatecoin.com
- Gdax.com

- Hitbtc.com
- Holytransaction.com
- Kraken.com
- Litebit.eu
- Livecoin.net
- Localbitcoins.com
- Minergate.com
- Okcoin.com
- Slushpool.com

The financial services sites included in the Onore2 campaign were targeted through webinjects and socks. They included but were not limited to:

- Allianzbank.it
- Bcc.it
- Bnl.it
- Bancacrfirenze.it
- Bancagenerali.it
- Bankingforyou.it
- Carifvg.it
- Caript.it
- Cedacri.it
- Credem.it
- Csebo.it
- Icb.mps.it
- Inbank.it
- Poste.it
- Relaxbanking.it
- Tecmarket.it

### Command and Control (C&C) Servers

The C&C server for this campaign is: hxxps://0a109ec2ab47[.]com/. Note the use of HTTPS for the malware phoning home through encryption to hide its exploits from traditional intrusion inspection controls.

*Figure 5: Italian campaign C&C Whois*

The domain is registered through Namesilo.com to a registrant with a fake address in the US, and an email contact at minex-coin.com. Minex-coin is also registered with Namesilo.com, but the Whois is privacy protected. The name servers are in Russia: samara.ens.mail.ru under a provider (ASN 47764) that comes up often in F5 Labs' threat research.

## May Campaign - Botnet "2.6.8" Targets US Financials

The latest sample analyzed from May 1, 2018 was marked as botnet "2.6.8". Comparing this botnet configuration to the Onore2 campaign and the other 2.6.8 campaign targeting Japanese financials (see next section), it has a different C&C address, and a "keylog_process." Instead of adding the Internet browsers, "putty.exe" was added.

*Figure 6: US campaign "2.6.8" dynamic configuration*

This is not the first time Panda has targeted US-based financial organizations. This campaign had targets in 8 industries, 76% of which were US financial organizations. This campaign also targeted half a dozen Canadian financial organizations, followed by cryptocurrency sites, global social media providers, search and email providers, payroll, entertainment, and tech providers.

*Figure 7: May Panda campaign "2.6.8" targets US and Canadian financial services, social media, search and email providers, cryptocurrency sites, and payroll sites*

Panda is hitting the typical large financial targets in the US, such as:

- Adp.com
- Bankofamerica.com
- Citi.com
- Paychex.com
- Wellsfargo.com

The Canadian financial organizations targeted are:

- bmo.com
- desjardins.com
- royalbank.com
- scotiabank.com

The cryptocurrency sites targeted are:

- Blockchain.info
- bbt.com

This campaign is also targeting major social media platforms like Facebook and Instagram, as well as messaging apps like Skype, and entertainment platforms like Youtube. Additionally, Panda is targeting Microsoft.com, bing.com, and msn.com.

**C&C Server**

The C&C server for this campaign is: hxxps://adshiepkhach[.]top/. Note the use of HTTPS again to hide from traditional intrusion inspection controls.

The registrant is in Russia. The domain for the email contact is bk.ru, which is owned by the same ASN 47764 that continually comes up in our threat research.

*Figure 8: US Campaign C&C Whois*

## May Campaign - Botnet “2.6.8” Also Targets Japanese Financials

This sample was also analyzed from May 1, 2018 and was also marked as botnet “2.6.8”. Comparing the two botnet configurations, there is an interesting change: when Zeus.Panda is targeting Japan, the authors removed the Content Security Policy (CSP) headers: remove_csp - 1 : The CSP header is a security standard for preventing cross-site scripting (XSS), clickjacking and other code injection attacks that could execute malicious code from an otherwise trusted site.[3]

*Figure 9: Japan campaign ”2.6.8” dynamic configuration*

In parallel with the US targeted campaign, this Panda campaign is targeting the following Japanese financial services organizations, most of which are credit card providers:

- saisoncard.co.jp
- idemitsucard.com
- mufg.jp
- aeon.co.jp
- lifecard.co.jp
- pocketcard.co.jp
- cedyna.co.jp
- eposcard.co.jp

- orico.co.jp
- rakuten*.co.jp
- smbc-card.com

This campaign also targets the ecommerce giant Amazon; entertainment platform Youtube; Microsoft.com, Live.com, Yahoo.com, Google.com, likely targeting email accounts; the social media leaders Facebook and Twitter; as well as a Japanese adult site Dmm.co, and Pornhub.

*Figure 10: May Panda "2.6.8" campaign targets Japanese financial services, search and email providers, social media, and adult sites*

**C&C Server**

The C&C server for this campaign is: hxxps://antrefurniture[.]top/. Again, note the use of HTTPS to hide activity from traditional intrusion inspection controls. It's also a .top top-level domain (TLD) like the US campaign. Spamhaus.org says 40% of .top TLDs are used for abusive purposes.[4]

The registrant is also in Russia, and the domain for the email contact is bk.ru like the US campaign, which again is owned by ASN 47764 that continually comes up in F5 Labs' threat research.

*Figure 11: Japan campaign C&C Whois*

## May Campaign - Botnet "Cosmos3" Targets Latin America Financial Services

The third parallel attack campaign, marked as botnet "cosmos3," is currently active and targeting financial institutions in Latin America.

*Figure 12: LATAM campaign "Cosmos3" dynamic configuration*

This campaign primarily focused on banks in Argentina, Columbia, and Ecuador, followed by the same social media (Facebook, Twitter, Instagram, Flickr), search, email (MSN, Bing), entertainment (YouTube) and tech provider (Microsoft) targets as the other campaigns.

*Figure 13: May Panda "Cosmos3" campaign targets LATAM financial services, social media, search, email, and tech providers*

The Latin American targets in this campaign are:

- avvillas.com.co
- bbvanet.com.co
- bancodebogota.com
- bancocredicoop.coop
- bancopatagonia.com.ar

- banco.colpatria.com.co
- davivienda.com
- pichincha.com
- santanderrio.com.ar
- transaccionesbancolombia.com

**C&C Server**

The C&C server for this campaign is: hxxps:// cotrus[.]co/. Note the use of HTTPS again to hide from traditional intrusion inspection controls.

The domain is registered in China. The email registrant domain GMZ.com resolves to the German service provider 1&1.

*Figure 14: LATAM campaign C&C Whois*

## QA in Production Tests

Continual maintenance is required to keep the fraud operations going and making money. Like any business, this involves testing, and sometimes testing in production like we saw in this campaign where the threat actors were infecting computers with different versions of the configuration.

This testing in production was against campaign 2.6.1 and had minor changes from the Onore2 campaign:

- “onore2” botnet was configured to grab cookies and cache
- “2.6.1” was marked to delete cookies and cache
- Grabber pause was marked 2, which is the indication on how long panda grabber will wait before starting the actual module.
- Grabber flags:
    - Grab_del_cookie - 0
    - Grab_del_cache - 0

*Figure 15: QA Test “2.6.1” dynamic configuration*

To make sure the injection was working correctly, the Panda authors tested against an Australian domain. Once the URL was detected, it sent an injection JS alert “Page Injected!”

*Figure 16: QA Injection alert, “Page Injected!”*

## Conclusion

Panda's expansion beyond traditional banking targets is following the trend we noticed during the 2017 holiday season.5 This is the first campaign we have seen targeting cryptocurrency sites, but it's a move that makes sense, given the popularity of cryptocurrency. This act of simultaneous campaigns targeting several regions around the world and industries indicates these are highly active threat actors, and we expect their efforts to continue with multiple new campaigns coming out as their current efforts are discovered and taken down. We will continue to look for patterns by monitoring this activity and the networks and services from which they are choosing to launch their activities. In the meantime, we highly recommend all businesses maintain up-to-date patches on endpoints and ensure AV controls are continuously updated so their systems don't get infected with this malware. To protect your business from infected consumers that cause costly fraud investigations, monetary returns, and so on, we recommend instituting advanced web fraud protections because this customized security control is not just for banks anymore!

## Indicators of Compromise

MD5

Italy and cryptocurrencies targets — e9d881b40d94a541b11fad44f1efbb7c

USA — 35a7e666942eb0c70e73d5dc502a97d2

Japan — 3b78b983ed00cfa580c0b1c9beda4ca2

Latin America — 8822dc8e66b51344b623c6cd29a91db1

QA in production — 5d4c4668567b0b3321b0125779bdb3ae

C&C servers

Italy: hxxps://0a109ec2ab47[.]com

US: hxxps://adshiepkhach[.]top

Japan: hxxps://antrefurniture[.]top

Latin America: hxxps://cotrus[.]co

---