Criminals in a festive mood

By Global Threat Intelligence

Published: 2017-12-12 · Archived: 2026-04-05 17:07:43 UTC

This morning the Fox-IT Security Operations Center observed a large number of phishing e-mails that contained a link to a downloadable zip file. Anyone downloading and opening that zip file would infect themselves with banking malware, that would subsequently try to lure the victim into divulging their credit card information.

So far nothing new: e-mail as attack vector, distribution of the Zeus Panda banking trojan, targeting the same institutions.

Except that this time, it appears the criminals are preparing for the festive season. What stood out to us is the inclusion of a number of local retailers that are now targeted by this banking trojan. Some targeted websites which were extracted from the configuration are:

- Coolblue
- Booking.com
- Otto
- Amazon
- De Volksbank (SNS, ASN & Regiobank)
- ING
- ABN Amro
- Knab
- Triodos

So now, when someone has infected themselves with this malware by opening the malicious zip file, not only will the malware ask for their credit card details when they visit their bank's website, but also when they visit an online retailer for (Christmas) shopping.

Read on for recommendations, notable observations, stats and screenshots and technical details including indicators of compromise.

Recommendations

The usual recommendations for end users apply: be alert for criminals attacking you by sending legitimate looking e-mails with links and attachments. And be alert for websites behaving differently and asking for credit card details or other personal data where they normally don't. If you suspect an infection, you may check out a website from a different device to see if it behaves the same. If it doesn't, you may be infected.

The e-mail itself is nothing out of the ordinary. It appears to be targeting the Netherlands and Germany, using Dutch text and faking the Dutch DHL Group. This is what it looks like:

> Beste heer/mevrouw,
> UW ZENDING IS ONDERWEG ,Informatie Over Uw Zending is in dokument.
>
> Controleer hieronder uw zending- en contactgegevens. Klik op om te bevestigen.
> Bedankt dat u heeft gekozen voor On Demand Delivery.
> DHL Express – Excellence. Simply delivered.
> Nederlandse Post DHL Group

For organisations, the recommendations are also familiar: isolate any infected systems prior to cleaning them, change any password that was used after infection and consider client certificates on that system compromised. You may refer to the indicators of compromise later on in this post.

Additional interesting observations
The malware that is being distributed is called Zeus Panda, which we've followed for almost two years now. This is a variant of the Zeus family of malware that Fox-IT has observed since around 2006, for the purpose of protecting its own customers. The name Zeus Panda comes from the web panel used by the malware operators.

At the time of writing, the two malicious zip file referred in the emails received a little over 48 thousand clicks, mostly in the Netherlands, but also in other parts of Western Europe and some in North America. Out of those 48 thousand clicks, only 11 thousand came from a Window system, which is the only platform that the malware runs on. The other 37 thousands people were safe! A clear example and proof of the shotgun approach that criminals still successfully use.

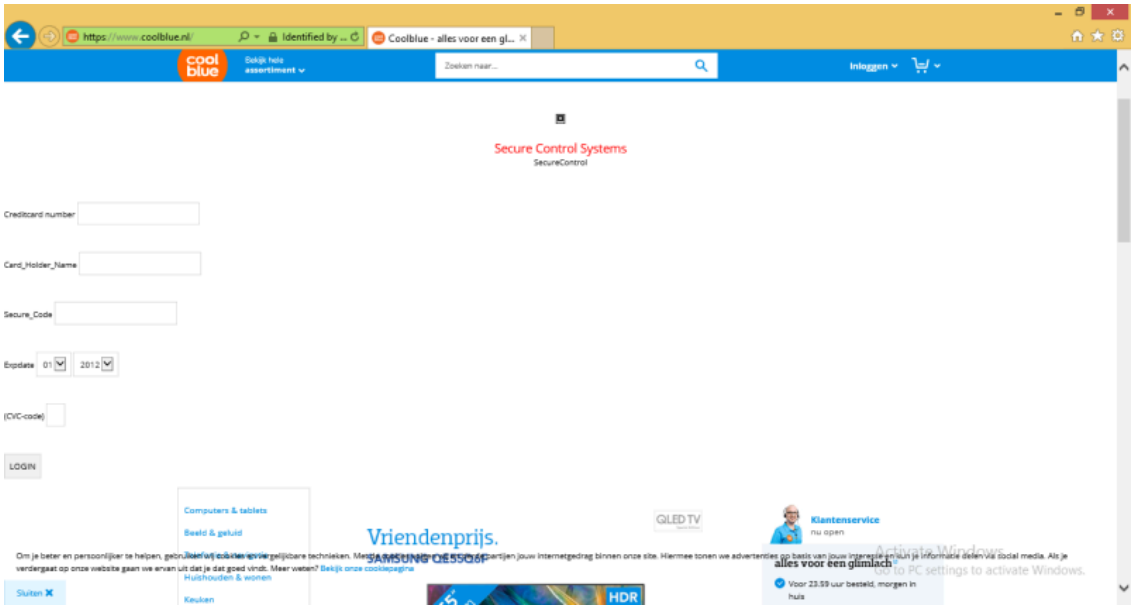
Also interesting is the clunky nature of the injects. As shown in the screenshots below, the code that the criminals inject into the website on the infected system looks, well, unfinished.

Full statistics
The link in the email is a Google Shortened URL, which downloads the zip-file from
hxxp://partytimeevents.nl/contactgegevens%2012_2017_10_00_.zip
hxxp://stegengaweb.nl/files/contactgegevens%2012_2017_10_00_.zip

By default Google shortened URL's keeps track of the following statistics:
– Amount of clicks
– Used Browsers
– Referrers
– Countries
– Platforms

Requesting the statistics of the shortened URL results in the following statistics for:

Screenshot of the inject asking for credit card details
From an infected system, Zeus Panda will inject extra code into a website. Once the code is injected into one of the targeted web pages, an extra form is added for creditcard information. For example, Coolblue's webshop page would look like this, clunky and unfinished. Please note that Coolblue has no control over the fact that criminals attempt to inject code into their website from infected machines.



Zeus Panda Banker web inject

EDIT: *the total click count for both domains has increased to a total of 66 thousand, even though both ZIP-files are not available anymore.*

> **Indicators of Compromise**
>
> —Dropper—
> hxxp://partytimeevents.nl/contactgegevens%2012_2017_10_00_.zip (compromised website)
> hxxp://stegengaweb.nl/files/contactgegevens%2012_2017_10_00_.zip (compromised website)
> hxxp://axprofessional.it/onenl.exe
>
> —Command-and-Control—
> hxxps://avimart.ru/3inexowtoqiyzlonyunku.dat
> hxxps://astronatal.ru/2odirnaogfaugdoxiwoex.dat
> hxxps://abci.ru/1yhubydnopyakleqinyyx.dat
> 185.224.133.57 (SSL connection)
>
> —External panel for injects—
> hxxps://adsfun.club/
>
> —Hashes—
> contactgegevens 2012_2017_10_00.zip
> MD5: aefc0fe15836165291cb66eac5ffd177
> SHA256: 588e31ac96bd6318f787602e87f86b75d4b5537679e11ba5a509589148033275
>
> contactgegevens 12_2017_10_00_.js
> MD5: deb9a0aa69270a0b263b80ed13880b24
> SHA256: eb65b1d5f5b3ccc263a4984275c084b63b0a262a87d55887d6a4d744a75e4112
>
> onenl.exe
> MD5: 4ac38a4efa276f8d64c1ed39a53e7ab8

> SHA256: e556273db50d4588d7e4b5183d06d39b0ebedbb094fc2a39b59416212c829324

Published December 12, 2017December 13, 2017
