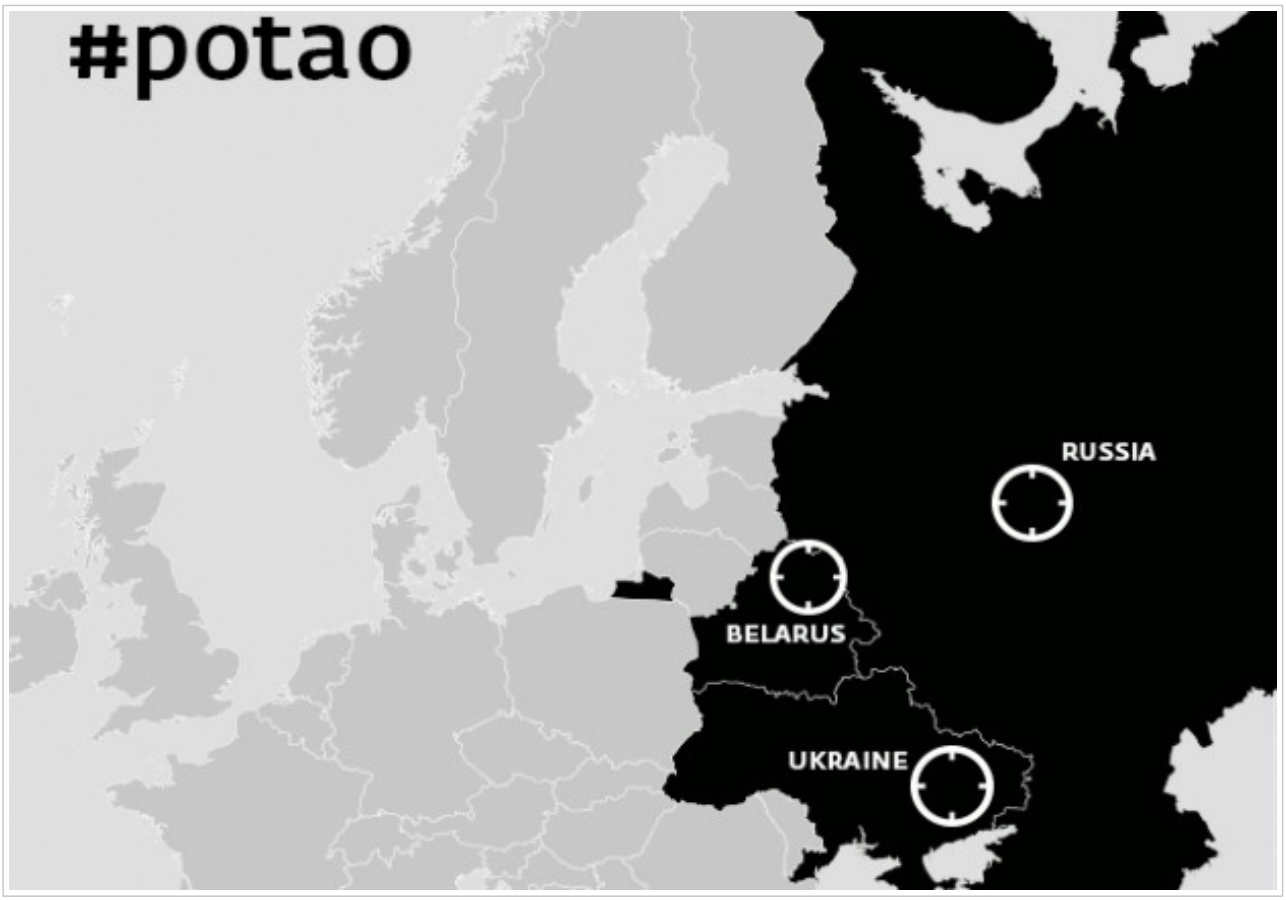
welivesecurity
News, views, and insight from the ESET security community

Operation Potao Express: Analysis of a cyber-espionage toolkit

BY ROBERT LIPOVSKY AND ANTON CHEREPANOV POSTED 30 JUL 2015 - 10:49AM



Attackers spying on high-value targets in Ukraine, Russia and Belarus, and their TrueCrypt-encrypted data

We presented our initial findings based on research into the **Win32/Potao** malware family in June, in our **CCCC 2015** presentation in Copenhagen. Today, we are releasing the **full whitepaper** on the Potao malware with additional findings, the cyberespionage campaigns where it was employed, and its connection to a backdoor in the form of a modified version of the TrueCrypt encryption software.

Like **BlackEnergy**, the malware used by the so-called Sandworm APT group (also known as Quedagh), Potao is an example of targeted espionage malware directed mostly at targets in Ukraine and a number of other post-Soviet countries, including Russia, Georgia and Belarus.

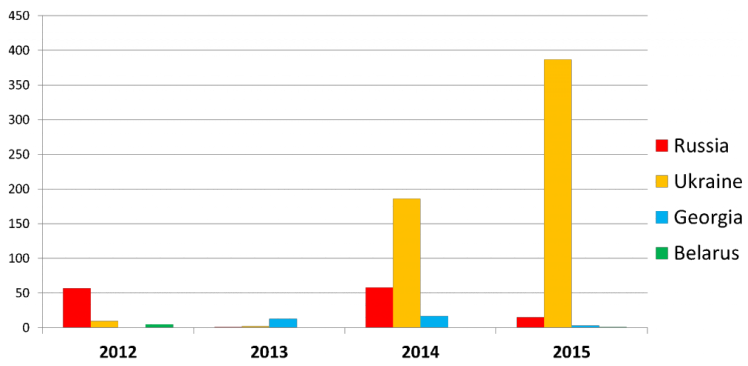


Figure 1- Detection statistics for Win32/Potao according to ESET LiveGrid®

Attack Timeline

The attacks conducted using the Win32/Potao malware family span the past 5 years, the first detections dating back to 2011. The attackers are, however, still very active, with the most recent infiltration attempts detected by ESET in July 2015.

The timeline below lists a selection of Potao attack campaigns and other related events.

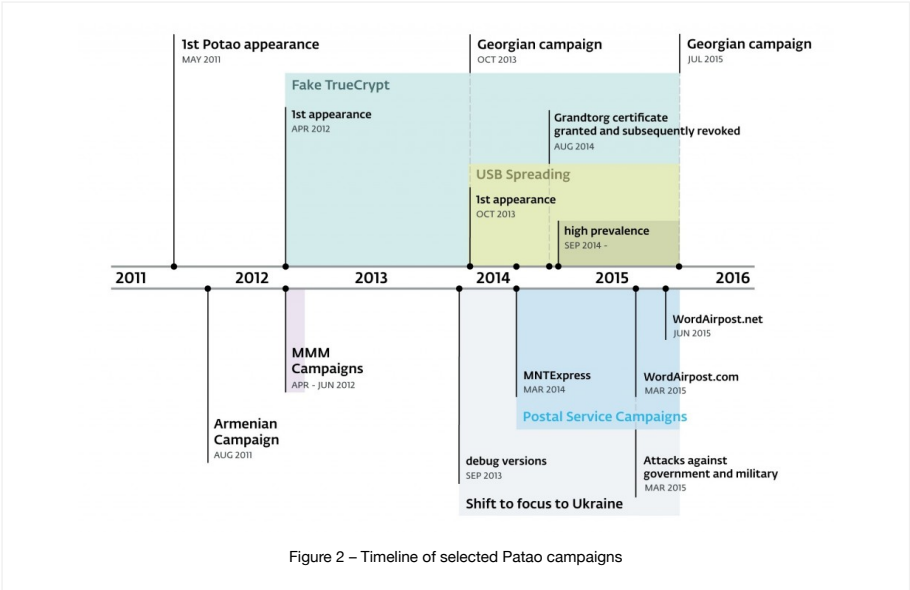


Figure 2 – Timeline of selected Patao campaigns

Among the victims identified, the most notable high-value targets include Ukrainian government and military entities and one of the major Ukrainian news agencies. The malware was also used to spy on members of **MMM**, a Ponzi scheme popular in Russia and Ukraine.

Malware Techniques

When the criminals shifted their focus from attacking targets in Russia to others in Ukraine, they began sending personalized SMS messages to their potential victims to lure them to landing pages hosting the malware, disguised as postal tracking sites.

We haven't noticed Win32/Potao employing any exploits and the malware isn't particularly technically advanced. (Shouldn't call it an *APT* then, right?) Yet it does contain a few other interesting techniques that 'get the job done', like the mechanism for spreading via USB drives and disguising executables as Word and Excel documents, as in the following examples:

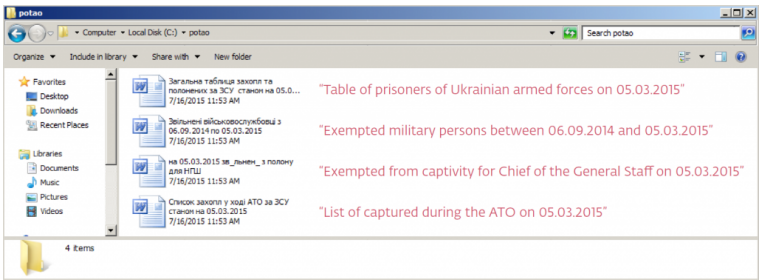


Figure 3 – Potao droppers with MS Word icons and file names used in attacks against high-value Ukrainian targets to capture the interest of recipients

Trojanized TrueCrypt

An (A)PT malware family that has gone relatively unnoticed for five years and that has also been used to spy on Ukrainian governmental and military targets is certainly interesting in and of itself. However, perhaps the most attention-grabbing discovery related to this case was when we observed a connection to the popular open-source encryption software, TrueCrypt.

We found out that the website *truecryptrussia.ru* has been serving modified versions of the encryption software that included a backdoor to selected targets. Clean versions of the application are served to normal visitors to the website, i.e. people who aren't of interest to the attackers. ESET detects the trojanized TrueCrypt as **Win32/FakeTC**. TrueCrypt Russia's domain was also used as a C&C server for the malware.

Figure 4 – TrueCrypt Russia's Website

The connection to Win32/Potao, which is a different malware family from Win32/FakeTC, is that FakeTC has been used to deliver Potao to victims' systems in a number of cases.

FakeTC is not, however, merely an infection vector for Potao (and possibly other malware) but a fully functional and dangerous backdoor designed to exfiltrate files from the espionage victims' encrypted drives.

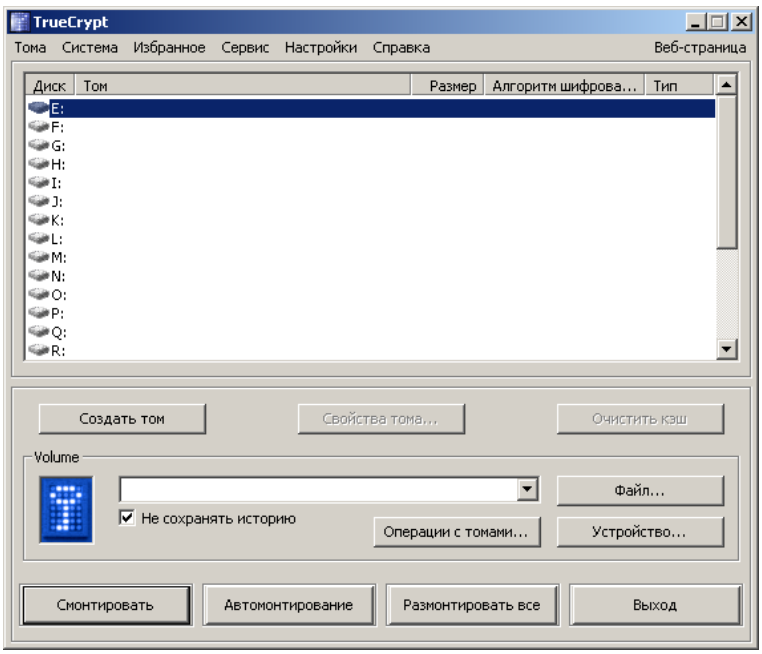


Figure 5 – Interface of the trojanized Russian TrueCrypt

In addition to the selective targeting (deciding to whom to serve the trojanized version instead of the clean one), the backdoor code also contained triggers that would only activate the malicious data-stealing functionality for active, long-term TrueCrypt users. These were surely contributing factors to the malware's going unnoticed for such a long time.

Further details on both Win32/Potao and Win32/FakeTC, including a technical analysis of the malware, description of plugins, infection vectors, C&C communication protocol and other spreading campaigns not mentioned in this blog post are included in our comprehensive whitepaper.

Indicators of Compromise (IOC) that can be used to identify an infection can be found in the whitepaper or on github:
https://github.com/eset/malware-ioc/tree/master/potao