Slave, Banatrix and ransomware

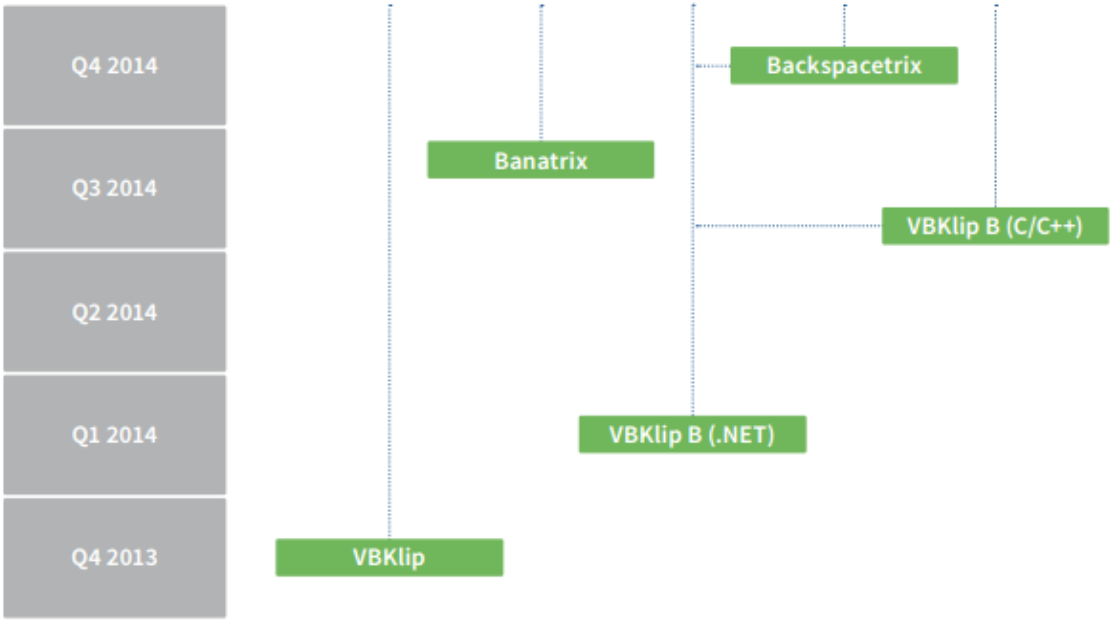
Archived: 2026-04-06 00:11:02 UTC

In March 2015, S21sec published their analysis of the new e-banking trojan horse targetting Polish users. They named it “Slave”, because such a string was part of a path to one of the shared libraries. We think (in part thanks to the kernelmode.info thread) that Slave was made by the same group of authors that are responsible for previously described Banatrix and a ransomware/Android malware campaign. This means that those authors are most certainly fluent in Polish.

History of Polish banking trojan malware

The first Polish malware that we discovered was VBKlip. Its purpose was to replace a bank account number that was copied to Windows clipboard. Then, because this method was widely publicized in Poland, another author started to make knock-offs. This malware, written in a few lines of .NET or C++ code, was even simpler. All of those simpler versions were made by the same person, known from earlier phishing attempts.

Next, Banatrix came on the scene. It was a really advanced trojan horse, which was able to execute any code on the infected machine, but was mainly used to steal password data from the Firefox web browser and replace the bank account number, when user tried to paste it on the e-banking website. The Banatrix infrastructure used Tor network and Bitcoins to make the botnet owners more anonymous.



The most recent Polish malware is Slave – e-banking trojan horse discovered by S21sec. We have multiple reasons to believe that the same group is responsible for creating Slave and Banatrix. Slave is based on webinjects – HTML or JavaScript snippets added to the website, when a user tries to display it in the browser. This code is responsible for e.g. extracting login information or performing a social engineering attack.

Technical details

Slave is dropped by another malware called “Andromeda”. This malware is only used as a mechanism for dropping the actual payload. Andromeda is sent using e-mail messages that suggest that the attachment is an outstanding invoice. Andromeda and Slave are two very different strains of malware and do not communicate with each other. The attacker however created a system in which only a machine infected with Andromeda first may download Slave malware. This most probably is a countermeasure to make the analysis more difficult – you cannot just download Slave using URL extracted from Andromeda.

Slave for the most part is no different than other trojan horses based on webinjects. However, there are some features that make it stand out. First, it only targets Polish banks and runs only after a specified date – 1st of April, 2015. Slave injects its code to Internet Explorer, Firefox and Chrome. However, Opera is currently unsupported. Content Security Policy headers are also stripped from server responses, so that the violation report will not be sent back to the bank.

Another interesting feature is the Bitcoin address replacement. Whenever there is a Bitcoin address in the clipboard, it is replaced with another one, hardcoded in the sample. Below is the code that does the switch.

The replaced address, 1NoKsR7jcTTufgrvh6zyvyJmL2z73aQXQP does not hold any assets at the moment.

Malware configuration is downloaded from a URI

/info.php?key=[value]

, where

value

is a part of a Bitcoin address, used for an unknown purpose. This configuration specified URLs to which specific external JavaScript code should be added. These scripts are used to exfiltrate login info and perform different kinds of social engineering attacks.

We also have information that the recently described Android/Windows malware campaign is also authored by the same group. This only shows that the attackers are very versatile and use several different methods to steal money from users.

Summary

It appears Polish malware authors are constantly working and upgrading their malware. Different groups present different technical abilities and different modi operandi. There is only a couple of different malware authors, and we are far away from having a cybercrime “malware writing” business in our country, but even so, we should take all of these kinds of threats seriously.

Sample hashes and VirusTotal scores

b92710a9a65e62accb5e6772704b20606d7f00a4f5e8d44758e0868a9cdd43af	22 / 56
ffc119b8eaff94b62810b82ab456e1e3f71b86d72e57cb45781878f5199fccbc	20 / 56
35c4b500b4c94f3dae0ce3604759787384ef7de9708add2c8de86dcf7e4b0322	38 / 55
ca7947dea43c200ce0c521b54baf60b973990af421b4cbafaba7eaddadb496f3	23 / 56
751866cb3f85e9c991187ff415010faba84903072cef2bf29bb24596fd1e6eca	35 / 55

P.S. Attribution is hard

Code attribution is a really hard task. Most of the authors – contradictory to what TV series and movies lead us to believe – do not “sign” their code in any way. However, some of the samples may contain some telltale signs – whether it is a specific object name or path to a local file. Based on this, researchers try to connect two different malware families and imply that they were made by the same author. However, this link is usually really limited. After all, malware authors can use this data to manipulate the researcher into thinking that they know the attacker. The most famous case of this is the string

Coded by BRIAN KREBS for personal use only. I love my job and my wife

present in some of the Citadel samples. Of course, Brian Krebs, renowned cybersecurity journalist, is not the author of Citadel code.

They are of course other sources providing a link between different malware families. One of them is information obtained from anonymous sources that sometimes disclose particular facts about the malware, which only people close to the author may know. However, this information is really hard to verify and must be used with caution. Lastly, the other popular link is the usage of the same infrastructure – whether it is the same hosting or even the same server.

All of these information are only small clues, which have to be combined in order to create a solid link between two malware strains. However, almost always we are not sure that there is in fact a connection. On the other hand, we cannot always disclose all of the information that we have. This

creates an environment that is prone to the manipulation and may be used for a PR gain. That is why all of this kind of revelations, even the ones described here, have to be taken with a grain of salt.
