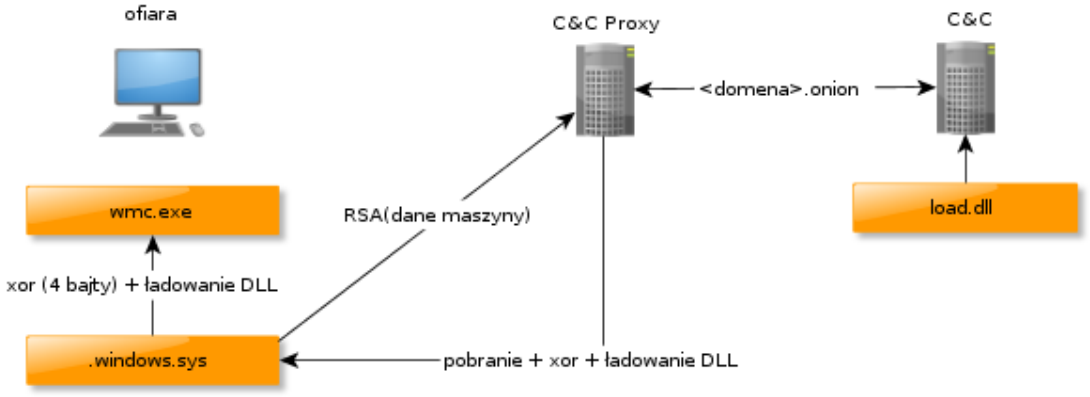
# Banatrix – an indepth look

Archived: 2026-04-05 21:15:44 UTC

Of all of the Polish malware families that we have seen last year, Banatrix seems to be the most technologically advanced one. This malware was used to replace the bank account number in the browser memory, however its implementation allowed an attacker to execute any arbitrary code on the victim's machine. This was used to extract passwords saved in the Mozilla Firefox browser. On this article we discuss the Banatrix C&C infrastructure and its use of TOR network both to hide the attacker's identity and to make the botnet takedown a challenge.

### What Banatrix does to the infected machine?

As we have described in our previous article Banatrix was used to replace the victim's bank account number in the browser memory. However, its architecture allows for a lot more. The general concept behind this malware is presented in the picture below.




### First stage: unpacking and persistence

Upon the first run malware drops two files: xor encrypted DLL and an exe file. This files are created in the

%AppData%

directory (which is

C:\Users\All Users

on Windows XP and

C:\ProgramData

on Windows Vista and newer). Encrypted DLL is saved either as

.sys

or as

.windows.sys

. Exe file (named

wms.exe

or

wmc.exe

) is added to the system as a Scheduled Task. The library file is decrypted and loaded into the process memory. It is then encrypted again, using a different, random key and saved with that key to the same file. This results in a different file every time the malware runs.

**Second stage: network communication**

The library, decrypted and loaded to the process memory, is responsible for communication with the C&C proxy. This includes downloading additional malicious code that is run on the infected machine. The first step in this communication is sending the RSA-encrypted machine configuration details, like the computer and user name, OS version or language. The new version of Banatrix uses a TOR proxy server to communicate with the real C&C. This is done using a custom proxy protocol. The malware contacts the hardcoded domain in one of the several TLDs, where the attacker set up a TOR proxy server. It then sends the

.onion

domain (along with some other data) to this proxy server and the server connects with that domain.

This real C&C then sends a xor-encrypted library, which is run on the infected machine. This library is again loaded into the process memory and the exported function called

init

is run. This, of course, allows the attacker to execute any code on the infected machine. This is also how the updates are being delivered.

The newest Banatrix version contains a DGA – algorithm responsible for creation of the domain names. However, it is somewhat different from the DGA in the other malware families. Banatrix has a list of domains in 25 different TLDs. Every one of these domains is then used to create 4 different domain names and perform DNS queries on each one. However only the fourth (last) domain will be used as a proxy C&C server – all others are simply there to confuse the researchers. Part of the decompiled DGA is presented in the screenshot below.

```
26  qmemcpy(proxy_domain, chosen_domain_name, v4);
27  v5 = domain_len;
28  proxy_domain[domain_len] = 0;
29  v6 = getDNS(proxy_domain);
30  domain_len = v5;
31  proxy_domain[v5 + 1] = v6 % 0xFF;
32  proxy_domain[0] += 2;
33  v7 = proxy_domain[v5 + 1];
34  v8 = getDNS(proxy_domain);
35  v9 = domain_len;
36  proxy_domain[domain_len + 1] = (v7 + v8) % 0xFFu;
37  ++proxy_domain[1];
38  v10 = proxy_domain[v9 + 1];
39  v11 = getDNS(proxy_domain);
40  proxy_domain[domain_len + 1] = (v10 + v11) % 0xFFu;
41  --proxy_domain[1];
42  --proxy_domain[0];
43  return getDNS(proxy_domain);
44}
```

**Third stage: code execution**

The downloaded library, as we have mentioned previously, iterates over all of the processes in the search of the browser process. It then searches the process memory for the bank account number and replaces it with the hardcoded one. However, we have also observed that some of the victims received another library – one that had a function to get the user passwords saved in the Mozilla Firefox browser and send them to the dropzone server. This proves that the malware architecture allows the flexibility to execute any arbitrary code.

## Summary

Banatrix remains a serious threat for the Polish Internet users. This claim is backed up by our sinkhole data – a little over 5,000 different IPs are trying to connect with the C&C server every day. It seems that the malware is also under a heavy development and new features are added every couple of weeks.

The SHA256 fingerprint of the analyzed sample is: 7c4d4e98601b2ae11c4a27299ded2a15e635b317ef32f48f683da016ca77c1c9. It's has a pretty high detection rate on VirusTotal, as you can see below.


---

Source: https://www.cert.pl/en/news/single/banatrix-an-indepth-look/