Polish Banks Infected with Malware Hosted on Their Own Government's Site

bleepingcomputer.com/news/security/polish-banks-infected-with-malware-hosted-on-their-own-governments-site/

Catalin Cimpanu

By
Catalin Cimpanu

- February 6, 2017
- 02:30 PM
- 0

Several Polish banks said they suffered malware infections after their employees visited the site of the Polish Financial Supervision Authority (KNF), which had been previously infected to host a malicious JavaScript file.

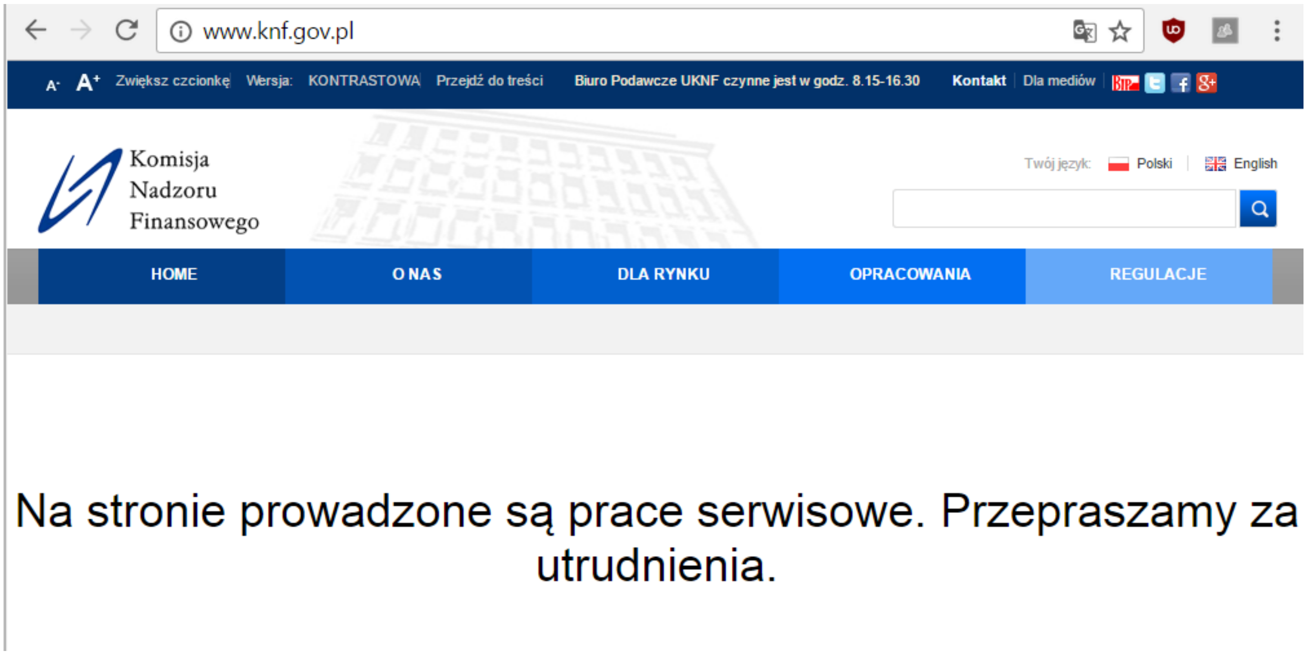
Zaufana Trzecia Strona, a local Polish news site, first reported the attacks late Friday, last week. The news site said that during the past week, the security teams at several, yet unnamed, Polish banks detected downloads of suspicious files and encrypted traffic going to uncommon IPs situated in many foreign countries.

As employees at different banks started looking into their systems, they found malware installed on numerous workstations and even some servers.

KNF website hosted malicious JavaScript file

Subsequent investigations and a cooperation between different banks eventually discovered the source of the infection as being the official website of KNF, which, ironically, is the regulating body that keeps an eye out for the security of financial systems in Poland.

According to reports, KNF's website had been compromised for well over a week, as an unidentified attacker had modified one of the site's JavaScript files.



Na stronie prowadzone są prace serwisowe. Przepraszamy za utrudnienia.

KNF website (via: Zaufana Trzecia Strona)

Visitors accessing the KNF website would load the malicious JavaScript file as part of the website's regular resources.

JavaScript file would lead to RAT infection

The JavaScript code worked by opening a hidden iframe and forcibly downloading a file on the victim's computers. Users that discovered and executed this file would install a remote access trojan (RAT) on their computers.

According to Zaufana Trzecia Strona, this malware has a zero detection rate on VirusTotal and appears to be a new malware strain, never-before-seen in live attacks.

KNF's staff have cleaned their site and along with the affected banks, have reported the incidents to CERT.pl. They also released a statement acknowledging the website hack on Friday, but haven't provided other details about the attack.

The affected Polish banks said the malware that infected their computers and servers encrypted its outgoing traffic and they weren't able to tell what the attackers stole.

No customer funds stolen

Banks reassured their clients and said they haven't detected any unauthorized transactions, but only the mysterious outgoing traffic.

Local media believes the attack is the work of a foreign intelligence agency. A more believable theory would be that this is the work of one of the many cyber-crime syndicates specialized in cyber-thefts from financial institutions.

The attacks have the signs of classic network reconnaissance operations, where hackers gather intelligence in order to create a map of a victim's network before launching their final assaults.

Related Articles:

New ChromeLoader malware surge threatens browsers worldwide

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

Popular Python and PHP libraries hijacked to steal AWS keys

Microsoft: Credit card stealers are getting much stealthier

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

- Bank
- JavaScript
- Malware
- Poland

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: