New bank attacks

Published on May 24, 2018

Finance/Banking

In mid-May 2018, the Expert Security Center (ESC) at Positive Technologies detected a phishing campaign directed at the financial sector. A number of signs suggest that the Cobalt group or its past participants continued to operate.
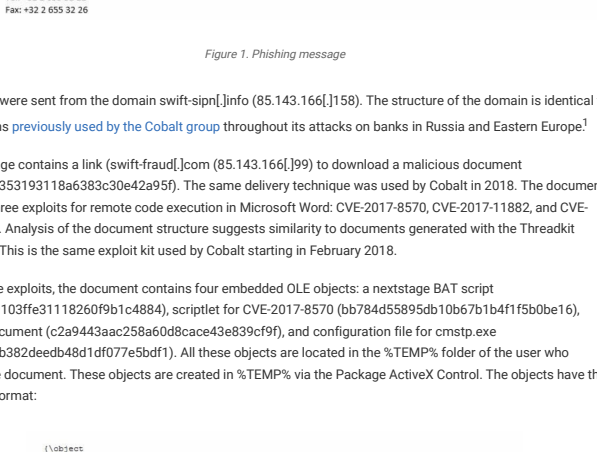

Figure 1. Phishing message

Messages were sent from the domain swift-sipni[.]info (85.143.166[.]158). The structure of the domain is identical to the domains previously used by the Cobalt group throughout its attacks on banks in Russia and Eastern Europe[1].

The message contains a link (swift-fraud[.]com (85.143.166[.]99) to download a malicious document (d117c73e35319311ba6383c30e42a95f). The same delivery technique was used by Cobalt in 2018. The document contains three exploits for remote code execution in Microsoft Word: CVE-2017-8570, CVE-2017-11882, and CVE-2018-0802. Analysis of the document structure suggests similarity to documents generated with the ThreadKit exploit kit. This is the same exploit kit used by Cobalt starting in February 2018.

Besides the exploits, the document contains four embedded OLE objects: a nextstage BAT script (4bee6ff391039fa31113826f9b1c4884), script for CVE-2017-8570 (bb784d55895db1db67b1d4f1f5b0be16), dummy document (c2a9443aac258a6b8cace3e83f9cf9f), and configuration file for cmstp.exe (581c2a76b382deedb48d1df077e9bdf1). All these objects are located in the %TEMP% folder of the user who opened the document. These objects are created in %TEMP% via the Package ActiveX Control. The objects have the following format:

Figure 2. Structure of an OLE object

After any of the exploits is triggered, the next-stage BAT script runs:

Figure 3. Next-stage BAT script

Interestingly, this script leads to launching the utility cmstp.exe, which then downloads COM-DLL-Dropper (f0e52df398b938bf82d9e71ce754ab34) from cloud.yourdocument[.]biz (31.148.219[.]17).

Use of this technique allows bypassing AppLocker, as well as downloading and running SCT or COM objects using the standard Windows utility regsvr32.exe. This method of bypassing AppLocker was discovered and described publicly this year.

cmstp.exe uses a configuration file that is also an OLE object in the original malicious document:

Figure 4. Configuration file for cmstp.exe

The main purpose of COM-DLL-Dropper is to place a JavaScript dropper on the system, which in turn downloads a JavaScript backdoor. But before performing these primary functions, COM-DLL-Dropper checks its process to see whether the name contains the ".txt" extension.

First, two random values are generated and stored in the registry key HKEY_CURRENT_USER\Software\Microsoft\Notepad\[username]:

Figure 5. Modified registry key

These values are used to name the malware modules: one of them will be the name of the JavaScript dropper created from the body of COM-DLL-Dropper, while the second value will be name of the JavaScript backdoor.

After these values are generated, persistence is ensured via a logon script:

Figure 6. Gaining persistence on the system

Then the DLL body is decrypted to generate an on-disk copy of the JavaScript dropper (%APPDATA%\.txt, C:\Users\\AppData\Roaming\.txt). The JavaScript dropper is encrypted with AES256-CBC. During the final stage, the JavaScript dropper starts and the DLL is deleted.

The scheme for delivery of the JavaScript dropper is the same as seen in summer 2017: then, too, AES256-CBC was used for decryption.

Figure 7. Delivery of the JavaScript dropper in 2017

The JavaScript dropper is obfuscated and encrypted with RC4. When the dropper runs, self-decryption is started:

Figure 8. Main function in the dropper code

The dropper itself is very similar to the 2017 version, with differences only in the names of some functions and variables. The dropper stays in a While True loop and tries to download a JavaScript backdoor from the command-and-control server nl.web-cdn[.]biz (185.162.130[.]155) and launch via regsvr32.exe. The name for the backdoor is taken from the registry.

The JavaScript backdoor, as well, is obfuscated and encrypted with RC4. It self-decrypts upon launch.

Figure 9. Configuration for the JavaScript backdoor

Like the 2017 version, the JavaScript backdoor has a number of functions:

- Reconnaissance via WMI
- Launch of programs via CMD
- Launch of new modules via regsvr32.exe
- Self-updates
- Self-removal
- Detection of antivirus software
- Encryption of traffic with RC4

A new backdoor function checks for the backdoor in %APPDATA% based on the registry key indicated above. If no registry key is present or the backdoor is not found in %APPDATA%, it will not run.

Recommendations

Cybercriminals increasingly use social engineering to penetrate infrastructures in targeted attacks. Time and again, incident investigation and security testing by Positive Technologies underline that the human factor is the weak point in security: statistics show that in 27 cases, recipients click links in phishing messages. Attackers are often able to draw employees into correspondence (and even secure staff, in 3 percent of cases). And if a message is sent from the address of a real company (a technique used by Cobalt), attackers' success rates jumps to 33 percent.

Therefore security awareness training for employees is more important than ever. Key recommendations for companies include:

- Regular awareness-building among employees
- Timely installation of security updates (both applications and operating systems)
- Use of capable protection solutions, including malware detection systems that allow employees to self-scan attachments and other files as needed
- Full investigation of all security incidents

1 In March 2018, the accused ringleader of the Cobalt group was arrested in Europe.

Download PDF

Share:

PT Application Firewall
Intelligent protection of business applications
Learn more

Related articles

April 4, 2019
Vulnerabilities in online banking applications

July 18, 2017
Security trends & vulnerabilities review: financial systems (2017)

April 23, 2019
Financial application vulnerabilities

All articles →

SOLUTIONS
Unified Application Security
Telecommunications
Vulnerability Management
Financial Services
Utilities
IDM Security

PRODUCTS
MaxPatrol
MaxPatrol SIEM
Telecom Security
PT ISIM
PT Network Attack Discovery
PT Telecom Attack Discovery

SERVICES
ICS/SCADA Security Assessment
Telecom Security Assessment
ATM Security Assessment
Web Application Security Services
Mobile Application Security Services
Custom Application Security Testing
SSDL Implementation

ANALYTICS
Threatscape
Research Blog
Distributors
Knowledge base

PARTNERS
Authorized Partners
Technology Partners

ABOUT
Clients
Press
News
Events
Insurance
Contacts
Documents and Materials

POSITIVE TECHNOLOGIES

Follow us
Terms of Use
Privacy policy
Positive Coordinated Vulnerability Disclosure
Help