Cobalt Strikes Again, Spam Runs Target Russian Banks

blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/

November 20, 2017

Spam

Backdoor-laden spam mail we saw targeting Russian-speaking businesses were apparently part of bigger campaigns. The culprit appears to be the Cobalt group. In recent campaigns, Cobalt used social engineering hooks designed to target bank employees.

By: Ronnie Giagone, Lenart Bermejo, Fyodor Yarochkin November 20, 2017 Read time: (words)

The waves of backdoor-laden spam emails we observed during June and July that targeted Russian-speaking businesses were part of bigger campaigns. The culprit appears to be the Cobalt hacking group, based on the techniques used. In their recent campaigns, Cobalt used two different infection chains, with social engineering hooks that were designed to invoke a sense of urgency in its recipients—the bank's employees.

Cobalt was named after Cobalt Strike, a multifunctional penetration testing tool similar to Metasploit. The hacking group misused Cobalt Strike, for instance, to perpetrate ATM cyber heists and target financial institutions across Europe, and interestingly, Russia. Unlike other groups that avoid Russia (or Russian-speaking countries) to elude law enforcement, Cobalt's attack patterns suggest that the group uses Russia as a testing ground where they try their latest malware and techniques on Russian banks. If successful, they go on to attack financial institutions outside the country. This resembles the tactics of another cybercriminal group, Lurk.

Of note were Cobalt’s other targets. The hacking group's first spam run also targeted a Slovenian bank, while the second run targeted financial organizations in Azerbaijan, Belarus, and Spain.

Changing Tacks

Apart from using a different vulnerability (CVE-2017-8759), what’s unique in their latest spear phishing campaigns, compared to their previous spam runs and even other related cybercriminal campaigns, is an apparent role change. The modus commonly seen in attack chains that target end users (i.e., bank customers) is now leveled against the banks themselves. While they previously posed as sales and billing departments of legitimate companies, they’re now masquerading as the customers of their targets (banks), a state arbitration court, and ironically, an anti-fraud and online security company notifying the would-be victim that his “internet resource” has been blocked.

They also diversified tacks. The first spam run on August 31 used a Rich Text Format (RTF) document laden with malicious macros. The second, which ran from September 20 to 21, used an exploit for CVE-2017-8759 (patched last September), a code injection/remote code execution vulnerability in Microsoft’s .NET Framework. The vulnerability was used to retrieve and execute Cobalt Strike from a remote server they controlled. We also saw other threat actors using the same security flaw of late, like the cyberespionage group ChessMaster.

Below are snapshots of some of the spam emails they sent to their targets:

Figure 1. Spam emails containing RTF documents embedded with malicious macros

Infection Chain via Macros

Here’s a visualization of this infection chain:

Figure 2. Infection chain of Cobalt’s latest spear phishing campaign using malicious macro

The RTF file contains macro codes that will execute a PowerShell command to retrieve a dynamic-link library (DLL) file before executing it using odbcconf.exe, a command-line utility related to Microsoft Data Access Components. The DLL will drop and execute a malicious JScript using regsvr32.exe, another command-line utility, to download another JScript and execute it using the same regsvr32.exe. This JScript will then connect to a remote server and wait for backdoor commands. During analysis, we received a PowerShell command that downloads Cobalt Strike from hxxps://5[.]135[.]237[.]216[/]RLxF. It will ultimately try to connect to their command and control (C&C) server, 5[.]135[.]237[.]216[:]443, which we found located in France.

Figure 3. The malicious RTF file asking would-be victims to “Enable Content” (left) and what happens after clicking it, when the macro codes are run (right)

To further illustrate this infection chain: after clicking “Enable Content”, it will run the macro codes that will check if the machine is 64-bit, decrypt and execute a PowerShell command, remove the picture in the document, and write “Call me” in it. The PowerShell command is for downloading a DLL file from hxxp://visa[-]fraud[-]monitoring[.]com[/]t[.]dll, saving it in the affected machine, then executing it via the command, *odbcconf.exe /S /A {REGSVR ""C:\Users\Public\file.dll""}.* The DLL file will drop a Windows Script Component (SCT) file embedded with JScript in the %AppData% folder using a random name and append it with a .TXT extension.

Figure 4. The macro codes (above) and the DLL file executing the SCT file via regsvr32.exe (below)

The SCT file will check if the system has an internet connection; if it's connected, it will proceed to download and execute a backdoor from the remote server.

Figure 5. The file downloaded from the remote server, which is actually a backdoor

Some of the backdoor’s commands are:

- d&exec — download and execute PE file
- more_eggs — download additional scripts
- gtfo — delete files/startup entries and terminate
- more_onion — run additional script
- more_power — run command shell commands

Infection Chain via CVE-2017-8759

The RTF attachment used in their second spam run contained an exploit for CVE-2017-8759. It entails downloading a specified Simple Object Access Protocol (SOAP) Web Services Description Language (WSDL) definition from a remote server, which is injected into memory. The codes include downloading and retrieving Cobalt Strike, which will connect to the C&C server 86[.]106[.]131[.]207 and wait for commands.

Figure 6. Infection chain using CVE-2017-8759

Figure 7. Spam emails whose attachments contain an exploit for CVE-2017-8759

The same exploit technique has been employed to deliver the cyberespionage malware FinSpy. In Cobalt’s case, a SOAP moniker is embedded in the RTF file, which facilitates the exploit for CVE-2017-8759 by retrieving the malicious SOAP WSDL definition via hxxp://servicecentrum[.]info[/]test[.]xml. Contents of this Extensible Markup Language (XML) file will be parsed, which will generate a Source Code (CS) file. It will then be compiled by the .NET Framework, which Microsoft Office will load as a library.

Depending on the infected machine’s architecture, the library will inject codes that will download and execute the final payload. It’s named “ZxT6” in 32-bit systems and “MZBt” in 64-bit machines. The endgame is to connect to the C&C server, 86[.]106[.]131[.]207, which we found located in Germany. The final payload is a DLL that is a component of Cobalt Strike. It will connect to 86[.]106[.]131[.]207[:]443 to wait for further commands.

This is what the attacker’s panel looks like when trying to interact with the targeted victims:

Figure 8. Dashboard of Cobalt Strike, which is also abused by various attackers

Mitigations

Many security technologies and security researchers may be utilizing newer detection mechanisms, but cybercriminals are also keeping up, adjusting their tactics to evade them. In Cobalt’s case, for instance, they’ve looked into instances of valid Windows programs or utilities as conduits that allow their malicious code to bypass whitelisting.

Indeed, Cobalt hacking group's attacks exemplify the importance of defense in depth. Here are some best practices to defend against these types of threats:

- Blacklist, disable, and secure the use of built-in interpreters or command-line applications, such as PowerShell, odbcconf.exe, and regsvr.exe
- Regularly patch and keep the system and its applications updated to prevent attackers from exploiting possible vulnerabilities; consider virtual patching for legacy/end-of-life systems
- Secure the email gateway, given how Cobalt still relies on email as entry point
- Implement network segmentation and data categorization to thwart lateral movement
- Proactively monitor the network and endpoint for anomalous activities; deploy firewalls and sandbox as well as intrusion detection and prevention systems to reduce attack surface
-
- ***Trend Micro Solutions***

Trend Micro XGen™ security provides a cross-generational blend of threat defense techniques against a full range of threats for data centers, cloud environments, networks, and endpoints. It features high-fidelity machine learning to secure the gateway and endpoint data and applications, and protects physical, virtual, and cloud workloads. With capabilities like web/URL filtering, behavioral analysis, and custom sandboxing, XGen™ protects against today’s purpose-built threats that bypass traditional controls, exploit known, unknown, or undisclosed vulnerabilities. Smart, optimized, and connected, XGen™ powers Trend Micro’s suite of security solutions: Hybrid Cloud Security, User Protection, and Network Defense.

Indicators of Compromise (IoCs):

Hashes related to the spear phishing campaign using malicious macro codes (SHA256):
Email attachments/RTF files detected as W2KM_CALLEM.ZGEI-A:

- ccb1fa5cdbc402b912b01a1838c1f13e95e9392b3ab6cc5f28277c012b0759f9
- dcad7f5135ffa5e98067b46feec2563be8c67934eb3b14ef1aad8ff7fe0892c5

Malicious DLL file detected as TROJ_DROPFCKJS.ZHEI-A

dab05e284a9cbc89d263798bae40c9633ff501e19568c2ca21ada58e90d66891

Malicious JScript file (35CE74A54720.txt) detected as JS_NAKJS.ZGEI-A:

2b4760b5bbe982a7e26af4ee618f8f2dcc67dfe0211f852bf549db457acd262c

Malicious TXT file (README.TXT) detected as JS_GETFO.ZIEI-A:

e9ab3195f3a974861aa1135862f6c24df1d7f5820e8c2ac6e61a1a5096457fc3

Backdoor (RLxF) detected as BKDR_COBALT.ZHEJ-A:

0dedb345d90dbba7e83b2d618c93d701ed9e9037aa3b7c7c58b62e53dab7d2ce

Hashes related to the spear phishing campaign exploiting CVE-2017-8759: Email attachments/RTF files detected as TROJ_MDROP.ZHEI-A:

- eb4325ef1cbfba85b35eec3204e7f79e4703bb706d5431a914b13288dcf1d598
- a0292cc74ef005b2e5e0889d1fc1711f07688b93b16ebc3174895d7752a16a23
- 94155a2940a1d49a92a602a5232f156eeb1d35018847edb9c6002cefe4c49f94
- 69e55d2e3207e29d9efc806ff36f13cd49fb92f7c12f0145f867674b559734a3

Malicious XML file (test.xml) detected as TROJ_CVE20178759.ZIEI-A:

0f5c5d07ed0508875330a0cb89ba3f88c58f92d5b1536d20190df1e00ebd3d91

Backdoor (ZxT6) detected as BKDR_COBALT.ZIEI-A:

9d9d1c246ba83a646dd9537d665344d6a611e7a279dcfe288a377840c31fe89c

Backdoor (MZBt) detected as BKDR64_COBALT.ZIEI-A:

e78e800bc259a46d51a866581dcdc7ad2d05da1fa38841a5ba534a43a8393ce9

Related malicious URLs:

- hxxp://visa-fraud-monitoring[.]com/t[.]dll

- hxxps://webmail[.]microsoft[.]org[.]kz/portal/readme[.]txt
- hxxps://webmail[.]microsoft[.]org[.]kz/portal/ajax[.]php
- hxxp://servicecentrum[.]info/test[.]xml
- hxxps://5[.]135[.]237[.]216[/]RLxF
- hxxps://86[.]106[.]131[.]207[/]ZxT6
- hxxps://86[.]106[.]131[.]207[/]MZB