Cobalt Hacking Group Tests Banks In Russia and Romania

bleepingcomputer.com/news/security/cobalt-hacking-group-tests-banks-in-russia-and-romania/

Ionut Ilascu

By
Ionut Ilascu

- August 30, 2018
- 07:31 PM
- 0

In new spear-phishing campaigns observed this month, the Cobalt hacking group targeted banks in Russia and Romania with emails containing two payloads pointing to two different command and control servers.

Cobalt is a cybercrime gang that operates since at least 2016 specialized in targeting financial organizations. According to data from Europol, the group is tied to cyberattacks against at least 100 banks across the world, stealing about one billion euros from them.

Although the alleged ringleader has been arrested in Spain this year, and three individuals believed to be members of the hacking crew have been charged at the beginning of the month, the group continues to operate.

Phishing email uses domain similar to financial organization

Arbor Networks ASERT Team on August 13 noticed a new campaign bearing the Cobalt signature. The target was NS Bank in Russia. ASERT's threat-intelligence partner Intel471 discovered another campaign aimed at Carpatica Commercial Bank/Patria Bank in Romania.

The emails delivered to the victims purported to be from other institutions related to the financial industry, a tactic intended to increase confidence in launching the weaponized files in the attachment.

The researchers with ASERT examined the domain rietumu[.]me, which is a command and control (C2) server connected to Cobalt activity, and found an email address that led them to five new domains created on August 1, one of them being inter-kassa[.]com.

The other domains the experts uncovered, and clearly trying to impersonate financial institutions are:

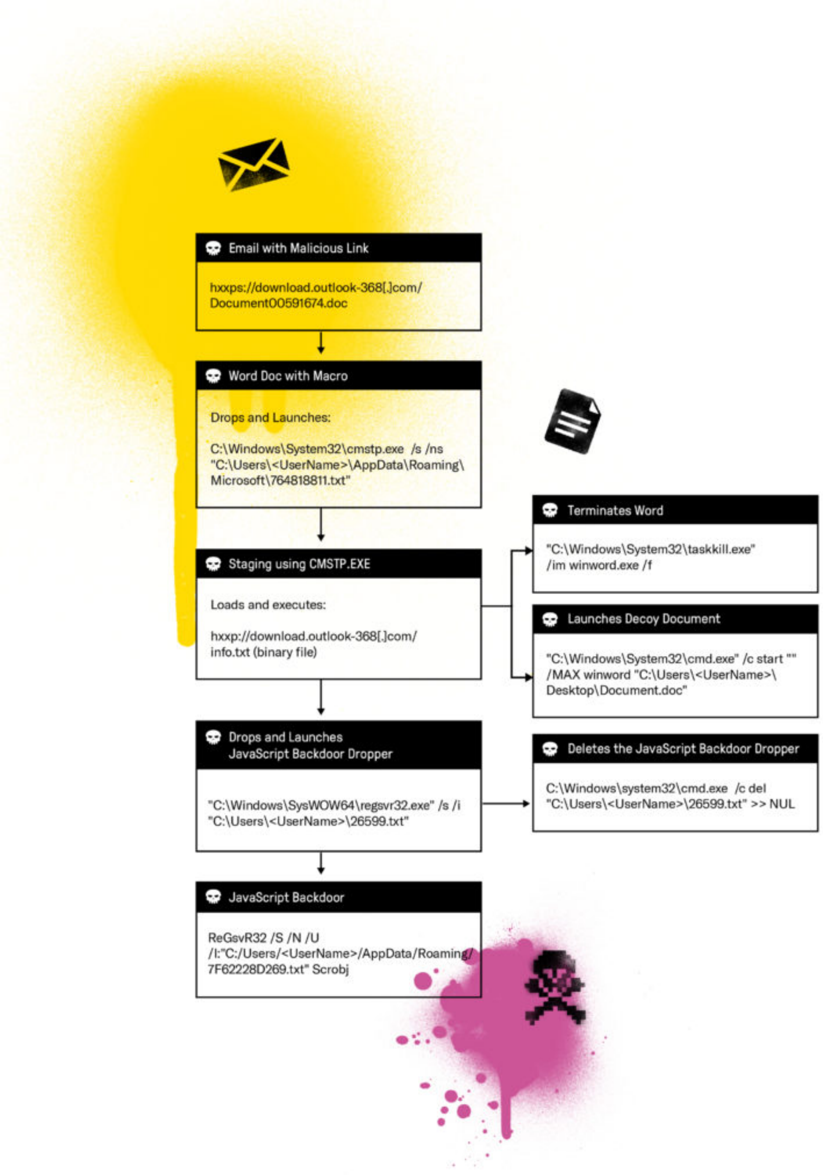
- compass[.]plus - probably posing as BBVA Compass Bancshares or Compass Savings Bank
- eucentalbank[.]com - probably posing as the European Central Bank
- europecentalbank[.]com - probably posing as the European Central Bank
- unibank[.]credit - probably posing as any Unibank financial entities across the globe

Interkassa is a legitimate payment processing system based in Georgia (the country) offering over 50 payment instruments for online transactions in multiple currencies.

Looking for samples associated with this domain, ASERT found a phishing email for an NS Bank employee. Contrary to the "norm," it included two links to malicious files: one to a Word document with obfuscated VBA scripts, and one for downloading a binary with the extension changed to JPG.

Email delivers links to two weaponized files

The weaponized Office file needs to have permission to run macros in order to be able to execute the VBA script. But if macros are enabled, a convoluted operation is triggered, ending with downloading and running a JavaScript backdoor very similar in functionality with another tool linked to the Cobalt group.



Email with Malicious Link

```
hxxps://download.outlook-368[.]com/
Document00591674.doc
```

Word Doc with Macro

Drops and Launches:

```
C:\Windows\System32\cmstp.exe  /s /ns
"C:\Users\<UserName>\AppData\Roaming\
Microsoft\764818811.txt"
```

Staging using CMSTP.EXE

Loads and executes:

```
hxxp://download.outlook-368[.]com/
info.txt (binary file)
```

Terminates Word

```
"C:\Windows\System32\taskkill.exe"
/im winword.exe /f
```

Launches Decoy Document

```
"C:\Windows\System32\cmd.exe" /c start ""
/MAX winword "C:\Users\<UserName>\
Desktop\Document.doc"
```

Drops and Launches
JavaScript Backdoor Dropper

```
"C:\Windows\SysWOW64\regsvr32.exe" /s /i
"C:\Users\<UserName>\26599.txt"
```

Deletes the JavaScript Backdoor Dropper

```
C:\Windows\system32\cmd.exe  /c del
"C:\Users\<UserName>\26599.txt" >> NUL
```

JavaScript Backdoor

```
ReGsvR32 /S /N /U
/I:"C:/Users/<UserName>/AppData/Roaming/
7F62228D269.txt" Scrobj
```

The executable file posing as JPEG image in the email to NS Bank came from hxxp://sepa-europa[.]eu, a domain pretending to be related to the Single Euro Payments Area (SEPA), an initiative for easier cross-border payments within the European Union space.

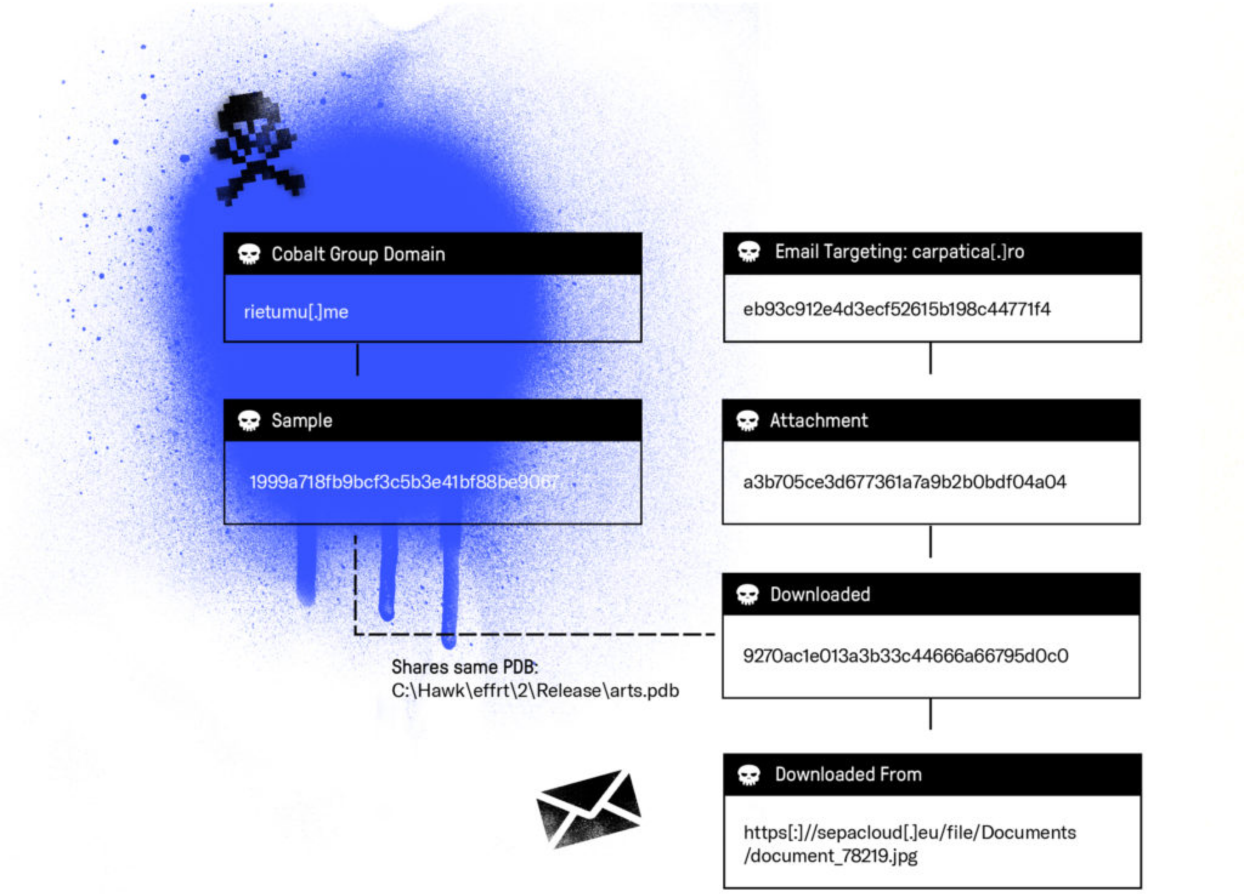
"UPX unpacked, is an executable rather than an image file. The sample is littered with junk code that spends CPU cycles before proceeding to de-obfuscate itself. The unpacking routine involves overwriting itself in memory with another executable," ASERT explains.

Following the analysis of this binary, the researchers determined it was a variant of CobInt/COOLPANTS - a reconnaissance backdoor found on a C2 operated by Cobalt hackers in the past.

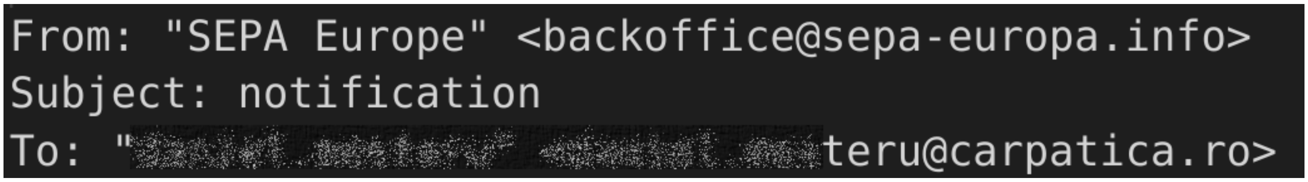
"Making use of separate infection points in one email with two separate C2s makes this email peculiar. One could speculate that this would increase the infection odds," ASERT concludes.

Spear phishing employee at Romanian bank

The spear-phishing campaign against Carpatica Commercial Bank, now merged with Patria Bank, delivered malware that shared the same program database with a sample from the domain rietumul[.]me, tied to the Cobalt group.


Cobalt Group Domain
rietumu[.]me
Sample
1999a718fb9bcf3c5b3e41bf88be9067
Email Targeting: carpatica[.]ro
eb93c912e4d3ecf52615b198c44771f4
Attachment
a3b705ce3d677361a7a9b2b0bdf04a04
Downloaded
9270ac1e013a3b33c44666a66795d0c0
Shares same PDB:
C:\Hawk\effrt\2\Release\arts.pdb
Downloaded From
https[:]//sepacloud[.]eu/file/Documents
/document_78219.jpg

The header of the phishing email shows that the attacker used SEPA once more as a cover for the malicious activity, using SEPA Europe as the sender of the message.



```
From: "SEPA Europe" <backoffice@sepa-europa.info>
Subject: notification
To: "[redacted]teru@carpatica.ro>
```

It is unclear when Intel471 caught the phishing email, but two weeks ago the Romanian Intelligence Service (SRI) announced that it had solid information about cyberattacks aimed at financial institutions in Romania.

According to the communication, the events occurred between June and August, a timeframe that overlaps with the campaigns discovered by the researchers at the two companies.

SRI says that analysis from its cyberintelligence unit, National Cyberint Center (CNC), shows that the arsenal of attack tools used by the hackers includes Cobalt Strike, a piece of software for penetration testing. This is confirmed by the numerous reports from various security companies that examined the group's activity.

Phishing is how it starts

Spear-phishing is an initial stage of the attack, where the group tries to gain a foothold access in the bank's digital infrastructure. Subsequent activity from the Cobalt group typically consists in reconnaissance and moving laterally inside the network.

After they learn how the target operates and get the same access as high-level employees, the hackers could execute money transfers, command ATMs, and steal money from payment gateways and SWIFT systems.

Cobalt

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: