

Cobalt Hacking Group Tests Banks In Russia and Romania

By Ionut Ilascu

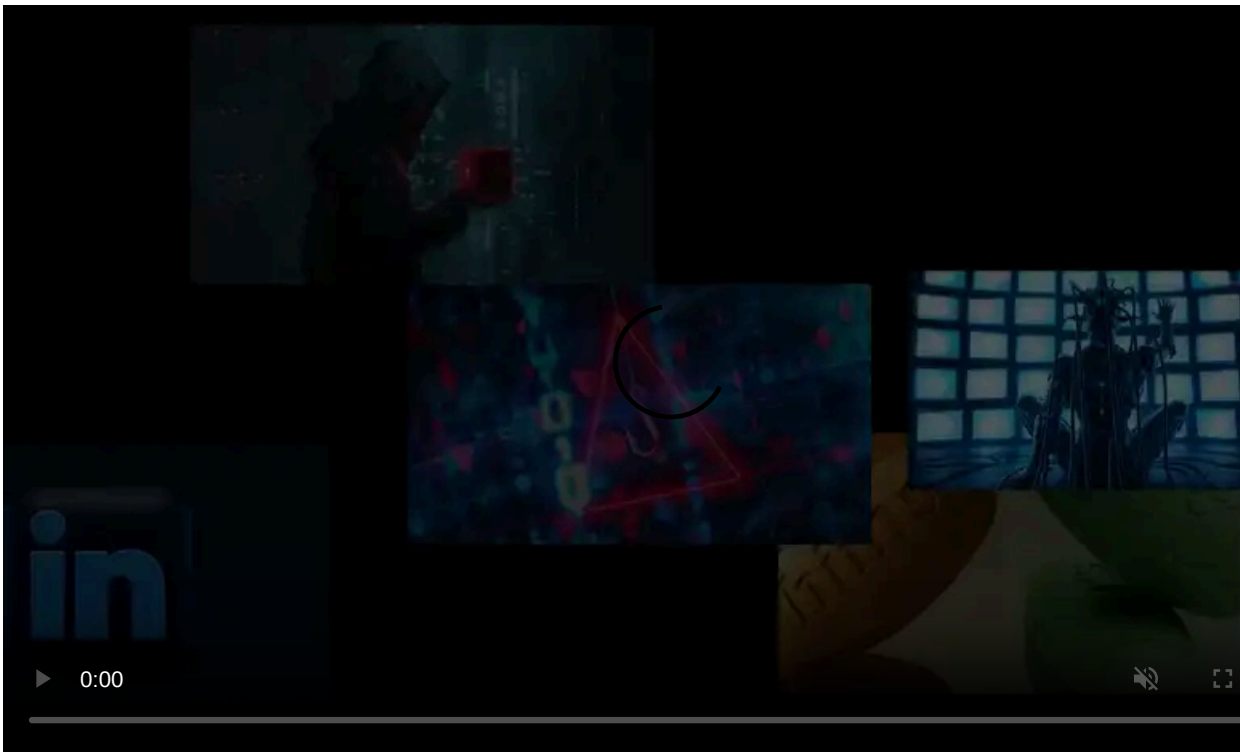
Published: 2018-08-30 · Archived: 2026-04-05 16:27:13 UTC



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.



Visit Advertiser website [GO TO PAGE](#)

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 interkassa[.]com.

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

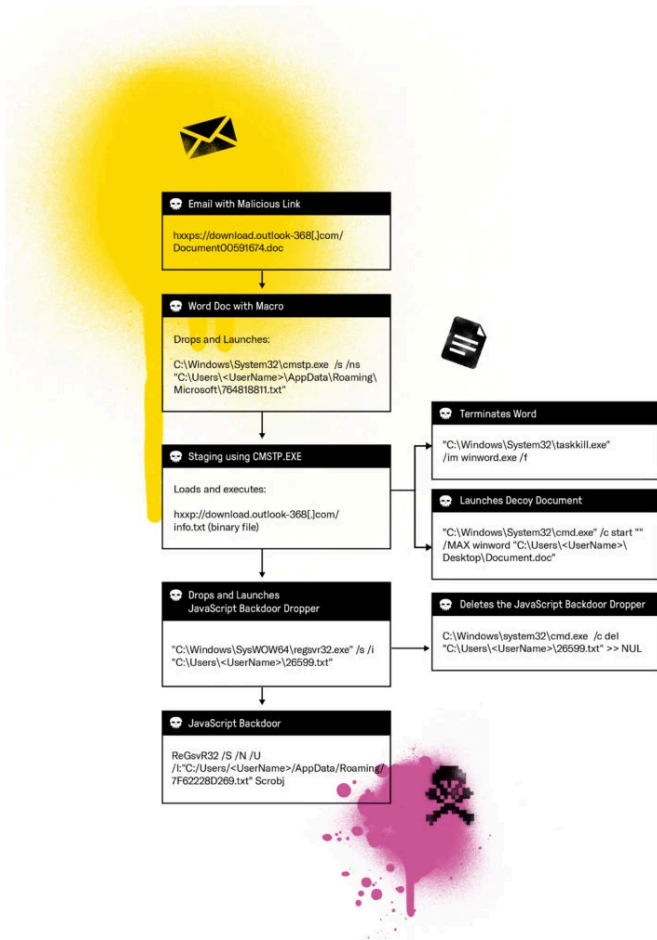
- compass[.]plus - probably posing as [BBVA Compass Bancshares](#) or [Compass Savings Bank](#)
- eucentalbank[.]com - probably posing as the [European Central Bank](#)
- europecentralbank[.]com - probably posing as the European Central Bank
- unibank[.]credit - probably posing as any [Unibank](#) financial 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.



The executable file posing as JPEG image in the email to NS Bank came from `hxxp://sepa-europa[.]Jeu`, 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.

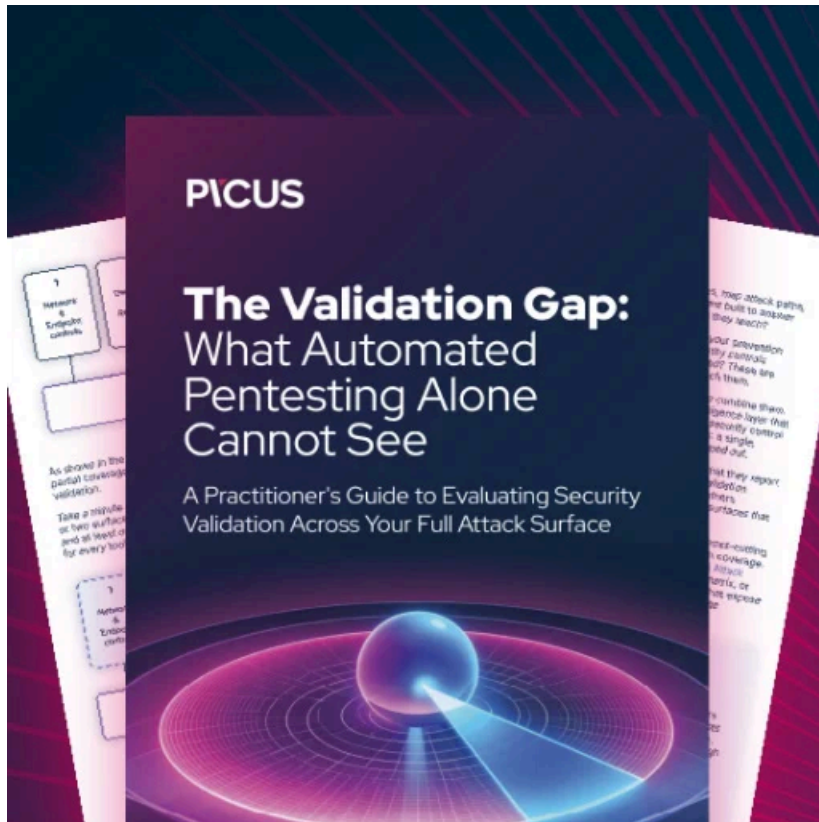
"UPX unpacked, is an executable rather than an image file. The sample is littered with junk code that spends CPU cycles before proceeding to de-obfuscate itself. The unpacking routine involves overwriting itself in memory with another executable," ASERT [explains](#).

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.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/cobalt-hacking-group-tests-banks-in-russia-and-romania/>