Cobalt Group - Threat Group Cards: A Threat Actor Encyclopedia

NamesCobalt Group *(Group-IB)*
Cobalt Gang *(Palo Alto)*
Cobalt Spider *(CrowdStrike)*
Gold Kingswood *(SecureWorks)*
ATK 67 *(Thales)*
TAG-CR3 *(Recorded Future)*
Mule Libra *(Palo Alto)*

G0080 *(MITRE)* Country Russia MotivationFinancial crime First seen2016 DescriptionCobalt Group is a financially motivated threat group that has primarily targeted financial institutions. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. Cobalt Group has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. The group has been known to target organizations in order to use their access to then compromise additional victims. Reporting indicates there may be links between Cobalt Group and both the malware Carbanak and the group Carbanak, Anunak. ObservedSectors: Financial, High-Tech, Media, Retail.
Countries: Argentina, Armenia, Austria, Azerbaijan, Belarus, Bulgaria, Canada, China, Czech, Estonia, Georgia, Italy, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Malaysia, Moldova, Netherlands, Poland, Romania, Russia, Spain, Taiwan, Tajikistan, Thailand, Turkey, UK, Ukraine, USA, Vietnam. Tools usedATMSpitter, ATMRipper, AtNow, Cobalt Strike, CobInt, Cyst Downloader, FlawedAmmyy, Formbook, Little Pig, Mimikatz, Metasploit Stager, More_eggs, NSIS, Pony, SDelete, SoftPerfect Network Scanner, Taurus Loader, ThreatKit, VenomKit. Operations performedJun 2016In June 2016, the first attack conducted by the Cobalt group was tracked at a large Russian bank, where hackers attempted to steal money from ATMs. The attackers infiltrated the bank’s network, gained control over it, compromised the domain administrator’s account, and reached the ATM control server. <https://www.group-ib.com/blog/cobalt> Jul 2016ATM heist at the First Commercial Bank in Taiwan <https://www.reuters.com/article/us-taiwan-cyber-atms/taiwan-atm-heist-linked-to-european-hacking-spree-security-firm-idUSKBN14P0CX> Aug 2016ATM heist at the Government Saving Bank in Thailand
ThaiCERT's whitepaper:
<https://www.dropbox.com/s/1xvhee0s7o12i61/Whitepaper ATM Heist GSB August 2016.pdf?dl=0> May 2017In May, Proofpoint observed multiple campaigns using a new version of Microsoft Word Intruder (MWI). MWI is a tool sold on underground markets for creating exploit-laden documents, generally used in targeted attacks. We previously reported about MWI when it added support for CVE-2016-4117. After the latest update, MWI is now using CVE-2017-0199 to launch an HTML Application (HTA) used for both information collection and payload execution.
This activity targets organizations in the financial vertical including banks, banking software vendors, and ATM software and hardware vendors. The emails are sent to technology and security personnel working in departments including Fraud and Information Security.
<https://www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-integrates-cve-2017-0199-utilized-cobalt-group-target> Aug 2017The 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. <https://blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/> Nov 2017On Tuesday, November 21, a massive spear-phishing campaign began targeting individual employees at various financial institutions, mostly in Russia and Turkey. Purporting to provide info on changes to 'SWIFT' terms, the email contained a single attachment with no text in the body. It was an attempt by the Cobalt Group to gain a foothold in the networks of the targeted individuals' organizations <https://www.riskiq.com/blog/labs/cobalt-strike/> Jan 2018Spear-phishing attacks to Russian banks
The emails were sent in the name of a large European bank in an attempt to social engineer the receiver into trusting the email. The emails were quite plain with only a single question in the body and an attachment with the name once.rtf. In other cases, we saw a file with the name Заявление.rtf attached to an email that was also written in Russian.
<https://www.riskiq.com/blog/labs/cobalt-group-spear-phishing-russian-banks/> May 2018On May 23, 1:21 p.m (Moscow time) Group-IB tracked a new large-scale Cobalt cyberattack on the leading banks of Russia and the CIS. It was like a challenge: phishing emails were sent acting as a major anti-virus vendor. Bank employees received a "complaint", in English, that their computers allegedly violated legislation.
<https://www.group-ib.com/blog/renaissance> Sep 2018In 2018, CTU researchers observed several GOLD KINGSWOOD campaigns involving SpicyOmelette, a tool used by the group during initial exploitation of an organization. This sophisticated JavaScript remote access tool is generally delivered via phishing, and it uses multiple defense evasion techniques to hinder prevention and detection activities.
<https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish> Oct 2018One of the latest examples related to the campaign under analysis was used in attacks just a few days ago. It shows the simplicity of the attack delivery employed by this group.
The attack reinforces the fact that email is still one of the primary attack vectors we continuously observe. This attack begins by targeting employees at several banking entities across the globe using an email with subject "Confirmations on October 16, 2018".
<https://unit42.paloaltonetworks.com/unit42-new-techniques-uncover-attribute-cobalt-gang-commodity-builders-infrastructure-revealed/> Oct 2019Magecart Group 4: A link with Cobalt Group?
<https://blog.malwarebytes.com/threat-analysis/2019/10/magecart-group-4-a-link-with-cobalt-group/> Counter operationsMar 2018Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain
<https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain> Aug 2018Three Carbanak cyber heist gang members arrested
<https://www.computerweekly.com/news/252446153/Three-Carbanak-cyber-heist-gang-members-arrested> Information<https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-2017-eng.pdf> <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-september-cobalt-spider/> MITRE ATT&CK<https://attack.mitre.org/groups/G0080/> Playbook<https://pan-unit42.github.io/playbook_viewer/?pb=mulelibra>
