GROUPS

Overview
admin@338
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
APT41
Axiom
BlackOasis
BRONZE BUTLER
Carbanak
Charming Kitten
Cleaver
Cobalt Group
CopyKittens
Dark Caracal
Darkhotel
DarkHydrus
Deep Panda
Dragonfly
Dragonfly 2.0
DragonOK
Dust Storm
Elderwood
Equation
FIN10
FIN4
FIN5
FIN6
FIN7
FIN8
Gallmaker
Gamaredon Group
GCMAN
Gorgon Group
Group5
Honeybee
Ke3chang
Kimsuky
Lazarus Group
Leafminer
Leviathan
Lotus Blossom
Machete
Magic Hound
menuPass
Moafee
Molerats
MuddyWater
Naikon
NEODYMIUM
Night Dragon
OilRig
Orangeworm
Patchwork
PittyTiger
PLATINUM
Poseidon Group

Home > Groups > Cobalt Group

Cobalt Group

Cobalt 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. One of the alleged leaders was arrested in Spain in early 2018, but the group still appears to be active. The group has been known to target organizations in order to use their access to then compromise additional victims. [1] [2] [3] [4] [5] [6] [7] Reporting indicates there may be links between Cobalt Group and both the malware Carbanak and the group Carbanak. [8]

ID: G0080

Associated Groups: Cobalt Gang, Cobalt Spider

Version: 1.1

Created: 17 October 2018

Last Modified: 26 July 2019

Associated Group Descriptions

Name	Description
Cobalt Gang	[1] [12][9]
Cobalt Spider	[12]

Techniques Used

ATT&CK® Navigator Layers

Domain	ID	Name	Use
Enterprise	T1088	Bypass User Account Control	Cobalt Group has bypassed UAC.[4]
Enterprise	T1191	CMSTP	Cobalt Group has used the command `cmstp.exe /s /ns C:\Users\ADMINI~W\AppData\Local\Temp\XKNqbpzl.txt` to bypass AppLocker and launch a malicious script.[1][9][10]
Enterprise	T1059	Command-Line Interface	Cobalt Group has used a JavaScript backdoor that is capable of launching cmd.exe to execute shell commands.[9]
Enterprise	T1173	Dynamic Data Exchange	Cobalt Group has sent malicious Word OLE compound documents to victims.[1]
Enterprise	T1203	Exploitation for Client Execution	Cobalt Group had exploited multiple vulnerabilities for execution, including Microsoft's Equation Editor (CVE-2017-11882), an Internet Explorer vulnerability (CVE-2018-8174), CVE-2017-8570, CVE-2017-0199, and CVE-2017-8759.[1][2][3][5][6][7][12][11]
Enterprise	T1068	Exploitation for Privilege Escalation	Cobalt Group has used exploits to increase their levels of rights and privileges.[4]
Enterprise	T1107	File Deletion	Cobalt Group deleted the DLL dropper from the victim's machine to cover their tracks.[1]
Enterprise	T1037	Logon Scripts	Cobalt Group has added persistence by registering the file name for the next stage malware under UserInitMprLogonScript.[9]
Enterprise	T1046	Network Service Scanning	Cobalt Group leveraged an open-source tool called SoftPerfect Network Scanner to perform network scanning.[2][3][4]
Enterprise	T1050	New Service	Cobalt Group has created new services to establish persistence.[4]
Enterprise	T1027	Obfuscated Files or Information	Cobalt Group obfuscated several scriptlets and code used on the victim's machine, including through use of XOR and RC4.[1][9]
Enterprise	T1086	PowerShell	Cobalt Group has used powershell.exe to download and execute scripts.[1][2][3][4][7][11]
Enterprise	T1055	Process Injection	Cobalt Group has injected code into trusted processes.[4]
Enterprise	T1108	Redundant Access	Cobalt Group has used TeamViewer to preserve remote access in case control using the Cobalt Strike module was lost.[4]
Enterprise	T1060	Registry Run Keys / Startup Folder	Cobalt Group has used Registry Run keys for persistence. The group has also set a Startup path to launch the PowerShell shell command and download Cobalt Strike.[4]
Enterprise	T1117	Regsvr32	Cobalt Group has used regsvr32.exe to execute scripts.[1][9][11]
Enterprise	T1219	Remote Access Tools	Cobalt Group used the Ammyy Admin tool as well as TeamViewer for remote access.[2][3][4]
Enterprise	T1076	Remote Desktop Protocol	Cobalt Group has used Remote Desktop Protocol to conduct lateral movement.[4]
Enterprise	T1105	Remote File Copy	Cobalt Group has used public sites such as github.com and sendspace.com to upload files and then download them to victim computers. The group's JavaScript backdoor is also capable of downloading files.[2][3][9]
Enterprise	T1053	Scheduled Task	Cobalt Group has created Windows tasks to establish persistence.[4]
Enterprise	T1064	Scripting	Cobalt Group has sent Word OLE compound documents with malicious obfuscated VBA macros that will run upon user execution and executed JavaScript scriptlets on the victim's machine. The group has also used an exploit toolkit known as Threadkit that launches .bat files.[1][2][4][9][10][11]
Enterprise	T1063	Security Software Discovery	Cobalt Group used a JavaScript backdoor that is capable of collecting a list of the security solutions installed on the victim's machine.[9]
Enterprise	T1218	Signed Binary Proxy Execution	Cobalt Group has used `odbcconf` to proxy the execution of malicious DLL files.[11]
Enterprise	T1193	Spearphishing Attachment	Cobalt Group has sent spearphishing emails with various attachment types to corporate and personal email accounts of victim organizations. Attachment types have included .rtf, .doc, .xls, archives containing LNK files, and password protected archives containing .exe and .scr executables.[1][2][3][4][5][6][10][11]
Enterprise	T1192	Spearphishing Link	Cobalt Group has sent emails with URLs pointing to malicious documents.[1]
Enterprise	T1071	Standard Application Layer Protocol	Cobalt Group has used HTTPS and DNS tunneling for C2. The group has also used the Plink utility to create SSH tunnels.[1][3][4]
Enterprise	T1032	Standard Cryptographic Protocol	Cobalt Group has used the Plink utility to create SSH tunnels.[4]
Enterprise	T1204	User Execution	Cobalt Group has sent emails containing malicious attachments or links that require users to execute a file or macro to infect the victim machine.[1][10]
Enterprise	T1220	XSL Script Processing	Cobalt Group used msxsl.exe to bypass AppLocker and to invoke Jscript code from an XSL file.[1]

PROMETHIUM
Putter Panda
Rancor
RTM
Sandworm Team
Scarlet Mimic
Silence
SilverTerrier
Soft Cell
Sowbug
Stealth Falcon
Stolen Pencil
Strider
Suckfly
TA459
TA505
Taidoor
TEMP.Veles
The White Company
Threat Group-1314
Threat Group-3390
Thrip
Tropic Trooper
Turla
Winnti Group
WIRTE

Domain	ID	Name	Use

Software

ID	Name	References	Techniques
S0154	Cobalt Strike	[1] [2] [4] [5] [6] [7] [12] [11]	Access Token Manipulation, BITS Jobs, Bypass User Account Control, Command-Line Interface, Commonly Used Port, Component Object Model and Distributed COM, Connection Proxy, Credential Dumping, Custom Command and Control Protocol, Data from Local System, Execution through API, Exploitation for Privilege Escalation, Indicator Removal from Tools, Input Capture, Man in the Browser, Multiband Communication, Network Service Scanning, Network Share Discovery, New Service, Parent PID Spoofing, Pass the Hash, PowerShell, Process Discovery, Process Hollowing, Process Injection, Remote Desktop Protocol, Remote Services, Remote System Discovery, Scheduled Transfer, Screen Capture, Scripting, Service Execution, Standard Application Layer Protocol, Timestomp, Valid Accounts, Windows Admin Shares, Windows Management Instrumentation, Windows Remote Management
S0002	Mimikatz	[2] [3] [4]	Account Manipulation, Credential Dumping, Credentials in Files, DCShadow, Pass the Hash, Pass the Ticket, Private Keys, Security Support Provider, SID-History Injection
S0284	More_eggs	[1]	Code Signing, Command-Line Interface, Data Encoding, Data Encrypted, Deobfuscate/Decode Files or Information, File Deletion, Regsvr32, Remote File Copy, Security Software Discovery, Standard Application Layer Protocol, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery
S0029	PsExec	[2] [4]	Service Execution, Windows Admin Shares
S0195	SDelete	[3]	Code Signing, Data Destruction, File Deletion

References

1. Svajcer, V. (2018, July 31). Multiple Cobalt Personality Disorder. Retrieved September 5, 2018.
2. Positive Technologies. (2017, August 16). Cobalt Strikes Back: An Evolving Multinational Threat to Finance. Retrieved September 5, 2018.
3. Positive Technologies. (2016, December 16). Cobalt Snatch. Retrieved October 9, 2018.
4. Matveeva, V. (2017, August 15). Secrets of Cobalt. Retrieved October 10, 2018.
5. Mesa, M, et al. (2017, June 1). Microsoft Word Intruder Integrates CVE-2017-0199, Utilized by Cobalt Group to Target Financial Institutions. Retrieved October 10, 2018.
6. Klijnsma, Y.. (2017, November 28). Gaffe Reveals Full List of Targets in Spear Phishing Attack Using Cobalt Strike Against Financial Institutions. Retrieved October 10, 2018.
7. Klijnsma, Y.. (2018, January 16). First Activities of Cobalt Group in 2018: Spear Phishing Russian Banks. Retrieved October 10, 2018.
8. Europol. (2018, March 26). Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain. Retrieved October 10, 2018.
9. Gorelik, M. (2018, October 08). Cobalt Group 2.0. Retrieved November 5, 2018.
10. Unit 42. (2018, October 25). New Techniques to Uncover and Attribute Financial actors Commodity Builders and Infrastructure Revealed. Retrieved December 11, 2018.
11. Giagone, R., Bermejo, L., and Yarochkin, F. (2017, November 20). Cobalt Strikes Again: Spam Runs Use Macros and CVE-2017-8759 Exploit Against Russian Banks. Retrieved March 7, 2019.
12. CrowdStrike. (2018, February 26). CrowdStrike 2018 Global Threat Report. Retrieved October 10, 2018.