COBALT GROUP

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON COBALT GROUP: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

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.

II. TARGETS

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

III. METHODS USED

Initial penetration : Spear phishing, attacks-as-a-service, exploiting system vulnerabilities.
Remoteaccess : Attackers use remote access tools to gain total control over the network.
Gaining privileges : Attackers use an open source tool Mimikatz to collect passwords for administrators of a specific server.
Data collection : Attackers look for computers with access to critical systems(core banking systems, SWIFT, card processing systems, ATM control systems, etc.)
Completion of the attack : With administrator privileges attackers can monitor activity of bank operators and perform the same actions.
Complicating investigation : Attackers remove malicious files they used and disable the bank's internal servers involved in the attack.

IV. CAMPAIGNS

- **Jun 2016** : In 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.
- **Jul 2016** : ATM heist at the First Commercial Bank in Taiwan
- **Aug 2016 :** ATM heist at the Government Saving Bank in Thailand
- **May 2017** : In 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
- **Aug 2017** : 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
- **Jan 2018** : Spear-phishing attacks to Russian banks
- **May 2018** : On 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.
- **Sep 2018** : In 2018, CTU researchers observed several GOLD KINGSWOOD campaigns involving SpicyOmelette, a tool used by the group during initial exploitation of an organization.
- **Oct 2018** : One 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.

AX1AL

V. IOCS

MD5 Hashes

7f0f3689b728d12a00ca258c688bf034
a26722fc7e5882b5a273239cddfe755f
ec33cc6cb625197587410840bce5983b
e43d92575f7df52f2dff863834a8328f
d893d8347ecad1a3d85064d2f5bded4f
bd27941ca6480e0656cfc88b25f9ae83
b4ba62e9136e5898802c8ea1efb7b49f

C2's

185[.]61[.]149[.]186
https://api[.]outlook[.]kz
http://api[.]fujitsu[.]org[.]kz
http://api[.]asus[.]org[.]kz
http://api[.]toshiba[.]org[.]http://api[.]miria[.]kz
http(s)://outlook[.]live[.]org[.]kz

TTP's

Cobalt Group has used HTTPS for C2.
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
Cobalt Group has added persistence by registering the file name for the next stage malware under HKCU\Environment\UserInitMprLogonScript
Cobalt Group has used powershell.exe to download and execute scripts.
Cobalt Group has created new services to establish persistence.
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.
Cobalt Group deleted the DLL dropper from the victim's machine to cover their tracks.
Cobalt Group leveraged an open-source tool called SoftPerfect Network Scanner to perform network scanning.
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

VI. REFRENCES / SOURCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Cobalt%20Group
https://www.group-ib.com/blog/cobalt
https://attack.mitre.org/groups/G0080/
https://www.group-ib.com/blog/cobalt
https://blog.talosintelligence.com/2018/07/multiple-cobalt-personality-disorder.html
https://otx.alienvault.com/pulse/5bbbe9e75db9653c97427893/related