cybereason®

Operation Cobalt Kitty

Threat Actor Profile & Indicators of Compromise

By: Assaf Dahan

Attribution

In this APT, the threat actor was very aware of the risks of exposure and tried to combat attribution as much as possible. This is often the case in this type of large-scale cyber espionage operations. At the time of the attack, there weren't many classic indicators of compromise (IOCs) that could lead to attribution. However, at the same time, the threat actors behind Operation Cobalt Kitty left enough "behavioral fingerprints" to suspect the involvement of the **OceanLotus Group (which also goes by the names APT-C-00, SeaLotus and APT32)**, which was first documented by Qihoo 360's SkyEye Labs in 2015 and further researched by other security companies, including FireEye's report. Reports of the group's activity in Asia date back to 2012, attacking Chinese entities. Over the years, the group was observed attacking a wide spectrum of targets in other Asian countries (Philippines and Vietnam). Cybereason concludes that the tactics, techniques and procedures (TTPs) observed throughout operation Cobalt Kitty are consistent with the group's previous APT campaigns in Asia.

The Lotus Group appears to have a tendency of using similar and even identical names for their payloads (seen in their PowerShell payloads, Denis backdoor and fake Flash installers). In addition, they also used similar anonymization services for their domains repeatedly. That type of "small" details also played a role in attributing Operation Cobalt Kitty to the OceanLotus Group.

Lastly, during the investigation, Cybereason noticed that some of the C&C domains and IPs started to emerge on VirusTotal and other threat intelligence engines, with payloads that were not observed during Cobalt Kitty. This was a cutting proof that Cobalt Kitty was not an isolated APT, but part of something bigger. Example of the C&C domains and IPs used by the group across different APT campaigns and caught in the wild:

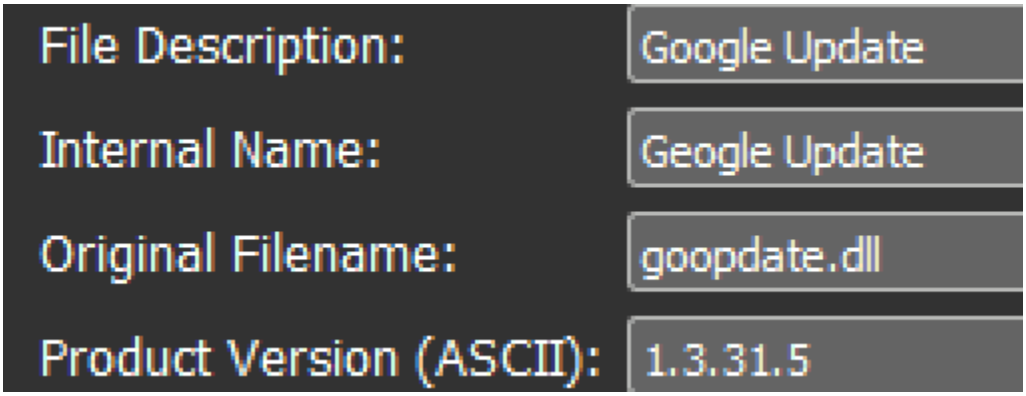
*.chatconnecting(.)com blog.versign(.)com vieweva(.)com tulationeva(.)com	teriava(.)com tonholding(.)com nsquery(.)net notificeva(.)com	23.227.196(.)210 104.237.218(.)72 45.114.117(.)137

Some of these domains were also mentioned in FireEye's APT32 report, further confirming our suspicions that the group behind the attack is the OceanLotus Group.

The group includes members who are fluent in at least two Asian languages. This claim is supported by the language used in the spear-phishing emails, which appear to be written by native speakers. In addition, the language localization settings found in few of the payloads suggest that the malware authors compiled the payloads on machines with Asian languages

support. The threat actors are not likely native English speakers since multiple typos were found in their payloads.

For example, the following typo was observed in the file metadata of one of the backdoors. Notice the “Internal Name” field (“Geogle Update”):



Threat Actor Profile

The attackers behind **Operation Cobalt Kitty** were extremely persistent. Even when their campaign was exposed, the attackers did not give up. They took “pauses” that lasted between 48 hours and four weeks and used the downtime to learn from their “mistakes” and develop workarounds before resuming the APT campaign.

The members of the **OceanLotus Group** demonstrated a remarkable ability to quickly adapt, introduce new tools and fine tune existing ones to bypass security solutions and avoid detection. The high number of payloads and the elaborate C2 infrastructure used in this attack can be indicative of the resources that the attackers had at their disposal. Simultaneously orchestrating multiple APT campaigns of such magnitude and sophistication takes time, financial resources and a large team who can support it.

Threat actor’s main characteristics

Here are the main characteristics that can help profile the threat actor:

- **Motivation** - Based on the nature of the attack, the proprietary information that the attackers were after and the high-profile personnel who were targeted, Cybereason concluded the main motivation behind the attack was cyber espionage. The attacker sought after specific documents and type of information. This is consistent with previous reports about the group’s activity show that the group has a very wide range of targets, spanning from government agencies, media, business sector, and more.

- **Operational working hours** - Most of the malicious activity was mostly done around normal business hours (8AM-8PM). Very little active hacking activity was detected during weekends. The attackers showed a slight tendency to carry out hacking operations towards the afternoon and evening time. These observations can suggest the following:
    - Time zone(s) proximity.
    - An institutionalized threat actor (possibly nation-state)
- **Outlook backdoor and data exfiltration** - One of the most interesting tools introduced by the attackers was the Outlook backdoor, which used Outlook as a C2 channel. This backdoor has not been publicly documented and is one of the most unique TTPs with regards to the threat actor. Outlook backdoors are not a new concept and have been observed in different APTs in the past. However, this specific type of Outlook backdoor is can be considered as one of the "signature tools" of the OceanLotus Group.

- **Publicly available tools** - The attackers showed a clear preference to use publicly available hacking tools and frameworks. Beyond being spared the hassle of creating a new tool, it is much harder to attribute a tool that can be used by anyone rather than a custom-made tool. However, the attackers should not be considered script-kiddies. Most of the publicly available tools were either obfuscated, modified and even merged with other tools to evade antivirus detection. This type of customization requires good coding skills and understanding of how those tools work.

- **Cobalt Strike usage in APT** - Cobalt Strike is a commercial offensive security framework designed to simulate complex attacks and is mainly used by security professionals in security audits and penetration testing. The **OceanLotus Group** was previously documented using Cobalt Strike as one of its main tools. Other Large scale APTs using Cobalt Strike have been reported before, such as APT-TOCS (could be related to OceanLotus), Ordinaff, Carbanak Group, and the Cobalt Group.

- **Custom-built backdoors -** The threat actor used very sophisticated and stealthy backdoors (Denis & Goopy) that were written by highly skilled malware authors. During the attack, the authors introduced new variants of these backdoors, indicating "on-the-fly" development capabilities. Developing such state-of-the-art backdoors requires skillful malware authors, time and resources. In addition, both the Denis and Goopy backdoors used DNS Tunneling for C2 communication. The OceanLotus Group is known to have a backdoor dubbed SOUNDBITE by FireEye that use this stealthy technique. However, no public analysis reports of SOUNDBITE is available to the time of writing this report.

- **Exploiting DLL hijacking in trusted applications** - The attackers exploited three DLL-hijacking vulnerabilities in legitimate applications from trusted vendors: **Microsoft, Google and Kaspersky**. This further indicates the group's emphasis on vulnerability research. DLL-hijacking / Side-loading attacks are not uncommon in APTs, some of which are also carried out by nation-state actors and advanced cyber-crime groups.

There have been reports in the past of GoogleUpdate exploited by PlugX by Chinese threat actors as well as the Bookworm RAT exploiting Microsoft and Kaspersky applications in APTs targeting Asia.

- **Insisting on fileless operation** - While fileless delivery infrastructure is not a feature that can be attributed to one specific group, it is still worth mentioning since the attackers went out of their way to restore the script-based PowerShell / Visual Basic operation, especially after PowerShell execution had been disabled in the entire organization.
- **C&C infrastructure**
  - **Divide and conquer** - Each tool communicated with different sets of C&C servers domains, which usually came in triads. For instance, Cobalt strike payloads communicated with certain sets of IPs/domains while the backdoors communicated with different sets of IPs/domains.
  - **Re-use of domains and IPs across campaigns -** Quite a few domains and IPs that were observed in Operation Cobalt Kitty were found in-the-wild, attacking other targets. It's rather peculiar why the threat actor re-used the same domains and IPs. It could be assumed that the malware operators wanted to have centralized C&C servers per tool or tools, where they could monitor all of their campaigns from dedicated servers.
  - **Anonymous DNS records** - Most of the domains point to companies that provide DNS data privacy and anonymization, such as PrivacyProtect and PrivacyGuardian.
  - **C&C server protection** - Most of the C&C servers IP addresses are protected by CloudFlare and SECURED SERVERS LLC.

OceanLotus Group activity in Asia

As part of the analysis of the domains and IPs that were used in this operation, Cybereason found samples that were caught "in-the-wild" (that were **not** part of Operation Cobalt Kitty). Analysis of those samples clearly indicates the involvement of the threat actor in Asia and Vietnam in particular. Both Qihoo 360 and FireEye demonstrate in their reports that the threat actor is involved in campaigns in different Asian countries, such as Vietnam, China, and the Philippines.

Most of the samples caught in-the-wild seem to target Vietnamese speakers. Some of the samples exhibit clear evidence of targeting Vietnamese entities. This conclusion is derived from the file names and file contents that are written in Vietnamese, as shown in the examples below:

File Name: Điện thoại bị cháy.doc
SHA-1: 38297392df481d2ecf00cc7f05ce3361bd575b04
Malicious Domain / IP: 193.169.245(.)137

File Name: ID2016.doc
SHA-1: bfb3ca77d95d4f34982509380f2f146f63aa41bc
Malicious Domain / IP: support.chatconnecting(.)com

File Name: Giấy yêu cầu bồi thường mới 2016 - Hằng.doc (Translation: "New Claim Form 2016")
SHA-1: A5bddb5b10d673cbfe9b16a062ac78c9aa75b61c
Malicious Domain / IP: blog.versign(.)info

Indicators of Compromise (IOCs)

Malicious files

Backdoors	
File name	**SHA-1 hash**
Msfte.dll ---------- Variant of Backdoor.Win32.Denis	be6342fc2f33d8380e0ee5531592e9f676bb1f94 638b7b0536217c8923e856f4138d9caff7eb309d dcbe007ac5684793ea34bf27fdaa2952c4e84d12 43b85c5387aafb91aea599782622eb9d0b5b151f
Goopdate.dll ---------- Goopy backdoor	9afe0ac621c00829f960d06c16a3e556cd0de249 973b1ca8661be6651114edf29b10b31db4e218f7 1c503a44ed9a28aad1fa3227dc1e0556bbe79919 2e29e61620f2b5c2fd31c4eb812c84e57f20214a c7b190119cec8c96b7e36b7c2cc90773cffd81fd 185b7db0fec0236dff53e45b9c2a446e627b4c6a ef0f9aaf16ab65e4518296c77ee54e1178787e21
product_info.dll [Backdoor exploiting DLL-hijacking against Kaspersky Avpia]	3cf4b44c9470fb5bd0c16996c4b2a338502a7517
VbaProject.OTM [Outlook Macro]	320e25629327e0e8946f3ea7c2a747ebd37fe26f
sunjavascheduler.ps1 sndVolSSO.ps1 SCVHost.ps1 fhsvcs.ps1 Goztp.ps1 [PowerShell versions of the Denis / Goopy backdoors]	0d3a33cb848499a9404d099f8238a6a0e0a4b471 c219a1ac5b4fd6d20a61bb5fdf68f65bbd40b453 91e9465532ef967c93b1ef04b7a906aa533a370e
Cobalt Strike Beacons	

File name	SHA-1 hash
dns.exe	cd675977bf235eac49db60f6572be0d4051b9c07
msfte.dll	2f8e5f81a8ca94ec36380272e36a22e326aa40a4
FVEAPI.dll	01197697e554021af1ce7e980a5950a5fcf88318
sunjavascheduler.ps1 syscheck.ps1 dns.ps1 activator.ps1 nvidia.db	7657769f767cd021438fcce96a6befaf3bb2ba2d Ed074a1609616fdb56b40d3059ff4bebe729e436 D667701804CA05BB536B80337A33D0714EA28129 F45A41D30F9574C41FE0A27CB121A667295268B2 7F4C28639355B0B6244EADBC8943E373344B2E7E
Malicious Word Documents ***Some of the phishing emails and Word documents were very targeted and personalized, therefore, they are not listed here for privacy reasons	
File name	**SHA-1 hash**
CV.doc Complaint letter.doc License Agreement.doc	[redacted]
Loader scripts	
File name	**SHA-1 hash**
syscheck.vbs	62749484f7a6b4142a2b5d54f589a950483dfcc9
SndVolSSO.txt	cb3a982e15ae382c0f6bdacc0fcecf3a9d4a068d

sunjavascheduler.txt	7a02a835016bc630aa9e20bc4bc0967715459daa
Obfuscated / customized Mimikatz	
File name	**SHA-1 hash**
dllhosts.exe	5a31342e8e33e2bbe17f182f2f2b508edb20933f 23c466c465ad09f0ebeca007121f73e5b630ecf6 14FDEF1F5469EB7B67EB9186AA0C30AFAF77A07C
KB571372.ps1	7CADFB90E36FA3100AF45AC6F37DC55828FC084A
KB647152.exe	7BA6BFEA546D0FC8469C09D8F84D30AB0F20A129
KB647164.exe	BDCADEAE92C7C662D771507D78689D4B62D897F9
kb412345.exe	e0aaa10bf812a17bb615637bf670c785bca34096
kb681234.exe	4bd060270da3b9666f5886cf4eeaef3164fad438
System.exe	33cb4e6e291d752b9dc3c85dfef63ce9cf0dbfbc 550f1d37d3dd09e023d552904cdfb342f2bf0d35
decoded base64 Mimikatz payload	c0950ac1be159e6ff1bf6c9593f06a3f0e721dd4
Customized credential dumpers	
File name	**SHA-1 hash**

log.exe [GetPassword_x64]	7f812da330a617400cb2ff41028c859181fe663f
SRCHUI.dll adrclients.dll [HookPasswordChange]	29BD1BAC25F753693DF2DDF70B83F0E183D9550D FC92EAC99460FA6F1A40D5A4ACD1B7C3C6647642
KB471623.exe [Custom password dumper]	6609A347932A11FA4C305817A78638E07F04B09F
doutlook.ps1 adobe.dat adrclients.ps1 [Custom password dumper]	EBDD6059DA1ABD97E03D37BA001BAD4AA6BCBABD B769FE81996CBF7666F916D741373C9C55C71F15 E64C2ED72A146271CCEE9EE904360230B69A2C1D
Miscellaneous tools	
File name	**SHA-1 hash**
pshdll35.dll pshdll40.dll [PSUnlock - PowerShell Bypass tool]	52852C5E478CC656D8C4E1917E356940768E7184 EDD5D8622E491DFA2AF50FE9191E788CC9B9AF89
KB-10233.exe kb74891.exe [NetCat]	C5e19c02a9a1362c67ea87c1e049ce9056425788 0908a7fbc74e32cded8877ac983373ab289608b3
IP.exe cmd.exe dllhost.exe [IP check Tool]	6aec53554f93c61f4e3977747328b8e2b1283af2

Payloads from C&C servers

URL	Payload SHA-1 hash

hxxp://104.237.218(.)67:80/icon.ico	6dc7bd14b93a647ebb1d2eccb752e750c4ab6b09
hxxp://support.chatconnecting(.)com:80/icon.ico	c41972517f268e214d1d6c446ca75e795646c5f2
hxxp://food.letsmiles(.)org/login.txt	9f95b81372eaf722a705d1f94a2632aad5b5c180
hxxp://food.letsmiles(.)org/9niL	5B4459252A9E67D085C8B6AC47048B276C7A6700
hxxp://23.227.196(.)210:80/logscreen.jpg	d8f31a78e1d158032f789290fa52ada6281c9a1f 50fec977ee3bfb6ba88e5dd009b81f0cae73955e
hxxp://45.114.117(.)137/eXYF	D1E3D0DDE443E9D294A39013C0D7261A411FF1C4 91BD627C7B8A34AB334B5E929AF6F981FCEBF268
hxxp://images.verginnet(.)info:80/ppap.png	F0A0FB4E005DD5982AF5CFD64D32C43DF79E1402
hxxp://176.107.176(.)6/QVPh	8FC9D1DADF5CEF6CFE6996E4DA9E4AD3132702C
hxxp://108.170.31(.)69/a	4a3f9e31dc6362ab9e632964caad984d1120a1a7
hxxp://support(.)chatconnecting(.)com/pic.png	bb82f02026cf515eab2cc88faa7d18148f424f72
hxxp://blog.versign(.)info/access/?version=4&lid=[redacted]&token=[redacted]	9e3971a2df15f5d9eb21d5da5a197e763c035f7a
hxxp://23.227.196(.)210/6tz8	bb82f02026cf515eab2cc88faa7d18148f424f72
hxxp://23.227.196(.)210/QVPh	8fc9d1dadf5cef6cfe6996e4da9e4ad3132702c5
hxxp://45.114.117(.)137/3mkQ	91bd627c7b8a34ab334b5e929af6f981fcebf268
hxxp://176.223.111(.)116:80/download/sido.jpg	5934262D2258E4F23E2079DB953DBEBED8F07981
hxxp://110.10.179(.)65:80/ptF2	DA2B3FF680A25FFB0DD4F55615168516222DFC10
hxxp://110.10.179(.)65:80/download/microsoftp.jpg	23EF081AF79E92C1FBA8B5E622025B821981C145
hxxp://110.10.179(.)65:80/download/microsoft.jpg	C845F3AF0A2B7E034CE43658276AF3B3E402EB7B

hxxp://27.102.70(.)211:80/image.jpg	9394B5EF0B8216528CED1FEE589F3ED0E88C7155

C&C IPs

45.114.117(.)137
104.24.119(.)185
104.24.118(.)185
23.227.196(.)210
23.227.196(.)126
184.95.51(.)179
176.107.177(.)216
192.121.176(.)148
103.41.177(.)33
184.95.51(.)181
23.227.199(.)121
108.170.31(.)69
104.27.167(.)79
104.27.166(.)79
176.107.176(.)6
184.95.51(.)190
176.223.111(.)116
110.10.179(.)65
27.102.70(.)211

C&C Domains

food.letsmiles(.)org
help.chatconnecting(.)com
*.letsmiles(.)org
support.chatconnecting(.)com
inbox.mailboxhus(.)com
blog.versign(.)info
news.blogtrands(.)net
stack.inveglob(.)net
tops.gamecousers(.)com
nsquery(.)net
tonholding(.)com
cloudwsus(.)net
nortonudt(.)net
teriava(.)com
tulationeva(.)com

vieweva(.)com
notificeva(.)com
images.verginnet(.)info
id.madsmans(.)com
lvjustin(.)com
play.paramountgame(.)com

Appendix A: Threat actor payloads caught in the wild

Domain	Details	VirusTotal
inbox.mailboxhus(.)com support.chatconnecting(.)com (45.114.117.137)	**File name:** Flash.exe **SHA-1:** 01ffc3ee5c2c560d29aaa8ac3d17f0ea4f6c0c09 **Submitted:** 2016-12-28 09:51:13	Link
inbox.mailboxhus(.)com support.chatconnecting(.)com (45.114.117[.]137)	**File name:** Flash.exe **SHA-1:** 562aeced9f83657be218919d6f443485de8fae9e **Submitted:** 2017-01-18 19:00:41	Link
support.chatconnecting(.)com (45.114.117[.]137)	**URL:** hxxp://support(.)chatconnecting.com/2nx7m **Submitted:** 2017-01-20 10:11:47	Link
support.chatconnecting(.)com (45.114.117[.]137)	**File name:** ID2016.doc **SHA-1:** bfb3ca77d95d4f34982509380f2f146f63aa41bc **Submitted:** 2016-11-23 08:18:43 Malicious Word document (Phishing text in Vietnamese)	Link
blog(.)versign(.)info (23.227.196[.]210)	**File name:** tx32.dll **SHA-1:** 604a1e1a6210c96e50b72f025921385fad943ddf **Submitted:** 2016-08-15 04:04:46	Link
blog(.)versign(.)info (23.227.196[.]210)	**File name:** Giấy yêu cầu bồi thường mới 2016 - Hằng.doc **SHA-1:** a5bddb5b10d673cbfe9b16a062ac78c9aa75b61c **Submitted:** 2016-10-06 11:03:54 Malicious Word document with Phishing text in Vietnamese	Link

blog(.)versign(.)info (23.227.196[.]210)	**File name:** Thong tin.doc **SHA-1:** a5fbcbc17a1a0a4538fd987291f8dafd17878e33 **Submitted:** 2016-10-25 Malicious Word document with Phishing text in Vietnamese	Link
Images.verginnet(.)info id.madsmans(.)com (176.107.176[.]6)	**File name:** WinWord.exe **SHA-1:** ea67b24720da7b4adb5c7a8a9e8f208806fbc198 **Submitted:** Cobalt Strike payload Downloads hxxp://images.verginnet(.)info/2NX7M Using Cobalt Strike malleable c2 oscp profile	Link
tonholding(.)com nsquery(.)net	**File name:** SndVolSSO.exe **SHA-1:** 1fef52800fa9b752b98d3cbb8fff0c44046526aa **Submitted:** 2016-08-01 09:03:58 Denis Backdoor Variant	Link
tonholding(.)com nsquery(.)net	**File name:** Xwizard / KB12345678.exe **SHA-1:** d48602c3c73e8e33162e87891fb36a35f621b09b **Submitted:** 2016-08-01	Link
teriava(.)com	**File name:** CiscoEapFast.exe **SHA-1:** 77dd35901c0192e040deb9cc7a981733168afa74 **Submitted:** 2017-02-28 16:37:12 Denis Backdoor Variant	Link

Appendix B: Denis Backdoor samples in the wild

File name	SHA-1	Domain
msprivs.exe	97fdab2832550b9fea80ec1b9c182f5139e9e947	teriava(.)com
WerFault.exe	F25d6a32aef1161c17830ea0cb950e36b614280d	teriava(.)com
msprivs.exe	1878df8e9d8f3d432d0bc8520595b2adb952fb85	teriava(.)com
CiscoEapFast.exe 094.exe	1a2cd9b94a70440a962d9ad78e5e46d7d22070d0	teriava(.)com, tulationeva(.)com,

		notificeva(.)com
CiscoEapFast.exe	77dd35901c0192e040deb9cc7a981733168afa74	teriava(.)com, tulationeva(.)com, notificeva(.)com
SwUSB.exe F:\malware\Anh Dương\lsma.exe	88d35332ad30964af4f55f1e44c951b15a109832	gl-appspot(.)org tonholding(.)com nsquery(.)net
Xwizard.exe KB12345678.exe	d48602c3c73e8e33162e87891fb36a35f621b09b	tonholding(.)com nsquery(.)net
SndVolSSO.exe	1fef52800fa9b752b98d3cbb8fff0c44046526aa	tonholding(.)com nsquery(.)net

cybereason®

Cybereason is the leader in endpoint protection, offering endpoint detection and response, next-generation antivirus, and active monitoring services. Founded by elite intelligence professionals born and bred in offense-first hunting, Cybereason gives enterprises the upper hand over cyber adversaries. The Cybereason platform is powered by a custom-built in-memory graph, the only truly automated hunting engine anywhere. It detects behavioral patterns across every endpoint and surfaces malicious operations in an exceptionally user-friendly interface. Cybereason is privately held and headquartered in Boston with offices in London, Tel Aviv, and Tokyo.