

Presenter + team



@cyberoverdrive

Senior Threat Intelligence Analyst...

@PwC UK

Sveva Vittoria Scenarelli

- Focus on APAC-based APTs
- "Malware intertextuality" & codebase evolution analysis
- CONFidence Online 2020, CyberThreat 2019

... but really, it takes a team.

John Southworth

@BitsOfBinary

Jason Smart

@pewpew_lazors

Disclosure of a campaign targeting Kimsuky: a timeline entities involved with the PveongChang Olympics with a PowerShell implant and GoldDragon RAT. Disclosure of an espionage AppleSeed campaign campaign targeting the Since at least February 2019, South Korean government Kimsuky introduces a RAT used to with a new RAT, MyDogs BabyShark begins target Japanese defence contractors. A multi-stage, script-based The website of Washington University downloader is used to target is compromised and used for C2. policy, national security, and cryptocurrency entities in the FlowerPower identified US, South Korea, Europe **KHNP Breach** A new first-stage victim KHNP employees hacked, profiling tool, used since at Kimsuky poses as "Who least November 2019, has Universities and public am I = No Nuclear Power" links to GoldDragon More WildCommand sector entities receive hacktivist persona and South Korea targeted WildCommand RAT malicious documents threatens sabotage attacks using server-side scripts resurfaces, is used to created by author "MOFA" similar to BabyShark ones target financial entities and leading to installation in South-East Asia of Kimsuky implants 2017 . . . 02 • • • 11 12 2019 • • 03 • 05 • 09 • • • • 02 03 04 · · 06 · · · · · · · · 2013 09 • 2014 • • 11 2015 • • • • 2016 2018 Kimsuky Winter Interests Disclosure of an espionage Credential phishing campaign Credential phishing campaign campaign targeting South since at least August 2018, **Autumn Aperture** targeting Japanese Korean defence think tanks targeting orgs and The BabvShark government and technology Government & research and Korea unification policy government depts, (mainly in campaign continues sector, diplomatic missions organisations credential phishing the US) involved in North targeting US entities in South Korean authorities Korea research, policy, the defence and Kimsuky supranational targeting attributed to Kimsukv a international relations, and national security space Since at least December 2019, a sanctions spear phishing campaign credential phishing campaign impersonating the targets the Office of the UN High Cheongwadae **Malicious HWP Spear** Commissioner for Human Rights phishing continues: Since at least December 2018, GoldDragon / GHOST419 Kimsuky introduces a RAT used to Return of the GoldDragon The continuing spearphishing target South Korean government Malicious HWP files are campaigns deliver an implant and media. In May 2019, the used to deliver GoldDragon To catch a Banshee September 2020 known as GHOST419 or same RAT is used to target the malware to private sector PwC UK

defence and aerospace sector

entities in South Korea

GoldDragon RAT

This presentation has many questions

How do Black Banshee's tools, infrastructure, targeting and strategic objectives intersect?

How do they connect Black Banshee's campaigns in a tight-knight web of activity?

What function do Black Banshee's campaigns perform, among other North Korea-based cyber threats?

To answer them, we need to:

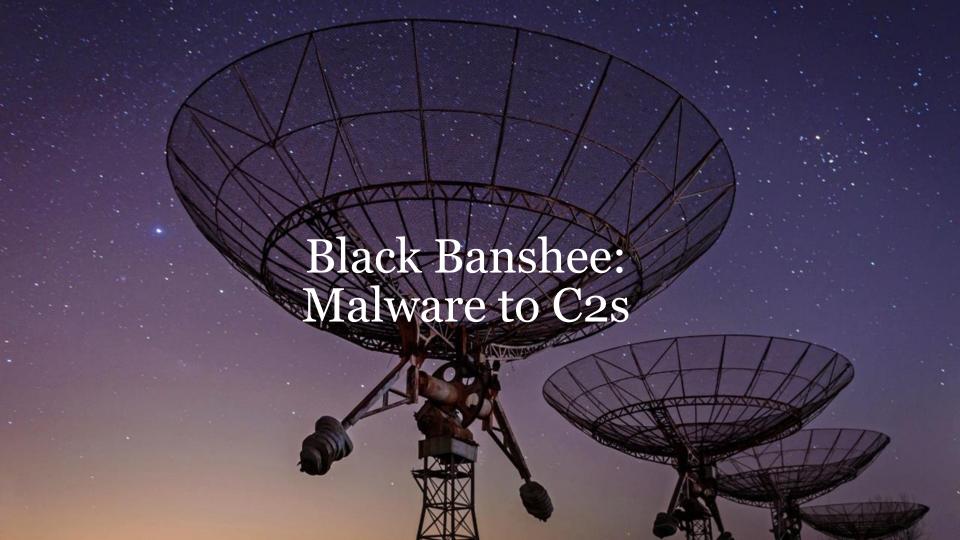
Understand the malware

Map out the infrastructure

Cluster the campaigns

Pinpoint their intersections

Identify the strategic targets





SHA256: 66AC66A8E2D8560F8287BFB23F0964CCB930585A96C0029292C4963FF896011A

VBScript-based, sequential malware: persistent downloader / loader, executing further scripts/payloads

Track through...

Encoding routine (roughly the same since at least 2018, different key; there is at least one other variant)

URL paths (incremental parameters; server-side script names)

```
On Error Resume Next

Function Co00(c): L=Len(c):s="":For jx=0 To d-1:For ix=0 To Int(L/d)-1:s=s&Mid(c,ix*d+jx+1,1):Next:Next:s=
s&Right(c,L-Int(L/d)*d):Co00=s:End Function
set fso = CreateObject("Scripting.FileSystemObject")
path= wscript.scriptfullname
set f = fso.OpenTextFile(path, 1, True)
data = f.ReadLine
f.Close
strl=Right(data,Len(data)=1)
sdgf:d=3:strl=Co00(strl):Execute(strl):sdfg
```

PWC UK 6



hxxps://jonashartley[.]com /hilaryolsen/wp-includes/ customize/1111/Brzol0.hta

hxxp://jonashartlev[.]com /archive/css/0924/ zjirz0.hta

hxxps://jonashartley[.]com /hilaryolsen/wp-includes/ customize/1111/res.php?op= 14.0

hxxps://jonashartley[.]com /hilaryolsen/wp-includes/ customize/1111/res.php?op=

2018-06-13

2018-06-21

2019-10-01

2019-11-12

2019-11-21

2019-11-22

2019-11-24

2019-11-26

hxxp://jonashartley[.]com /hilaryolsen/wp-admin/ network/run.php

hxxp://jonashartley[.]com /hilarvolsen/wpadmin/network/cow.php

hxxps://jonashartley[.]com/ hilaryolsen/wp-includes/ customize/1111/expres.php

hxxp://jonashartley[.]com /hilaryolsen/wpincludes/images/crystal/ 1122/upload.php

hxxp://jonashartlev[.]com /hilarvolsen/wpincludes/images/crystal/ 1122/dbrcn0.hta

hxxps://jonashartley[.]com/ archive/css/0924/Zjirz.hta

hxxp://jonashartley[.] com/hilarvolsen/wpincludes/customize/1111 /res.php?op=12.0

hxxps://jonashartley[.] com/hilaryolsen/wpincludes/random compat/ 1122/expres.php

September 2020



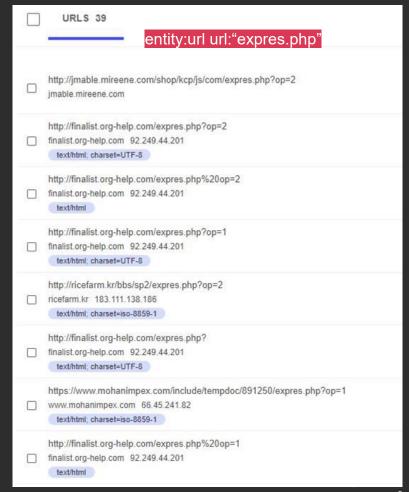
BabyShark URL structure:

Known server-side scripts:

- expres.php?op=
- cow.php

Recent server-side scripts and payloads:

- cross.php?op=
- res.php?op=
- .php?er=
- pre.hta
- suf.hta





SHA256: 9e004a659e8cb6236ac56671e4afa4b8fbb6f394807aa3decf6e268e17359ec6

Backdoor that uses temporary JavaScript files (executed via WScript) to connect with the C2

- In use since at least October 2019
- Mutex: I'M POSSIBLE or <*IMPOSSIBLE*>
- Masquerading as AVs
 - o ESTsoft\Common
 - o %APPDATA%\software\microsoft\windows\
 Autopatch\autopatch.dll
 - o %PROGRAMDATA%\software\microsoft\
 windows\defender\autoupdate.dll
- Tiny Banshee self-delete batch script



909d3f529b6990d0129ba356ec8163e9f30658649a9f d3201ad776aaa56fa35c26712ce488a6a3ec813337ee23 e9117e9bfc06571fb2c36fbc693 1b24f3b562dd37640999ae1c6be7fcbb7834a67d7acbd1 8e30d3e083cf31c9f918270bd1c40290a1 37c666b69c8e69731fa7838f40b7ddac73c7ce08e40f14 p2=%s-%s-v%d http:// http://%s/%s/ 455301367a247db9eec4da21193c0c1135077227353f26 3cf84870abc8e7c8490a20594520c9d66ff8d6d20ea732 4811f7391203be771804e6d62c888aa31f67fea3deaa67

```
.bat
:repeat
del "%s"
if exist "%s" goto repeat
del "%%~f0"
```



AppleSeed: C2 Hunting

Track through...

Unique encoding routine:

- Hex strings, each with unique 16-byte key
- Each char XOR'ed with corresponding key byte + XOR'ed with previous char

AppleSeed URL structure:

e.g.

hxxp://suzuki[.]datastore[.]pe[.]hu/?m=a&p1= 1253dc67f01a&p2=win_6.1.7601-x64_DROPPER

entity:url url:"m=a&p1="
http://depts.washington.edu/dswkshp/wordpress/wp-content/themes/twentyfifteen/inc/io/?m=a&p1=qweasdzxc&p2= depts.washington.edu 140.142.11.80 text/html; charset=UTF-8
http://eastsea.or.kr/?m=a&p1=00000009&p2=Win6.1.7601x64-Spy-v2370390 eastsea.or.kr 45.13.135.103 text/html; charset=UTF-8
http://www.gotoclean.com.co/wp-content/themes/purify/manapater/?m=a&p1=1866da123456&p2=win_6.1.7601-x64 www.gotoclean.com.co 23.111.164.98 text/html; charset=UTF-8
http://dongnam2014.cafe24.com/image/main/sub/?m=a&p1=00163eebca74&p2=win_6.1.7601-x32_SPY dongnam2014.cafe24.com 183.111.174.11 [text/html; charset=iso-8859-1]
http://dept.lab.hol.es/?m=a&p1=080027ce3723&p2=win_10.0.18363-x64_SPY dept.lab.hol.es
http://upload.bigfile.hol.es/?m=a&p1=[ID]&p2=version-x32_DROPPER3 upload.bigfile.hol.es 45.13.135.103 text/html; charset=UTF-8
http://upload.bigfile.hol.es/?m=a&p1=[ID]&p2=version-x32_DROPPER upload.bigfile.hol.es 45.13.135.103
http://dept.lab.hol.es/?m=a&p1=b4c87b339433&p2=win_6.1.7601-x64_SPY dept.lab.hol.es 45.13.135.103 text/html; charset=UTF-8
http://suzuki.datastore.pe.hu/?m=a&p1=a86dd8e43948&p2=win_6.1.7601-x64_DROPPER suzuki.datastore.pe.hu 45.13.135.103 text/html; charset=UTF-8



SHA256: d36ac36d278c264362ec31e116a46daaa4a7287a9dcd689d665a5ab1fd5416b8

PowerShell victim profiling tool: Initial persistent implant; identify victim and/or drop further payloads

Server-side folders names change every time; but sometimes there is correspondence: e.g. "mybobo" payload and "mybobo" C2 domain; "flower", as per below, was where the name came from)

Track through...

Unobfuscated functions and execution logs (e.g. "Success"; "UpLoad Fail!!!")

Function name	Functionality		
main	Sets persistence through a Run Key, creates a log file, and executes all other functions in the script in this order: Get_Info, FileUploading, and Download.		
Get_info	Gathers basic system information and performs basic file listing.		
FileUploading	Calls UpLoadFunc and echoes whether UpLoadFunc worked successfully.		
UpLoadFunc	Encodes all data in the log file and sends it to the C2 via HTTP POST.		
Download	Downloads a resource from the C2 and executes it through PowerShell.		
decode	Uses a 160-bit key to encode data sent to the C2 and decode data received.		



FlowerPower: C2 Hunting

entity:url url:"/flower01/"
http://mybobo.mygamesonline.org/flower01/post.php mybobo.mygamesonline.org 185.176.43.82 text/html; charset=UTF-8
http://mybobo.mygamesonline.org/flower01/flower01.down mybobo.mygamesonline.org 185.176.43.82 text/html
http://mybobo.mygamesonline.org/flower01/del.php?filename=flower01 mybobo.mygamesonline.org
http://pootbal2020tennis.mypressonline.com/flower01/flower07/flower07.ps1 pootbal2020tennis.mypressonline.com
text/html
http://mybobo.mygamesonline.org/flower01 mybobo.mygamesonline.org 185.176.43.82 text/html
http://pootbal2020tennis.mypressonline.com/flower01/flower07/post.php pootbal2020tennis.mypressonline.com 185.176.43.82 text/html; charset=UTF-8
text/html
http://mybobo.mygamesonline.org/flower01/flower01.ps1 mybobo.mygamesonline.org 185.176.43.82

entity:url url:"/eodo/"
http://foxhunter.medianewsonline.com/eodo/download.php?filename= foxhunter.medianewsonline.com 185.176.43.80 text/html; charset=UTF-8
http://foxhunter.medianewsonline.com/eodo/down.txt foxhunter.medianewsonline.com 185.176.43.80 fext/plain
http://foxhunter.medianewsonline.com/eodo/post.php foxhunter.medianewsonline.com 185.176.43.80 text/html; charset=UTF-8
http://foxhunter.medianewsonline.com/eodo/download.php foxhunter.medianewsonline.com 185.176.43.80 text/html; charset=UTF-8
http://foxonline123.atwebpages.com/eodo/1.ps1 foxonline123.atwebpages.com 185.176.43.80 fext/html
http://mybobo.scienceontheweb.net/eodo/bobo.ps1 mybobo.scienceontheweb.net 185.176.43.82 text/html
http://mybobo.myartsonline.com/eodo/blank.php?v=freestrong mybobo.myartsonline.com 185.176.43.82 image/png
http://mybobo.scienceontheweb.net/eodo/bobo.down mybobo.scienceontheweb.net 185.176.43.82 text/html
http://mybobo.myartsonline.com/eodo/bobo.ps1 mybobo.myartsonline.com 185.176.43.82

To catch a Banshee: WebForm Boundaries

WebForm boundaries are a KEY component in tracking Black Banshee malware as well as C2 Infrastructure.

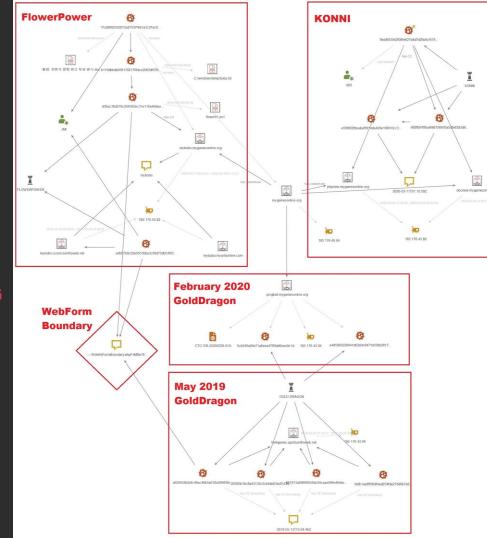
Notable examples:

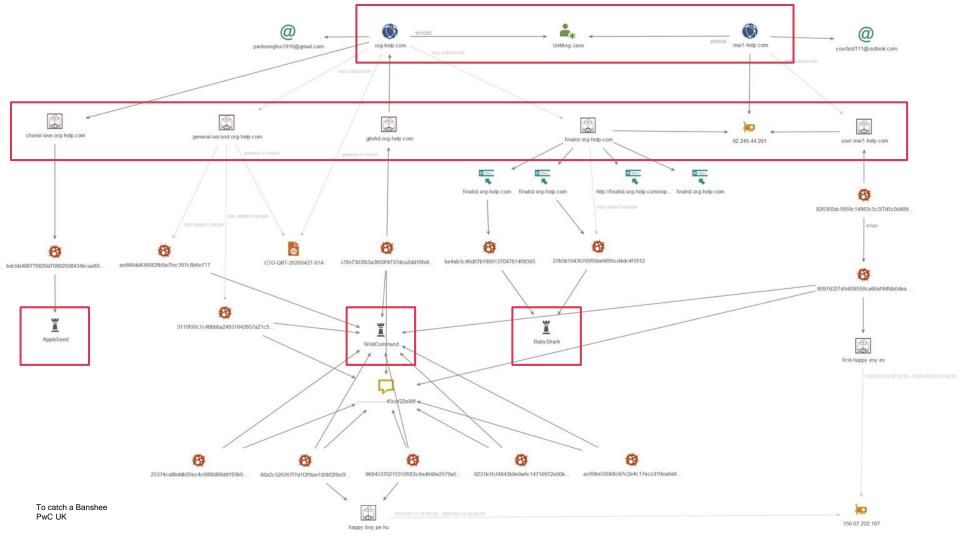
----WebKitFormBoundarywhpFxMBe19cSjFnG

• In both GoldDragon and FlowerPower

----4cef22e90f

• Across samples of WildCommand







To catch a Banshee: One pivot to find them

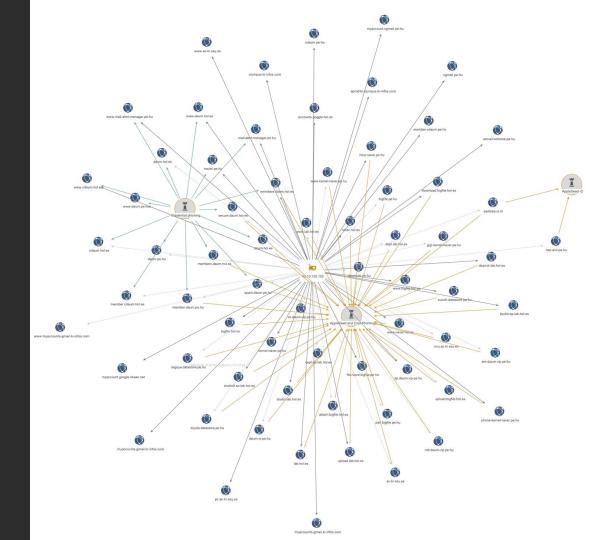
Black Banshee C2 infrastructure tends to have many overlaps

Let's take a single IP: 45.13.135[.]103

- Different domains over months
- Goldmine of email phishing (Gmail, Naver, Daum...)
- Crossover with AppleSeed C2s
- MIND THE HYPHEN

More specific targeting examples:

snu[.]ac-kr[.]esy[.]es
toyota[.]datastore[.]pe[.]hu
suzuki[.]datastore[.]pe[.]hu



To catch a Banshee: Domain names & patterns

Generic Themes	Specific Themes	Banshee-registered domains	(Shared) parent domains
Account	AhnLab	org-help[.]com	pe[.]hu
Login	Alyac	ma1I-help[.]com	hol[.]es
Mail	Daum	manager-alert[.]com	esy[.]es
Manage	Kakao	org-view[.]work	*[.]work
Member	Naver	doc-view[.]work	atwebpages[.]com
Secure	NTT Docomo	account-protect[.]work	mygamesonline[.]org
User	OHCHR	com-ssinet[.]work	myartsonline[.]com

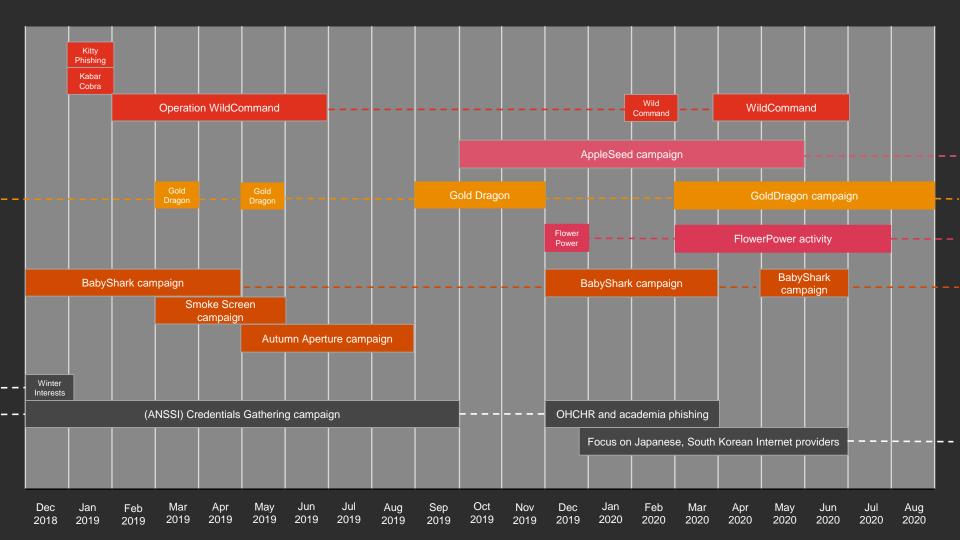
Recent examples:

user[.]mai1-help[.]com

ohchr[.]org-view[.]work

ramble[.]myartsonline[.]com





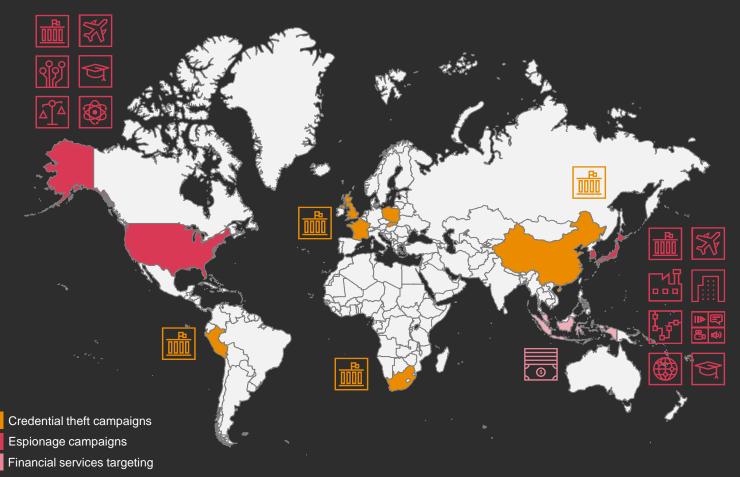
Targeting

Supranational targeting









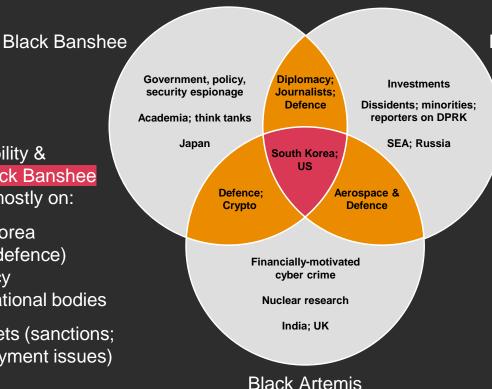
To catch a Banshee PwC UK September 2020

Pieces of a puzzle

From our visibility & collection, Black Banshee has focused mostly on:

- South Korea
- Japan (defence)
- US policy
- Supranational bodies

Strategic targets (sanctions; THAAD deployment issues)



Black Shoggoth

Progressive evolution from Banshee's 2019 targeting, in 2020 Black Artemis has "picked up" some traditional Black Banshee targets (e.g. energy, nuclear).

Black Shoggoth & Banshee continue overlapping in targeting of journalists, NGOs, plus East & SE Asia.



This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2020 PricewaterhouseCoopers LLP. All rights reserved. PwC refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

PwC public reporting on Black Banshee

'Tracking 'Kimsuky', the North Korea-based cyber espionage group: Part 1', PwC UK, https://www.pwc.co.uk/issues/cyber-espionage-group-part-1.html (18th February 2020)

'Tracking 'Kimsuky', the North Korea-based cyber espionage group: Part 2', PwC UK, https://www.pwc.co.uk/issues/cyber-espionage-group-part-2.html (9th March 2020)

Tracking 'Kimsuky', the North Korea-based cyber espionage group: Part 1

18 February, 2020

For years, we have tracked the espionage threat actor we call Black Banshee (also known in open source as Kimsuky). In 2019, it launched multiple parallel cyber espionage campaigns, from large-scale credential harvesting to narrowly targeted espionage and exfiltration operations.

The foundations for this activity began in August 2018, when we observed Black Banshee setting up a substantial number of domains impersonating organisations across the government, academia, and policy sectors. This formed the basis for multiple spear-phishing and credential harvesting campaigns.

Tracking 'Kimsuky', the North Korea-based cyber espionage group: Part 2

09 March 2020

In 2019, PwC observed an increase in activity by North Korea-based threat actor Black Banshee, also known as 'Kimsuky'.

In <u>our previous blog</u>, we examined some of the tradecraft exhibited by Black Banshee in its infrastructure setup. We discussed the threat actor's reliance on certain IP ranges and domains, as well as its naming conventions for malicious domains and command and control server paths.

References

'The Kimsuky Operation: A North Korean APT?', Kaspersky, https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/ (11th September 2013)

'Commissioner of the National Police Agency "Blue House Impersonation E-mail, North Korean Hacker Action', Hani, http://www.hani.co.kr/arti/PRINT/730395.html (15th February 2016)

'Malicious Document Targets PyeongChang Olympics', McAfee, https://securingtomorrow.mcafee.com/mcafee-labs/malicious-document-targets-pyeongchang-olympics/ (6th January 2018)

'Gold Dragon Widens Olympics Malware Attacks, Gains Permanent Presence on Victims' Systems', McAfee, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/ (2nd February 2018)

'오퍼레이션 김수키(Kimsuky)의 은밀한 활동, 한국 맞춤형 APT 공격은 현재 진행형', EST Security, https://blog.alyac.co.kr/1536 (12th February 2018)

'Kimsuky hacking group's targeted APT attack in Korea... Even now', DailySecu, https://www.dailysecu.com/news/articleView.html?idxno=30007 (13th February 2018)

References

'김수키(Kimsuky) 조직, 스텔스 파워(Operation Stealth Power) 침묵 작전', EST Security, <u>https://blog.alyac.co.kr/2234</u> (4th March 2019)

'한・미 겨냥 APT 캠페인 '스모크 스크린' Kimsuky 실체 공개', EST Security, https://blog.alyac.co.kr/2243 (17th March 2019)

'Analysis of the APT Campaign Smoke Screen targeting to Korea', EST Security, http://blog.alyac.co.kr/attachment/cfile5.uf@99A0CD415CB67E210DCEB3.pdf (30th April 2019)

'BabyShark Malware Part Two: Attacks Continue Using KimJongRat and PCRat', Palo Alto Networks, https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using-kimjongrat-and-pcrat/
(26th April 2019)

'The All-Purpose Sword: North Korea's Cyber Operations and Strategies', J.Y. Kong, J.I. Lim, and K.G. Kim, 2019 11th International Conference on Cyber Conflict: Silent Battle, eds. T. Minárik, et al., https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf (2019)

'Operation Kabar Cobra', AhnLab, https://global.ahnlab.com/global/upload/download/techreport/ [Analysis_Report]Operation%20Kabar%20Cobra%20(1).pdf (7th January 2019)

The Double Life of Sector A05 Nesting in Agora (Operation Kitty Phishing)', ThreatRecon, https://threatrecon.nshc.net/2019/01/30/operation-kitty-phishing/ (30th January 2019)

References

'Suspected North Korean Cyber Espionage Campaign Targets Multiple Foreign Ministries and Think Tanks', Anomali, https://www.anomali.com/blog/suspected-north-korean-cyber-espionage-campaign-targets-multiple-foreign-ministries-and-think-tanks (22nd August 2019)

'Credentials Gathering Campaign: Large clusters of malicious infrastructure targeting government bodies and other strategic entities', Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-CTI-002-EN.pdf (2nd September 2019)

'Autumn Aperture Report', Prevailion, https://blog.prevailion.com/2019/09/autumn-aperture-report.html (11th September 2019)

'Kimsuky Group: Track the King of the Spear-Phishing", Financial Security Institute: Jaeki Kim, Kyoung-Ju Kwak, Min-Chang Jang, https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-Kim.pdf (4th October 2019)

'Security Issue: Analysis Report on Operation Red Salt', in 'ASEC Report Vol. 96 Q3 2019', AhnLab, https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.96_ENG.pdf (2019)

'[스페셜 리포트] 미국 MS가 고소한 탈륨 그룹, 대한민국 상대로 '페이크 스트라이커' APT 캠페인 위협 고조', EST Security, https://blog.alyac.co.kr/3120 (25th July 2020)