To catch a Banshee:
How Kimsuky’s tradecraft betrays its complementary campaigns and mission

Sveva Vittoria Scenarelli
September 2020
To catch a Banshee

PwC UK

September 2020

@cyberoverdrive

Presenter + team

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
Kimsuky: a timeline

**To catch a Banshee**
Disclosure of a campaign targeting entities involved with the PyeongChang Olympics with a PowerShell implant and GoldDragon RAT.

**Olympics PowerShell + GoldDragon**
Disclosure of a campaign targeting entities involved with the PyeongChang Olympics with a PowerShell implant and GoldDragon RAT.

**BabyShark begins**
A multi-stage, script-based downloader is used to target policy, national security, and cryptocurrency entities in the US, South Korea, Europe.

**Operation Red Salt**
Disclosure of an espionage campaign targeting the South Korean government with a new RAT, MyDogs

**AppleSeeds campaign**
Since at least February 2019, Kimsuky introduces a RAT used to target Japanese defense contractors. The website of Washington University is compromised and used for C2.

**Operation Kabar Cobra / Kitty Phishing / WildCommand**
Since at least December 2018, Kimsuky introduces a RAT used to target South Korean government and media. In May 2019, the same RAT is used to target the defense and aerospace sector

**More WildCommand**
WildCommand RAT resurfaces, is used to target financial entities in South-East Asia

**Operation Stealth Power**
South Korea targeted using server-side scripts similar to BabyShark ones

**FlowerPower identified**
A new first-stage victim profiling tool, used since at least November 2019, has links to GoldDragon

**Malicious HWP Spear phishing continues: GoldDragon / GHOST419**
The continuing spear phishing campaigns deliver an implant known as GHOST419 or GoldDragon RAT

**KHNP Breach**
KHNP employees hacked, Kimsuky poses as “Who am I = No Nuclear Power” hacktivist persona and threatens sabotage attacks

**KHNP Breach**
KHNP employees hacked, Kimsuky poses as “Who am I = No Nuclear Power” hacktivist persona and threatens sabotage attacks

**Government & research credential phishing**
South Korean authorities attributed to Kimsuky a spear phishing campaign impersonating the Cheongwadae

**Malicious HWP Spear phishing**
Universities and public sector entities receive malicious documents created by author “MOFA” and leading to installation of Kimsuky implants

**Kimsuky Winter Interests**
Credential phishing campaign since at least August 2018, targeting orgs and government depts. (mainly in the US) involved in North Korea research, policy, international relations, and sanctions

**Autumn Aperture**
The BabyShark campaign continues targeting US entities in the defense and national security space

**Kimsuky Winter Interests**
Since at least December 2018, Kimsuky introduces a RAT used to target South Korean government and media. In May 2019, the same RAT is used to target the defense and aerospace sector

**Operation Kabar Cobra / Kitty Phishing / WildCommand**
Since at least December 2018, Kimsuky introduces a RAT used to target South Korean government and media. In May 2019, the same RAT is used to target the defense and aerospace sector

**Operation Kabar Cobra / Kitty Phishing / WildCommand**
Since at least December 2018, Kimsuky introduces a RAT used to target South Korean government and media. In May 2019, the same RAT is used to target the defense and aerospace sector

**To catch a Banshee**
Credibility phishing campaign targeting Japanese government and technology sector, diplomatic missions

**Return of the GoldDragon**
Malicious HWP files are used to deliver GoldDragon malware to private sector entities in South Korea

---

*PwC UK*
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**
BabyShark

SHA256: 66AC66A8E2D8560F8287BFB23F0964C8B930585A96C0029292C4963FF896011A

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)
To catch a Banshee

BabyShark: C2 testing

hxps://jonashartley[.]com/hilaryolsen/wp-includes/customize/1111/Brzol0.hra
hxps://jonashartley[.]com/hilaryolsen/wp-includes/customize/1111/res.php?op=14.0
hxps://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

hxps://jonashartley[.]com/hilaryolsen/wp-admin/network/run.php
hxps://jonashartley[.]com/hilaryolsen/wp-admin/network/cow.php
hxps://jonashartley[.]com/hilaryolsen/wp-includes/images/crystal/1122/upload.php
hxps://jonashartley[.]com/hilaryolsen/wp-includes/images/crystal/1122/dbrcn0.hra
hxps://jonashartley[.]com/hilaryolsen/wp-includes/random_compat/1122/expres.php
hxps://jonashartley[.]com/archive/css/0924/Zjirz0.hra
hxps://jonashartley[.]com/archive/css/0924/0924/Zjirz.hra

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

To catch a Banshee
PwC UK

September 2020
BabyShark: C2 hunting

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
AppleSeed

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
  - ESTsoft\Common
  - %APPDATA%\software\microsoft\windows\Autopatch\autopath.dll
  - %PROGRAMDATA%\software\microsoft\windows\defender\autoupdate.dll
- Tiny Banshee self-delete batch script

```
bat
:repeat
    del "%s"
    if exist "%s" goto repeat
:repeat
```

- Database
- History
- update.dll
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.

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

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. “mybob0” payload and “mybob0” C2 domain; “flower”, as per below, was where the name came from)

Track through…

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

<table>
<thead>
<tr>
<th>Function name</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>main</td>
<td>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.</td>
</tr>
<tr>
<td>Get_info</td>
<td>Gathers basic system information and performs basic file listing.</td>
</tr>
<tr>
<td>FileUploading</td>
<td>Calls UpLoadFunc and echoes whether UpLoadFunc worked successfully.</td>
</tr>
<tr>
<td>UpLoadFunc</td>
<td>Encodes all data in the log file and sends it to the C2 via HTTP POST.</td>
</tr>
<tr>
<td>Download</td>
<td>Downloads a resource from the C2 and executes it through PowerShell.</td>
</tr>
<tr>
<td>decode</td>
<td>Uses a 160-bit key to encode data sent to the C2 and decode data received.</td>
</tr>
</tbody>
</table>
FlowerPower: C2 Hunting

URLS 20
text:
http://mybobo.mygamesonline.org/flower01/post.php
http://mybobo.mygamesonline.org 185 176.43.82
http://mybobo.mygamesonline.org/flower01/flower01.down
http://mybobo.mygamesonline.org 185 176.43.82
http://mybobo.mygamesonline.org/flower01/del.php?filename=flower01
http://mybobo.mygamesonline.org
http://poobta2020tennis.mypressonline.com/flower01/flower07/flower07.ps1
poobta2020tennis.mypressonline.com

entity:url url:"/flower01/"

URLS 11
text:
http://foxhunter.medianewsonline.com/eodo/download.txt
http://foxhunter.medianewsonline.com 185 176.43.80
text/plain
http://foxhunter.medianewsonline.com 185 176.43.80
http://foxhunter.medianewsonline.com/eodo/download.php
http://foxhunter.medianewsonline.com 185 176.43.80
http://foxonline123.atwebpages.com/eodo/1.ps1
http://foxonline123.atwebpages.com 185 176.43.80
text/html
http://mybobo.scienceontheweb.net/eodo/bobo.ps1
http://mybobo.scienceontheweb.net 185 176.43.82
http://mybobo.scienceontheweb.net/eodo/blank.php?v=feestrong
http://mybobo.myartsonline.com 185 176.43.82
image/png
http://mybobo.scienceontheweb.net/eodo/bobo.dwn
http://mybobo.scienceontheweb.net 185 176.43.82
text/html
http://mybobo.myartsonline.com/eodo/bobo.ps1
http://mybobo.myartsonline.com 185 176.43.82

entity:url url:"/eodo/"
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
Black Banshee: C2s to more C2s
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

<table>
<thead>
<tr>
<th>Generic Themes</th>
<th>Specific Themes</th>
<th>Banshee-registered domains</th>
<th>(Shared) parent domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>AhnLab</td>
<td>org-help[.]com</td>
<td>pe[.]hu</td>
</tr>
<tr>
<td>Login</td>
<td>Alyac</td>
<td>ma1l-help[.]com</td>
<td>hol[.]es</td>
</tr>
<tr>
<td>Mail</td>
<td>Daum</td>
<td>manager-alert[.]com</td>
<td>esy[.]es</td>
</tr>
<tr>
<td>Manage</td>
<td>Kakao</td>
<td>org-view[.]work</td>
<td>*[.]work</td>
</tr>
<tr>
<td>Member</td>
<td>Naver</td>
<td>doc-view[.]work</td>
<td>atwebpages[.]com</td>
</tr>
<tr>
<td>Secure</td>
<td>NTT Docomo</td>
<td>account-protect[.]work</td>
<td>mygamesonline[.]org</td>
</tr>
<tr>
<td>User</td>
<td>OHCHR</td>
<td>com-sslnet[.]work</td>
<td>myartsonline[.]com</td>
</tr>
</tbody>
</table>

Recent examples:

- user[.]mail-help[.]com
- ohchr[.]org-view[.]work
- ramble[.]myartsonline[.]com
Black Banshee: campaigns
Kitty Phishing
Kabar Cobra

Operation WildCommand

Wild Command

WildCommand

Gold Dragon

AppleSeed campaign

Gold Dragon

GoldDragon campaign

FlowerPower activity

BabyShark campaign

Smoke Screen campaign

Winter Interests

(ANSSI) Credentials Gathering campaign

Focus on Japanese, South Korean Internet providers

Autumn Aperture campaign

BabyShark campaign

Operation WildCommand

BabyShark campaign

Autumn Aperture campaign

Smoke Screen campaign

Winter Interests

(ANSSI) Credentials Gathering campaign

Focus on Japanese, South Korean Internet providers
To catch a Banshee
PwC UK

Targeting

- Credential theft campaigns
- Espionage campaigns
- Financial services targeting
From our visibility & collection, Black Banshee has focused mostly on:

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

Strategic targets (sanctions; THAAD deployment issues)

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.
Thank you
PwC public reporting on Black Banshee


To catch a Banshee  
PwC UK

---

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 our previous blog, 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


References


References


