VOL. 12, NO. 12, JUNE 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

NETWORK DETECTION OF RANSOMWARE DELIVERED BY EXPLOIT KIT

Pratyush Raunak and Prabhakar Krishnan
Amrita Center for Cybersecurity Systems and Networks Amrita School of Engineering, Amritapuri Amrita Vishwa Vidyapeetham
Amrita University, India
E-Mail: kprabhakar@am.amrita.edu

ABSTRACT

Ransomware is an emerging cyber threat having a clear intention of money making in the form of ransom. This timeits not a virus or a root-kit but its a whole bunch of malware targeting innocent users for financial gain. The main motive behind such attacks is to directly or indirectly drain out the money from the victims. Ransomware is one of the popular malware today which turns out to be the most advanced of its class. More than 60% of the Ransomware gets into the system through drive-by downloads. The format of the drive-by download has changed drastically in the last few years. What was disorganised has now evolved as a sophisticated source of distributing Ransomware. We are now in the era where drive-by downloads are mostly controlled by Exploit Kits aka EK. Depending upon the vulnerabilities, the control panel of the Exploit Kit will choose a malware for you. In this paper, we have analysed the droppers, Cerber and Crypt XXX Ransomware which was distributed by Rig Ek during the year 2016-17. We have also intercepted and dissected around 10 different variants of Rig EK communication and reverse engineered its working methodology. At the end, we have proposed a framework for the detection of malicious communication and prevention of the user data, from being encrypted by using a combination of Software Defined Networking and Certificate Authority Checker aka CAC respectively.

Keywords: ransomware, exploit kit, software defined networking, certificate authority checker.

INTRODUCTION

Detection and Mitigation of Ransomware are becoming more complicated because of secure coding practices and anonymity being taken care of by the authors of the malware. Today, most of the Ransomware are dropped using Exploit Kit which uses layers of abstraction/obfuscation techniques to make it difficult for the security expert to figure out the actual working of these Exploit Kits. Most of the Ransomware dropped by the EK uses steganography techniques to hide the actual payload from the plain sight of the victim (eg. CerberRansomware). The authors of most Exploit Kits use Product as a Service (PaaS) as their business model. This model is also sometimes called as EK as a Service (EKaaS).

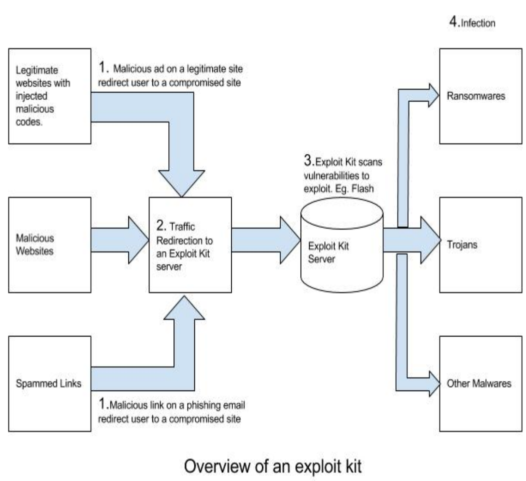

Figure-1. Overview of an exploit kit.

EKs are sold in the underground market, where the rental price for most sophisticated EK is often from a few hundred to few thousand dollars per month. The EK owner provides the buyer with a control panel console to manage the rented EK servers, but the buyer must provide an attack model. A distinct attack model combined with the EK is considered as a campaign. Rig Ek is the most wanted of them all after Angler Ek demise in 2016. Rig took over from Neutrino when the latter fleetingly succeeded to Angler from June to September 2016. RIG has dominated the exploit kit topography as seen in Figure-2, thanks to major distribution campaigns from compromised websites and malvertising.

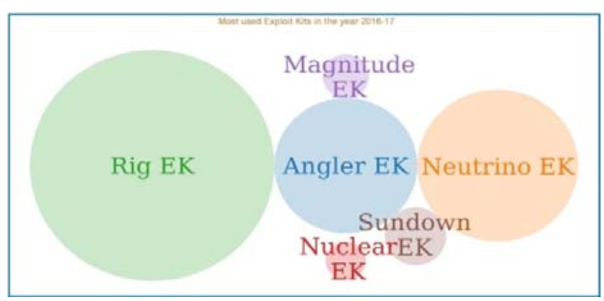

Figure-2. Most used exploit kit in the year 2016-17.

From the above illustration, we can say that Rig EK is one of the most favourite exploit kit among adversaries. Detection of exploit kits and its payload poses a great challenge for the cyber security community. There are three different versions of Rig Ek, prominent in past one year:

ARPN Journal of Engineering and Applied Sciences

- Rig-V EK - Rig-V is the VIP version of the regular Rig EK which started to show its-presence in late August and early September 2016 and showed similar patterns like Neutrino. Rig-V is distributed mostly via two campaigns, the Afraidgate and pseudo-Darkleech campaigns.
- Rig-E Ek - this version is called as the Empire Pack of Rig EK and slightly different from its brothers by the original URL patterns.
- Rig Ek - The standard version of Rig Ek. The drive-by downloads force the RIG Exploit Kit to infect systems by dropping a newer variant of Locky Ransomware (Odin).

One can question on what is the use of exploit kit on distribution of Ransomware and other trojans is because today's campaigns are distributing malwares based on geographical location and OS settings and less regular Ransomware. Here, the TDS or Traffic Distributing System comes into the picture. The TDS feature allows the operator of exploit kit to attach more than one payloads to a new thread. It is actually a key feature to a payload seller. This document is a template. An electronic copy cans be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

Furthermore, the payload is made to adapt based on the geo-location and OS settings of the target. However, there is one condition put up by the seller that the customers must create at least one Exploit Kit thread per payload, using an external TDS like Sutra/BlackHat TDS and from that TDS, target the traffic to the correct Exploit Kit thread or, can ask the provider of the traffic (if customer has bought the traffic) where to send the traffic for each country that is being targeted.

Given this notable growth of Ransomware attacks using exploit kit, it is very important to develop a detection mechanism against this type of malware. However, designing effective defence mechanisms is near to impossible without having an intuitive understanding of these attack vectors.Currently, security reports mainly focus on the advancements in ransomware attacks and their increasing sophistication, rather than coming up with a solid defence technique that should be adopted against this threat. In this paper, we analysed the behaviour of Ransomware as a dropper along with Rig exploit kit analysis with network indicators such that we can propose effective detection/mitigation mechanisms leveraging our findings.

Rig EK framework

The following analysis focuses on a drive-by download campaign observed and researched from jan-2016 till the date of writing this paper. It forces the Rig exploit kit to infect systems and drop Cerber, Crypt XXX, Qakbotmalware.

User visits a compromised but legitimate website:

- Malicious ad in the form of iFrame redirects user to another compromised website.
- Another redirect lure the user to land onto a Rig exploit kit.
- Rig Exploit kit scans the browser for security loop-holes.
- Rig exploit kit exploits the vulnerability and based on that vulnerability drops a malware into the system.

The diagram below shows the various components of the Rig exploit kit and how they communicate with each other.

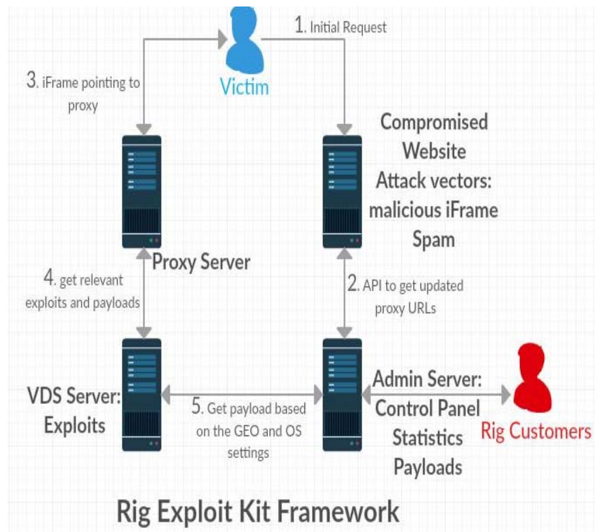

Figure-3. Rig exploit kit framework.

Based on the incident reported of potential malware attacks, here is the timeline, ranging from 2016-17, of incidents where Rig-V EK was used to send Ransomwares.

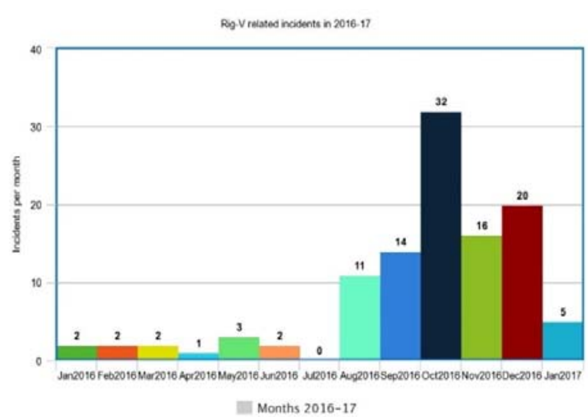

Figure-4. Rig V related incidents.

Analysis

Environmental Setup- In this paper, we have done both, Static and Dynamicanalysis of the Rig EK as well as its corresponding droppers. The initial environmental setup includes:

- One Linux machine with two VMs running windows and Security Onion respectively. All the malware samples were brought using USB key with write protected feature.
- VM running Windows OS is the test bed where all the analysis was done. While on another VM Security Onion is, running and listening to eth0.
- For detailed analysis, a fake DNS server is used to lure the malware to talk to this and make the communication function successful.
- Fiddler session is used to analyze the full infection cycle.
- A bunch of tools like File system and registry monitoring tool, Process monitoring, Network monitoring and change detection tools were used for better understanding of the methodology of the malware and its communication.
- For code analysis we used IDA Pro.
- For DE obfuscation of flash files (.swf) and to analyse the Action Script we used flash decompiler tool called FFDec and Flare.
- At last we followed the cheat sheet for reverse engineering the malware [9] and analysing malicious document [10].
- The Ransomware samples were taken from [11, 12] and mostly by visiting compromised website.

There has been no change in Rigs working to lure the users to Rig exploit kit through malvertising and compromised sites, what we have seen in the past. Compromised sites usually contain an Iframe which leads to Rig EK. The Iframe is in the page header that loads the Rig proxy domains which also contains an Iframe which leads to the RIG landing page. The full infection cycle is shown in the below Figure.

#	Comments	Result	Prot...	Host	URL	Body	C...	Content-...	Method
1	Compromised Site	200	HTTP	www.southcoast...	/	36,013	no...	text/html;...	GET
2	Child Request	200	HTTP	realstatistics.info	/js/analytic.php?id=4	794		text/html	GET
3	Child Request	200	HTTP	realstatistics.info	//js/analytic.php?id=4&tz=9&rs=13...	383		text/html	GET
4	Rig Landing Page	200	HTTP	df.jerseyalmana...	/?wX6OcbieKhvGCYQ=l3SKfPrfJxzF...	2,185		text/html	GET
5		200	HTTP	Tunnel to	199.59.149.233:443	475			CONNECT
6		200	HTTP	Tunnel to	199.59.149.233:443	475			CONNECT
7	Rig Flash Exploit	200	HTTP	df.jerseyalmana...	/index.php?wX6OcbieKhvGCYQ=l3...	24,439		applicatio...	GET
8		0	HTTP	df.jerseyalmana...	/index.php?wX6OcbieKhvGCYQ=l3...	0			GET
9	Rig Encrypted binary(Exploit Succes)	200	HTTP	df.jerseyalmana...	/index.php?wX6OcbieKhvGCYQ=l3...	2,04...		applicatio...	GET
10		200	HTTP	ipinfo.io	/json	203		application...	GET
11	Ip Check	404	HTTP	www.doswf.com	/copyright/files/c.c	56		text/html	GET

Figure-5. Fiddler session.

The second run through the same infection cycle gives the below result.

#	Comments	Result	Prot...	Host	URL	Body	Conte...	Method
1	Compromised Site	200	HTTP	www.southco...	/	36,013	text/h...	GET
2	Child Request	200	HTTP	realstatistics....	/js/analytic.php?id=4	794	text/html	GET
3	Child Request	200	HTTP	realstatistics....	//js/analytic.php?id=4...	389	text/html	GET
4	Rig Landing Page	200	HTTP	jy.infogiovan...	/?xHiNdbSeLhzHC4U=...	3,071	text/html	GET
5	Flash Exploit 1	200	HTTP	jy.infogiovan...	/index.php?xHiNdbSe...	24,439	applica...	GET
6	Flash Exploit 2	200	HTTP	jy.infogiovan...	/index.php?xHiNdbSe...	24,439	applica...	GET
7	Rig Encrypted Binary(Exploit Success)	200	HTTP	jy.infogiovan...	/index.php?xHiNdbSe...	6,31,072	applica...	GET
8	Ip Check	200	HTTP	ipinfo.io	/json	217	applica...	GET
9	Obfuscation tool	404	HTTP	www.doswf.com	/copyright/files/c.c	56	text/html	GET
10		302	HTTP	cerberhhyed5...	/3AC6-9E8A-C2A4-021...	20	text/h...	GET
11	GET request after the payload was sent	200	HTTP	cerberhhyed5...	/3AC6-9E8A-C2A4-021...	1,549	text/h...	GET

Figure-6. Fiddler session with different results.

The infection starts the moment victim browse a compromised website. The compromised website replies with a HTTP response. The most interesting aspect of Rig EK is that the actual payload is obtained in a distinct GET request. In the usual behaviour of malware communication, the exploit kit is tunneled or as an obfuscated payload in the HTTP packets. But in this case of Rig EK, the payload consists of distinct GET request, which is the malware executable in the byte stream. Like any other exploit kit, RIG EK compromises the user by redirecting the HTTP browser to another landing page hosted on the attacker's website or CC server. This redirection with malign intent is usually done through smart malvertising or malicious iFrames. The redirection link points to a javascript such as:

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://www.google.com/url?
sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj4qoG1kMbNAhUr6IMKHXzfBW0QFggcMAA&url=http%3A%2F
%2Fwww.southcoastdrones.com.au%2F&usg=AFQjCNHia0-yK9kF5H0Qa-OcFRIdqFbZjw&bvm=bv.125596728,d.amc
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.southcoastdrones.com.au
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sun, 26 Jun 2016 16:37:40 GMT
Server: Apache/2.2.31 (Unix) mod_ssl/2.2.31 OpenSSL/1.0.1e-fips mod_bwlimited/1.4
X-Powered-By: PHP/5.4.45
Expires: Mon, 1 Jan 2001 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: 93925714efd11d81a9c4bc96fcf2195b=c46dd0b2443b5e9f545972e4770ac2af; path=/; HttpOnly
Last-Modified: Sun, 26 Jun 2016 16:37:41 GMT
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

8ca0

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en-gb" lang="en-gb" dir="ltr">
<head>

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

      <base href="http://www.southcoastdrones.com.au/" />
  <meta http-equiv="content-type" content="text/html; charset=utf-8" />
  <meta name="author" content="Administrator" />
  <meta name="description" content="South Coast Drones" />
  <meta name="generator" content="Joomla! - Open Source Content Management" />
  <title>South Coast Drones Home</title>
  <link href="http://www.southcoastdrones.com.au/index.php" rel="canonical" />
  <link href="/templates/ice_future/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />
```

Figure-7. Javascript redirection link.

Then the user request is redirected to receive this:

```
GET //js/analytic.php?id=4&tz=8&rs=1366x768 HTTP/1.1
Accept: application/javascript, */*;q=0.8
Referer: http://www.southcoastdrones.com.au/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: realstatistics.info
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sun, 26 Jun 2016 16:37:41 GMT
Server: Apache/2.2.27 (Unix) mod_ssl/2.2.27 OpenSSL/1.0.1e-fips
X-Powered-By: PHP/5.4.45
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

179
document.write("<div style='width: 300px; height: 300px; position: absolute; left:-500px; top: -500px;'><iframe
src='http://jy.INFOGIOVANINEBRODI.INFO/?xHiNdbSeLhzHC4U=l3SKfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqk10vHjUnH1cmQ9laHYghP7cOSFuA73ln0mbNFIp0mlUSK4DIGzrkVU10W5AwS
z_ie8KqE' width='250' height='250'></iframe></div>");
0
```

Figure-8. Iframe which receives the landing page.

The above HTML page shows a simple iframe which retrieves the landing page from the attacker's website. The HTTP request for the landing page can be like this:

Figure-9. Landing page request.

When the malware script on the user HTTP browser retrieves the landing page, it is usually highly obfuscated with high randomness and not follows the usual grammar or normal English language-based text we can see in other exploit kits. The following HTML page is displayed as the landing page:

Figure-10. Obfuscated landing page.

RIG EK does the following actions: First it probes the HTML browser and then delivers the EK with malicious payload to the end user. This figure shows the exploit in the flash player delivered by RIG EK:

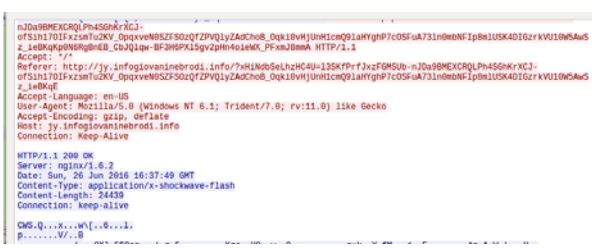

Figure-11. Flash exploit.

As mentioned earlier that Rig exploit kit payload is not delivered together with the exploit as it happens in the case of many exploit kits like Neutrino but in this case a separate GET request contains the actual payload:

Figure-12. Separate GET Request with actual payload.

The naming convention for the malicious executables delivered by Rig EK as payloads are designed to be not-suspicious to the users, because the filenames closely resemble the system executables. For example, in the case of Rig EK exploiting a Windows system, the naming conventions are: systemrestore.exe, defrag.exe, dissdkchk.exe. These malicious programs may not raise a warning flag as these names looks similar to that of system management services like ’defrag’ or ’diskchk’ or sytem restore in a windows system. These malicious programs are dropped into the following path: % APPDATA %/TEMP folders instead of SYSTEM32 folder.

CONCLUSIONS

The presented experimental analysis and results suggest that preventing such advanced Ransomware attacks delivered through popular exploit kits, is not as complex. In this paper, we presented our behavioural analysis of variants of network directed Ransomware, delivered through network and we also proved the accuracy of our detection approach by conducting combination of both dynamic and static analysis on a large data set samples.

Our run-time malware detection system when deployed in the network utilizes traffic patterns of Ransomware communication, key network indicators of exploit kits and signatures of Ransomware families and combines with the pro-file data from the host or end-points and generates actionable rules and alerts to an Software-Defined-Networking (SDN) based IDS/IPS system, which facilitates timely response to the threats. Evaluations on various simulation of live Ransomware attacks in our Ransomware infrastructure, exploit kits and tools and data set crowd sourced from external victims, prove that our hybrid approach is more efficient with reasonable performance overhead, less false-positives, high accuracy than the standalone network IDS or host-based end-point detection mechanisms. Our future work will address how our defence architecture can be used in an operational setting for risk-based incident response system.

REFERENCES

[1] K. Savage, P. Coogan, and H. Lau, “The evolution of ransomware,” Symantec, Mountain View, 2015.

[2] A. PaSeshagiri, Vazhayil and P. Sriram, “Ama: Static code analysis of web page for the detection of malicious scripts,” Procedia Computer Science, 2016.

[3] T. Yang, Y. Yang, K. Qian, D. C.-T. Lo, Y. Qian, and L. Tao, “Automated detection and analysis for android ransomware,” in High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conference on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on. IEEE, 2015, pp. 1338-1343.

[4] A. Gazet, “Comparative analysis of various ransomwarevirii,” Journal in computer virology, vol. 6, no. 1, pp. 77-90, 2010.

[5] K. Cabaj, P. Gawkowski, K. Grochowski, and D. Osojca, “Network activity analysis of cryptowallransomware,” Przeglad Elektrotechniczny, vol. 91, no. 11, pp. 201-204, 2015.

[6] S. Patton, W. Yurcik, and D. Doss, “An achilles heel in signature-based ids: Squealing false positives in snort,” in Proceedings of RAID, vol. 2001. Citeseer, 2001.

[7] S. L. Harrington, “Cyber security active defense: Playing with fire or sound risk management?” Rich. JL& Tech., vol. 20, pp. 12-14, 2014.

[8] P. Pathak and Y. M. Nanded, “A dangerous trend of cybercrime: Ransomware growing challenge,” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 5, no. 2, 2016.

[9] Scott-Hayward, Sandra, Gemma O'Callaghan, and SakirSezer. "SDN security: A survey." Future Networks and Services (SDN4FNS), 2013 IEEE SDN For. IEEE, 2013.

[10] A. A. Acharya and K. Arpitha, “An intrusion detection system against udp flood attack and ping of death attack (ddos) in manet.”