Exploit Kit still sharpens a sword

nao-sec.org/2021/04/exploit-kit-still-sharpens-a-sword.html

2021-04-15
Note: This blog post doesn't make sense to many

It's 2021 now. Moreover, the quarter has already passed. I thought Drive-by Download attack was dead four years ago. Angler Exploit Kit has disappeared, pseudo-Darkleech and EITest campaign have disappeared, and RIG Exploit Kit has also declined. At that time, Drive-by

Download attack was definitely supposed to die. However, even if in 2021, it will not disappear fire still slightly.

In April 2021, I received some incredible notices. For example, there are the following notifications.

- PurpleFox Exploit Kit has started exploiting CVE-2021-26411
- RIG Exploit Kit has started exploiting CVE-2021-26411
- Bottle Exploit Kit is back, and has started exploiting CVE-2020-1380 and CVE-2021-26411
- Underminer Exploit Kit is back

Repeat again. It's 2021 now. Not 2017. Internet Explorer was taken away by Chrome and Edge, and Drive-by Download attack was supposed to die. Why are there still Drive-by Download attacks? Here are some reasons, including the opinions of your friends.

1. Internet Explorer is still used in some countries/regions including Japan
2. Due to the influence of corona, remote work has increased, and the number of users with network security vulnerabilities has increased
3. Internet Explorer vulnerabilities still discovered and exploit code published

In reality, these are intricately intertwined, and there may be different reasons.

In any case, Drive-by Download attacks are still being observed. Moreover, it is a little more active. This is irrelevant for most people. Because most people don't use Internet Explorer. If you don't use Internet Explorer, a typical Exploit Kit attack is not a threat. A small number of targeted attacks may use Chrome's 0day, which is not discussed here.

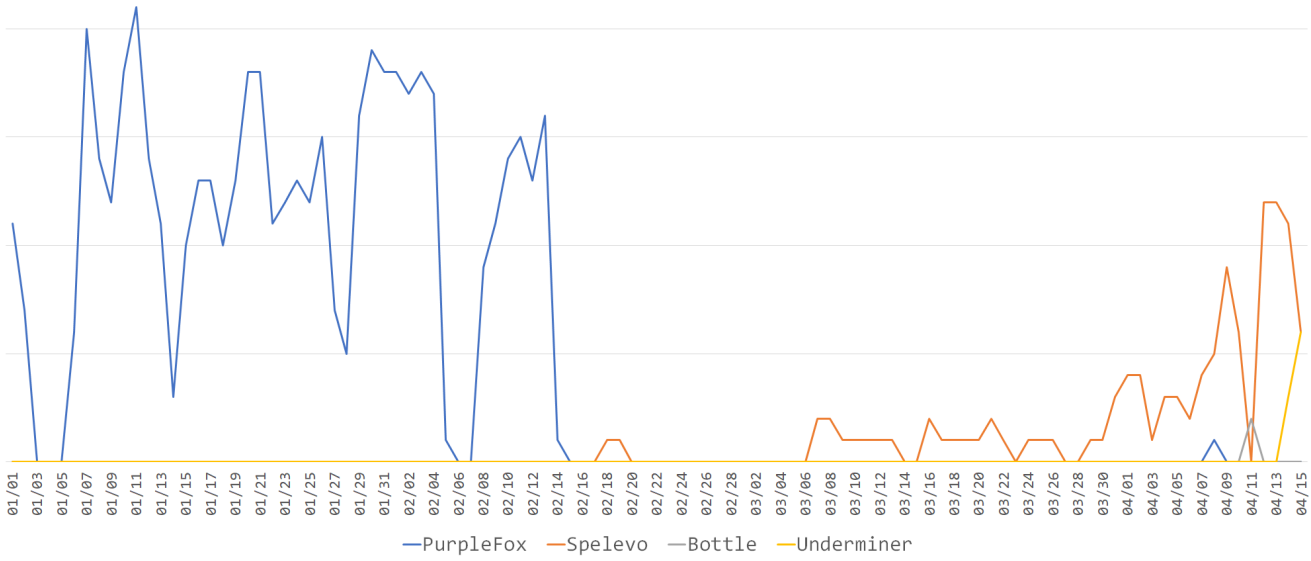
For the few enthusiastic Internet Explorer users that exist, I write this blog post. In other words, as of April 2021, I will introduce the characteristics of common Drive-by Download attacks that you may encounter. Thanks to my friends (@jeromesegura, @nao_sec members) for helping me write this blog post.

Exploit Kit Landscape

As of April 2021, the following 6 types of Exploit Kits have been observed to be active.

- RIG
- Spelevo
- PurpleFox
- Underminer
- Bottle
- Magnitude

nao_sec has been running a fully automatic Drive-by Download attack observation environment called Augma System[1] for three years. The data observed by this is as follows. Some Exploit Kits are not counted because they are observed in different environments.



The features of the 6 types of Exploit Kits currently observed are as follows.

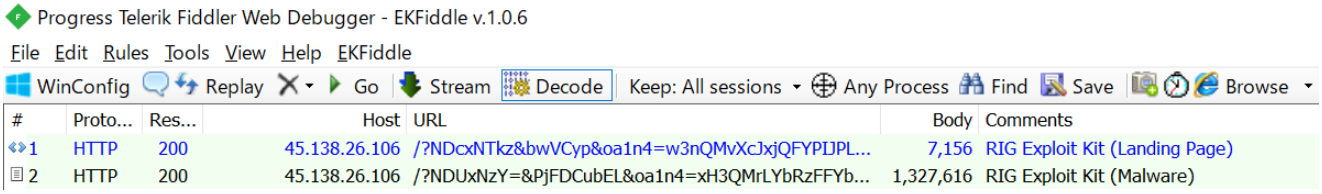
	Private	Update	Exploit
RIG	No	Yes	CVE-2020-0674, CVE-2021-26411
Spelevo	No	No	CVE-2018-8174, CVE-2018-15982
PurpleFox	Yes	Yes	CVE-2021-26411
Underminer	Yes	No	CVE-2018-15982
Bottle	Yes	Yes	CVE-2020-1380, CVE-2021-26411
Magnitude	Yes	Yes	CVE-2021-26411

Here is sample traffic for each.

RIG Exploit Kit

RIG is an Exploit Kit that has been active since around 2014. It was extremely active from 2016 to 2017, but then declined with the advent of Fallout and others. However, it is still active in 2021.

RIG started abusing CVE-2021-26411 in April 2021 and are still incorporating changes. Landing Pages are not obfuscated as they used to be. Very simple code. The malware is RC4 encrypted.



#	Proto...	Res...	Host	URL	Body	Comments
1	HTTP	200	45.138.26.106	/?NDcxNTkz&bwVCyp&oa1n4=w3nQMvXcJxjQFYPIJPL...	7,156	RIG Exploit Kit (Landing Page)
2	HTTP	200	45.138.26.106	/?NDUxNzY=&PjFDCubEL&oa1n4=xH3QMrLYbRzFFYb...	1,327,616	RIG Exploit Kit (Malware)

Download sample traffic here.

Spelevo Exploit Kit

Spelevo is an Exploit Kit that appeared in 2019. 2020 was very mature, but 2021 is one of the most active Exploit Kits.

Spelevo hasn't changed for a long time. Spelevo hides the malware in the image. See this article[2] for detailed behavior.

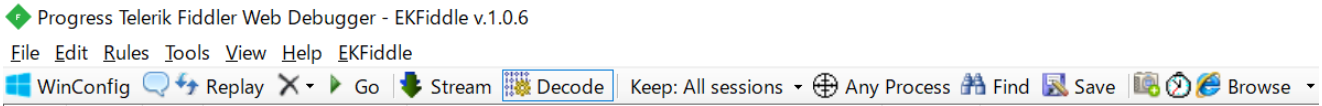
#	Proto...	Res...	Host	URL	Body	Comments
1	HTTP	200	charlotte.bavywoums...	/36dbsk72ci0uh/duckie-jon-pegging	39,705	Spelevo Exploit Kit (Landing Page)
2	HTTP	200	charlotte.bavywoums...	/36dbsk72ci0uh/?e3569687670bd29563efaa7affe97e5...	1,907	Spelevo Exploit Kit (SWF Loader)
3	HTTP	200	charlotte.bavywoums...	/36dbsk72ci0uh/?c08b54157fea29403a3cem	22,035	Spelevo Exploit Kit (SWF Exploit)
4	HTTP	200	charlotte.bavywoums...	/36dbsk72ci0uh/?c08b54157fee	167,686	Spelevo Exploit Kit (Maware)
5	HTTP	404	charlotte.bavywoums...	/36dbsk72ci0uh/?c08b54157fee&00000111&11	259	Spelevo Exploit Kit (Checker)

Download sample traffic here.

PurpleFox Exploit Kit

PurpleFox is an Exploit Kit that has been active since 2019. A private exploit kit for sending PurpleFox malware. It's enthusiastic about exploit and is fairly fast at incorporating new vulnerabilities.

Spelevo has started to exploit CVE-2021-26411 in April 2021. However, the other parts have not changed for a long time.



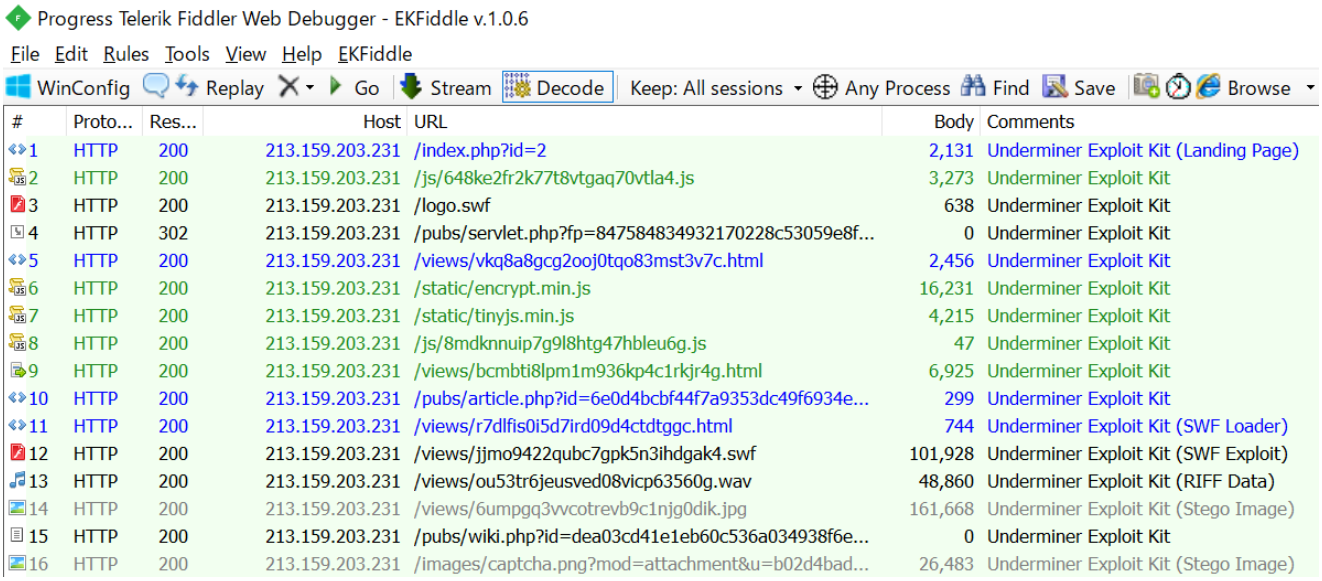
#	Proto...	Res...	Host	URL	Body	Comments
1	HTTPS	200	jolly-frost-a95b.yeakr...	/in.php?key=FEC82D2FEA01F09F&id=2&netid=AC5C9...	19,369	PurpleFox Exploit Kit (Landing Page)
2	HTTPS	200	jolly-frost-a95b.yeakr...	/crypto-js.min.js	16,761	PurpleFox Exploit Kit
3	HTTPS	200	jolly-frost-a95b.yeakr...	/zepto.min.js	9,794	PurpleFox Exploit Kit
4	HTTPS	200	jolly-frost-a95b.yeakr...	/aes.min.js	1,098	PurpleFox Exploit Kit
5	HTTPS	200	rawcdn.githack.net	/up.php?key=5	66,742	PurpleFox Exploit Kit (PowerShell)
6	HTTPS	200	rawcdn.githack.net	/up.php?key=6	1,019,904	PurpleFox Exploit Kit (Malware-1)
7	HTTPS	200	rawcdn.githack.net	/M0021.cab	2,600,942	PurpleFox Exploit Kit (Malware-2)

Download sample traffic here.

Underminer Exploit Kit

Underminer is an Exploit Kit that appeared in 2018. It's a pretty distinctive Exploit Kit. It is known to be extremely difficult to analyze. It is used to deliver its unique malware called Hidden Bee. See this article[3] for more details.

Underminer has a cycle of activity for several months and then silence for several months. It has been silent since the November 2020, but was revived in April 2021. But the essence hasn't changed at all.



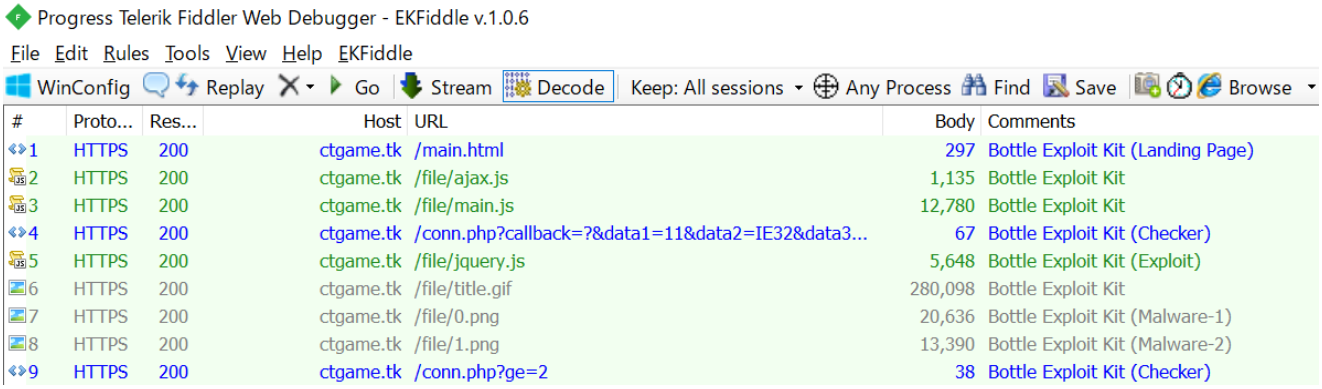
#	Proto...	Res...	Host	URL	Body	Comments
1	HTTP	200	213.159.203.231	/index.php?id=2	2,131	Underminer Exploit Kit (Landing Page)
2	HTTP	200	213.159.203.231	/js/648ke2fr2k77t8vtgaq70vtla4.js	3,273	Underminer Exploit Kit
3	HTTP	200	213.159.203.231	/logo.swf	638	Underminer Exploit Kit
4	HTTP	302	213.159.203.231	/pubs/servlet.php?fp=847584834932170228c53059e8f...	0	Underminer Exploit Kit
5	HTTP	200	213.159.203.231	/views/vkq8a8gcg2ooj0tqo83mst3v7c.html	2,456	Underminer Exploit Kit
6	HTTP	200	213.159.203.231	/static/encrypt.min.js	16,231	Underminer Exploit Kit
7	HTTP	200	213.159.203.231	/static/tinyjs.min.js	4,215	Underminer Exploit Kit
8	HTTP	200	213.159.203.231	/js/8mdknnuip7g9l8htg47hbleu6g.js	47	Underminer Exploit Kit
9	HTTP	200	213.159.203.231	/views/bcmbti8lpm1m936kp4c1rkjr4g.html	6,925	Underminer Exploit Kit
10	HTTP	200	213.159.203.231	/pubs/article.php?id=6e0d4bcbf44f7a9353dc49f6934e...	299	Underminer Exploit Kit
11	HTTP	200	213.159.203.231	/views/r7dlfis0i5d7ird09d4ctdtggc.html	744	Underminer Exploit Kit (SWF Loader)
12	HTTP	200	213.159.203.231	/views/jjmo9422qubc7gpk5n3ihdgak4.swf	101,928	Underminer Exploit Kit (SWF Exploit)
13	HTTP	200	213.159.203.231	/views/ou53tr6jeusved08vicp63560g.wav	48,860	Underminer Exploit Kit (RIFF Data)
14	HTTP	200	213.159.203.231	/views/6umpgq3vvcotrevb9c1njg0dik.jpg	161,668	Underminer Exploit Kit (Stego Image)
15	HTTP	200	213.159.203.231	/pubs/wiki.php?id=dea03cd41e1eb60c536a034938f6e...	0	Underminer Exploit Kit
16	HTTP	200	213.159.203.231	/images/captcha.png?mod=attachment&u=b02d4bad...	26,483	Underminer Exploit Kit (Stego Image)

Download sample traffic here.

Bottle Exploit Kit

Bottle is an Exploit Kit that appeared in 2019. An extremely rare Exploit Kit that targets only Japan. It is used to deliver its unique malware called Cinobi.

It is one of the most active Exploit Kits in Japan. It has not been observed since November 2020, but it was revived in April 2021. It's also worth noting that unlike other Exploit Kits, it exploits CVE-2020-1380 and CVE-2021-26411. It has been pointed out that it is related to MageCart and phishing campaigns. See this article[4] for more details.



Download sample traffic here.

Magnitude Exploit Kit

Magnitude is one of the oldest existing Exploit Kits. It has been observed only in certain countries/regions such as South Korea and Taiwan, and the details have not been reported much.

Its activity was also reported in April 2021. It exploits CVE-2021-26411 and is still actively evolving.

> One more: #MagnitudeEK pic.twitter.com/pOuIZzAPZG
>
> — Jérôme Segura (@jeromesegura) April 14, 2021

Finally

Drive-by Download attacks are still observed in 2021. It has nothing to do with most people. As with Adobe Flash Player, stop using Internet Explorer immediately. That is the simplest solution. Drive-by Download attacks continue to exist with Internet Explorer.

References

[1] https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-KoikeChubachi.pdf
[2] https://insight-jp.nttsecurity.com/post/102gsqj/pseudogatespelevo-exploit-kit
[3] https://blog.malwarebytes.com/threat-analysis/2019/08/the-hidden-bee-infection-chain-part-1-the-stegano-pack/
[4] http://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_103_koike-takai_jp.pdf