SEPTEMBER 2017

virus BULLETIN

Covering the global threat landscape

VBWEB COMPARATIVE REVIEW SUMMER 2017

Martijn Grooten & Adrian Luca

When we think of malware spreading via the web, it is tempting to imagine an executable sitting on a rogue (or compromised) server that gets downloaded via a web browser and then run on the local machine. While this scenario does happen, there is a far more subtle way in which malware can make it onto one's device during a browsing session: exploit kits.

Exploit kits have been a threat for several years, and though recently in decline, they remain an infection vector that is not to be ignored. Other than the fact that they often don't require any user interaction, exploit kits often execute malware on the local machine without a malicious executable being downloaded in the browser, thus making detection difficult.

While keeping your software up to date remains the first and most important step you should take to avoid being infected via an exploit kit, it is good to know that security solutions are able to block such activity, even if you (or your employees) are behind schedule on patching. Indeed, this report once again shows that there are solutions that provide excellent protection against today's web threats.

MULTIPLE SOLUTIONS TO THE SAME THREAT

During August 2017, a number of web security products were run in *Virus Bulletin*'s test lab and exposed to various real-time, web-based threats, including exploit kits and direct malware downloads. *Virus Bulletin* applies the same rule to all of its tests: each participating vendor must decide prior to the start of the test whether they want the results of the test to be made public, or whether they want to keep the results private, for internal use as quality assurance. In this test two vendors opted to go public with their results, while another four were tested privately.

The products blocked between 90 and 100 per cent of exploit kits, and between 87 and 99 per cent of direct malware downloads. While this shows what a great job products are doing of blocking malware, the details show that there are

Time	Protocol	Method	Result	Host	URL	Body	Content-Type	Comments
27/07/2017 13:30:48	HTTP	GET	200	194.58.58.70	/signup1.php	324	text/html	RIG_EK_injection_url
27/07/2017 13:30:49	HTTP	GET	200	188.225.33.135	/?MTAyNzE0NzIx&rand=xX_QMvWdbRXQC53EKvncT6NEMVHRH0CL2YydmrHQefjaelWkzrHFTF_xozKASAS…	122,434	text/html;charset=UTF-8	RIG_EK_URL (Landing Page)
27/07/2017 13:30:55	HTTP	GET	200	188.225.33.135	/?MTE5MDU2MjQw&elsa=QXnjBaAKQdpItcVFoW9a-r2kDczkSeh8GB_xeFYAhHqceXFeA92Qv9xrAkc80lwh…	15,933	application/x-shockwa…	RIG_EK_URL (Flash Exploit)
27/07/2017 13:31:22	HTTP	GET	200	188.225.33.135	/?OTY0MTkzNzM=&rand=xHzQMrPYbR3FFYPfKPrEUKREMU7WA0SKwYyZhazVF5yxFDTGpbL1FxzspVydCF-…	262,144	application/x-msdownl…	RIG_EK_URL (Malware Payload)
Time	Protocol	Method	Result	Host	URL	Body	Content-Type	Comments
29/07/2017 14:34:31	HTTP	GET	200	www.pro-redirect.ru	/hl	655	text/html; charset=utf-8	RIG_EK_injection_url (Landing Pag
29/07/2017 14:34:32	HTTP	GET	200	188.225.74.3	/?OTg1MTYyNDY=&rand=xX_QMvWdbRXQC53EKvncT6NHMVHRH0CL2Y-dmrHTefjaelWkzrHFTF_yozKASw…	122,390	text/html;charset=UTF-8	RIG_EK_URL (Landing Page)
29/07/2017 14:34:39	HTTP	GET	200	188.225.74.3	/?ODgxMTMzODg=&elsa=vpjBPVcgQwnNtcBFkb9aGoj0DTyB-egJLX_0CNYAtN-paXE7M82VjyzrMkdssmxxO…	13,740	application/x-shockwave-flash	RIG_EK_URL (Flash Exploit)
29/07/2017 14:34:48	HTTP	GET	200	188.225.74.3	/?OTY0OTU4MDQ=&info=MjY5MjI1NTc=&rand=xXzQMvWebRXQCJ3EKvncT6NHMVHRH0CL2YydmrHTefja…	205,824	application/x-msdownload	RIG_EK_URL (Malware Payload)
Time	Protocol	Method	Result	Host	URL	Body	Content-Type	Comments
28/07/2017 14:26:03	HTTP	GET	200	www.casinoab.xyz	/	13,503	text/html; charset=UTF-8	Heur_Risky_Domains (Landing Pag
28/07/2017 14:26:13	HTTP	GET	200	212dljhkugj.tk	/moops/index.php?dd=32408874093	573	text/html; charset=UTF-8	RIG_EK_injection_url (Landing Pag
28/07/2017 14:26:18	HTTP	GET	200	188.225.38.131	/?ODAzNjk1OTM=&info=NTA5NDI2NTE=&elsa=RDQHijxGGcwQwm4hfAVgV9fyoiUPdmh-egsPR_x3YYAhG9…	122,437	text/html;charset=UTF-8	RIG_EK_URL (Landing Page)
28/07/2017 14:26:22	HTTP	GET	200	188.225.38.131	/?OTI1NTgwMTA=&rand=xHzQMrPYbR3FFYDfKPnEUKREMU3WA0eKwY-ZhazVF5-xFDfGpbH1FxzspV-dCF…	15,933	application/x-shockwave-flash	RIG_EK_URL (Flash Exploit)
28/07/2017 14:26:55	HTTP	GET	200	188.225.38.131	/?MTEyNDk2Nzk3&rand=xHzQMrDYbR3FFYPfKPnEUKREMU7WA0SKwY-Zha_VF5yxFDfGpbL1FxzspV-dCFy…	256,512	application/x-msdownload	RIG_EK_URL (Malware Payload)
Time	Protocol	Method	Result	Host	URL	Body	Content-Type	Comments
29/07/2017 00:57:16	HTTP	GET	200	www.iwankto.com	/?loc=284553	51,845	text/html	
29/07/2017 00:57:20	HTTP	GET	200	www.iwankto.com	/static/popunder.php	1,255	text/html	PopUnder_URL
29/07/2017 00:57:28	HTTP	GET	200	flements.info	/banners/countryhits	6,429	text/html; charset=utf-8	Banners_URL (Landing Page)
29/07/2017 00:57:32	HTTP	POST	200	188.225.74.233	/?OTQyNDcwNDU=&elsa=SwcyyIxaBFsQ9Kv4i0PWnRebg5XTrxSEMwhArZDHQrNujlykyLNCJMpxwxTU4iW…	122,356	text/html;charset=UTF-8	RIG_EK_URL (Landing Page)
29/07/2017 00:57:35	HTTP	GET	200	188.225.74.233	/?ODYzMzM3Mzk=&elsa=yyIxaBFgQ9Kj4i0PWnRSbg5XTrxSEMwhArZPHQrNujl-kyLBCJMpxwxTU4WMDyus…	13,470	application/x-shockwave-flash	RIG_EK_URL (Flash Exploit)
29/07/2017 00:57:57	HTTP	GET	200	188.225.74.233	/?MTA1NjkzMjI1&elsa=1jELWeAdiyotcUQ4U9ar_3EPcmxOd0sXU_0DbMAhCqcaXQrVt2lWmybAkdM0lzx6A6…	352,256	application/x-msdownload	RIG_EK_URL (Malware Payload)

RIG exploit kit traffic.

ISSN 1749-7027

differences between the products: a web security gateway can help a lot, but some can help a more than others.

THE WEB THREAT LANDSCAPE, SUMMER 2017

Though the web threat landscape remains volatile, on the face of it, not much has changed since spring: RIG remains by far the most prevalent exploit kit, with others either having disappeared or having become very localized threats. If you were infected through an exploit kit this year, it was most likely to have been RIG.

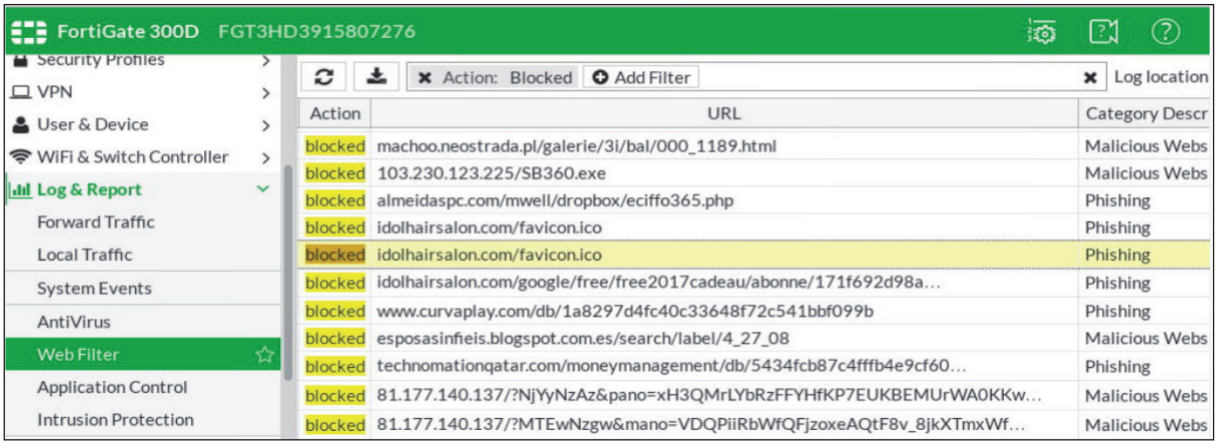
RIG uses various campaigns though, each with slightly different characteristics, thus making it far more than a single threat. This was also reflected in the variety of payloads we saw during the test period, which included various kinds of ransomware and other kinds of malware.

RESULTS

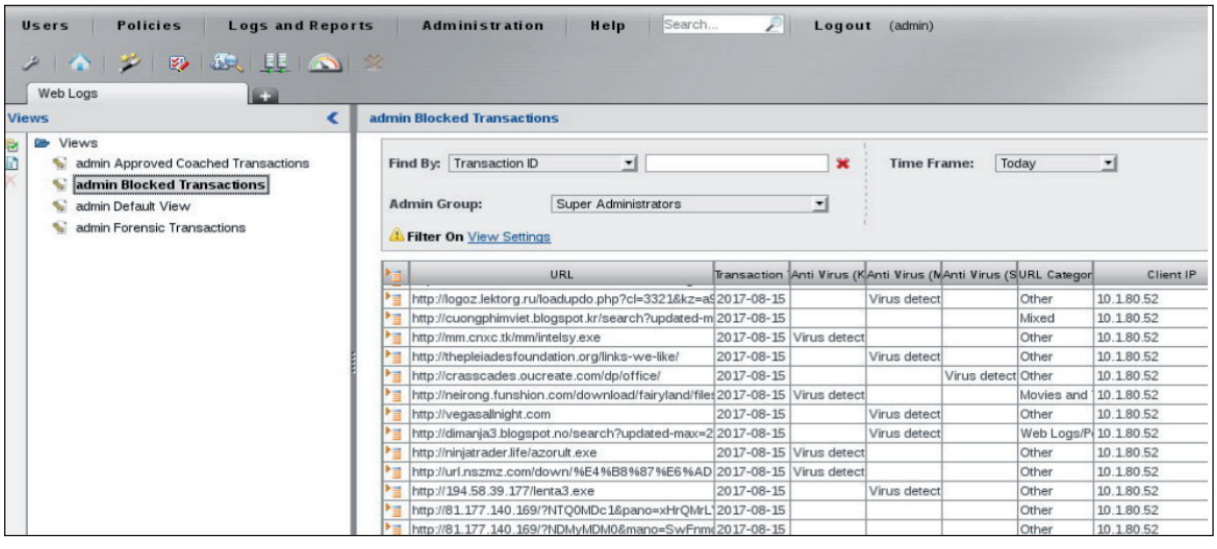
Fortinet FortiGate

Drive-by download rate: 100.0%
Malware block rate: 98.6%
Weighted average: 99.9%
Potentially malicious rate: 97.5%

Fortinet's *FortiGate* appliance blocked all of the more than 400 exploit kits seen in this test, demonstrating that the gateway product continues to provide an excellent first line



FortiGate interface.



Trustwave interface.

of defence. The detection rate of direct malware downloads was very good too, with only a handful missed.

Thus both for keeping up with the threat landscape and for the continued protection it offers, *Fortinet* is well deserving of another VBWeb award and we are pleased to recommend this product to organizations looking to mitigate web-based threats.

Trustwave Secure Web Gateway

Drive-by download rate: 100.0%
Malware block rate: 96.6%
Weighted average: 99.7%
Potentially malicious rate: 99.2%

Exploit kits remain no problem for *Trustwave*'s *Secure Web Gateway*: once again, not one was missed by the product, while more than 96% of direct malware downloads (where a web gateway is the first line of defence before an endpoint security product will try and block the threat) were blocked too. But besides the excellent performance in this test, it is the product's strong performance over several tests that its developers can be proud of.

As such, *Trustwave* fully deserves another VBWeb award and we are pleased to recommend this product to organizations looking to mitigate web-based threats.

APPENDIX: THE TEST METHODOLOGY

The test ran from 27 July to 15 August 2017, during which period we gathered a large number of URLs (most of which were found through public sources) which we had reason to believe could serve a malicious response. We opened the URLs in one of our test browsers, selected at random.

When our systems deemed the response sufficiently likely to fit one of various definitions of 'malicious', we made the same request in the same browser a number of times, each with one of the participating products in front of it. The traffic to the filters was replayed from our cache within seconds of the original request having been made, thus making it a fully real-time test.

We did not need to know at this point whether the response was actually malicious, thus our test didn't depend on malicious sites that were already known to the security community. During a review of the corpus some days later, we analysed the responses and discarded cases for which the traffic was not deemed malicious.

In this test, we checked products against 428 drive-by downloads (exploit kits) and 584 direct malware downloads.

To qualify for a VBWeb award, the weighted average catch rate of these two categories, with weights of 90% and 10% respectively, needed to be at least 70%.

We also checked the products against 241 URLs that we deemed 'potentially malicious'. These were URLs for which we had strong evidence that they would serve a malicious response in some cases, but they didn't when we requested it. There could be a number of reasons for this, from server-side randomness to our test lab being detected by anti-analysis tools.

While one can have a perfectly good web security product that doesn't block any of these, we believe that blocking such URLs can serve as an indication of a product's ability to block threats proactively without inspecting the traffic. For some customers this could be important, and for developers this is certainly valuable information, hence we decided to include it in this and future reports.

The test focused on unencrypted HTTP traffic. It did not look at extremely targeted attacks or possible vulnerabilities in the products themselves.

TEST MACHINES

Each request was made from a randomly selected virtual machine using one of the available browsers. The machines ran either *Windows XP Service Pack 3 Home Edition 2002* or *Windows 7 Service Pack 1 Ultimate 2009*, and all machines ran slightly out-of-date browsers and browser plug-ins.

Editor: Martijn Grooten

Head of Testing: Peter Karsai

Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Ionuț Răileanu, Chris Stock

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Developer: Lian Sebe

Tel: +44 (0)1235 555139 Email: editor@virusbulletin.com

Web: https://www.virusbulletin.com/