NOVEMBER 2018

virus BULLETIN

Covering the global threat landscape

VBWEB COMPARATIVE REVIEW AUTUMN 2018

Martijn Grooten & Adrian Luca

Together with email[1], the web is one of the two major infection vectors through which organizations and individuals get infected with malware, and often the two go hand in hand, with email-based threats linking to web-based malware. However, some attacks exist on the web only, and recently there has been an uptick in exploit kit activity, if not in the number of attacks then at least in the number of active kits: *Malwarebytes*' most recent report[2] lists five kits that were active at some point during the autumn.

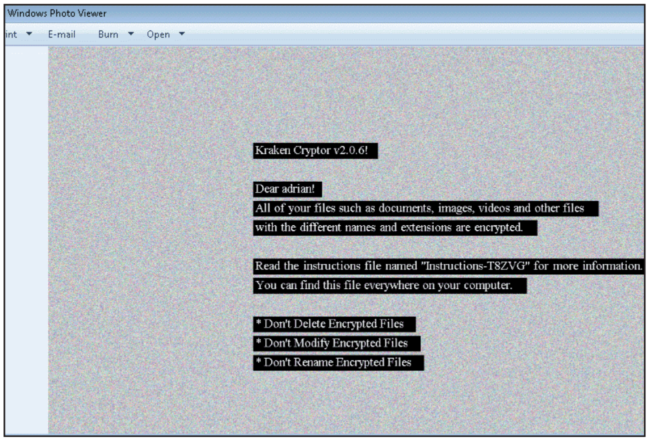
To protect against such exploit kits, regular patching remains the best strategy and it is encouraging to note that automatic patching is becoming increasingly common. But as a backstop against forgotten or ignored patches, and as protection against web-based malware that uses social engineering, web security products are an important protection layer.

THE AUTUMN 2018 THREAT LANDSCAPE

Though the prevalence of exploit kits is nowhere near its peak of a few years ago, the threat landscape remains varied, with more than half a dozen different kits seen during this test – suggesting there is still money to be made by cybercriminals this way.

All the known active kits were seen during this test with the exception of the very geographically targeted Magnitude. One particularly noteworthy kit was Fallout, a new exploit kit, first seen in August 2018[3], that is based on the code of the old Nuclear exploit kit. Interestingly, we saw some instances of Fallout being missed in this test.

A large range of malware was observed in this test, including the new Kraken Cryptor ransomware[4].



Kraken Cryptor v2.0.6!

Dear adrian!
All of your files such as documents, images, videos and other files
with the different names and extensions are encrypted.

Read the instructions file named "Instructions-T8ZVG" for more information.
You can find this file everywhere on your computer.

* Don't Delete Encrypted Files
* Don't Modify Encrypted Files
* Don't Rename Encrypted Files

Kraken Cryptor.

Thanks to the availability of free TLS certificates, we continue to see many threats using HTTPS to deliver their payload. Though the privacy implications of an organization intercepting HTTPS for its employees should be well understood, it is important to note that not doing so would mean that a not insignificant amount of malicious web traffic would bypass the security product in place.

The recent threat of web-based illicit cryptocurrency miners[5] continues to be seen; we spotted more than 450 instances of such threats during the test. However, despite the various obfuscation applied by these threats, we found that the products we tested blocked almost all of them.

[1] See the regular VBSpam reports on the email-based threat landscape and email security products' ability to protect email accounts: https://www.virusbulletin.com/testing/vbspam/.

[2] https://blog.malwarebytes.com/threat-analysis/2018/10/exploit-kits-fall-2018-review/.

[3] https://www.nao-sec.org/2018/09/hello-fallout-exploit-kit.html.

[4] https://www.recordedfuture.com/kraken-cryptor-ransomware/.

[5] https://www.virusbulletin.com/blog/2018/10/vb2018-paper-drive-download-drive-mining-understanding-new-paradigm/.

ISSN 1749-7027

RESULTS

Fortinet FortiGate

Drive-by download rate	85.6%
Malware block rate	99.3%
Weighted average	87.0%
Potentially malicious rate	96.5%
Cryptocurrency miner block rate	100.0%
False positive rate	0.00%

vb VERIFIED WEB virusbtn.com

As in previous tests, *Fortinet*'s *FortiGate* appliance performed well in this test, easily achieving its seventh VBWeb award and justifying its customers' trust in the product.

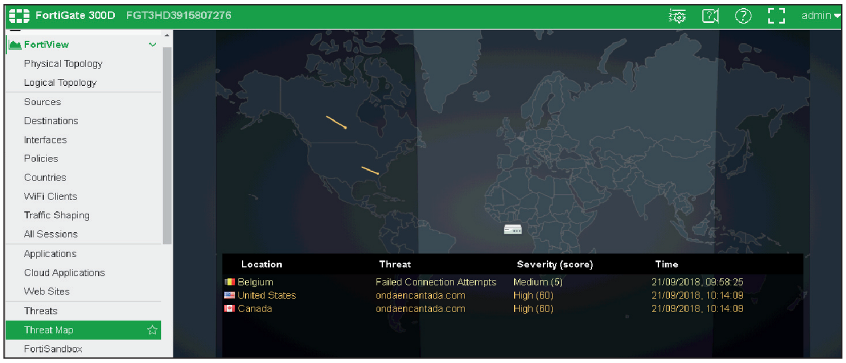
However, *FortiGate* did have some issues with some of the earlier instances of the new Fallout exploit kit seen during the test, which reduced its drive-by download catch rate. There were fewer issues with later instances of the same threat though, and the product did block the increasingly common threat of malware downloads very effectively.

Kaspersky Web Traffic Security 6.0

Drive-by download rate	100.0%
Malware block rate	99.2%
Weighted average	99.9%
Potentially malicious rate	99.2%
Cryptocurrency miner block rate	100.0%
False positive rate	0.00%

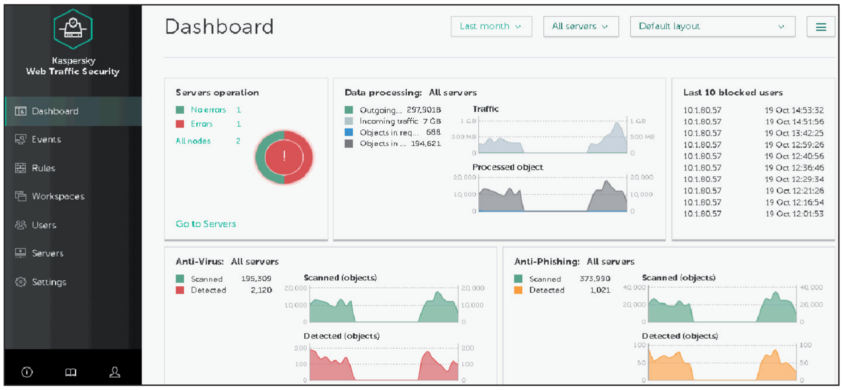
vb VERIFIED WEB virusbtn.com

Kaspersky Lab is hardly a new name in IT security, yet the company's submission of *Kaspersky Web Traffic Security* to



Location	Threat	Severity (score)	Time
Belgium	Failed Connection Attempts	Medium (5)	21/09/2018, 09:58:25
United States	ondaencantada.com	High (60)	21/09/2018, 10:14:09
Canada	ondaencantada.com	High (60)	21/09/2018, 10:14:09

Fortinet FortiGate.



Servers operation

No errors	1
Errors	1
All nodes	2

Data processing: All servers

Outgoing...	297,901B
Incoming traffic	7 GB
Objects in req...	688
Objects in ...	194,621

Last 10 blocked users

10.1.80.57	19 Oct 14:53:32
10.1.80.57	19 Oct 14:51:56
10.1.80.57	19 Oct 13:42:25
10.1.80.57	19 Oct 12:59:26
10.1.80.57	19 Oct 12:40:56
10.1.80.57	19 Oct 12:36:46
10.1.80.57	19 Oct 12:29:34
10.1.80.57	19 Oct 12:21:26
10.1.80.57	19 Oct 12:16:54
10.1.80.57	19 Oct 12:01:53

Anti-Virus: All servers

Scanned	195,309
Detected	2,120

Anti-Phishing: All servers

Scanned	373,990
Detected	1,021

Kaspersky Web Traffic Security.

this test marks its first public participation in our VBWeb tests. The 6.0 version of the product was released in October 2018.

Its performance was impressive – it was the only product to block all exploit kits, and also blocked almost all direct downloads of malware. The product's first VBWeb award is thus fully deserved and *Kaspersky*'s customers can feel confident in the product's ability to protect them from web-based threats.

Trustwave Secure Web Gateway

Drive-by download rate	95.3%
Malware block rate	98.6%
Weighted average	95.7%
Potentially malicious rate	94.2%
Cryptocurrency miner block rate	100.0%
False positive rate	0.00%

vb VERIFIED WEB virusbtn.com

Trustwave's *Secure Web Gateway* product is a regular in the VBWeb tests, always performing well. This test was no exception, with high block rates in all categories.

There were some misses among earlier instances of the new Fallout exploit kit, but after that all instances of Fallout were consistently blocked. Yet another VBWeb award, the product's sixth, was easily achieved and the product's good reputation once again affirmed.

APPENDIX: THE TEST METHODOLOGY

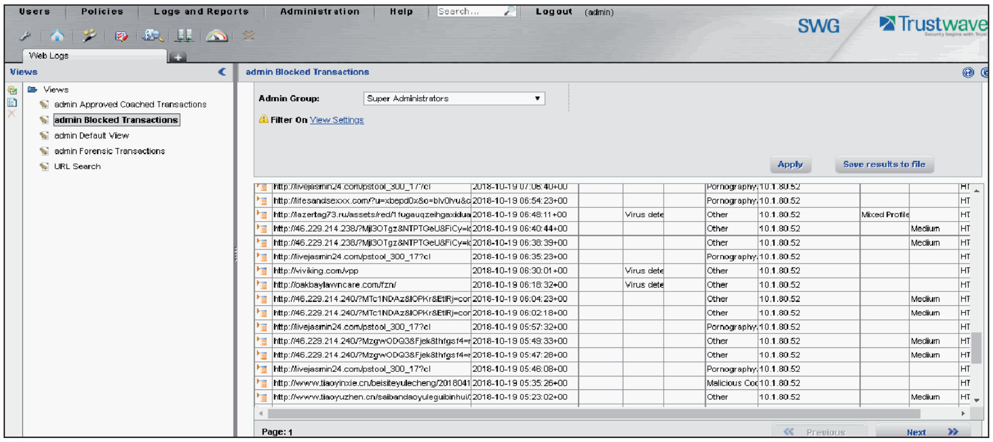
The test ran from 10 September to 23 October 2018 (with a short break in the early part of October when the team attended the VB Conference), during which period we gathered a large number of URLs (most of which were found through public sources) which we had reason to believe could serve a malicious 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 test 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 257 drive-by downloads (exploit kits) and 1,452 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 1,013 URLs that we call '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.



Admin Group: Super Administrators

Filter On View Settings

http://livejasmin24.com/pstool_300_17?cl	2018-10-19 07:06:40+00				Pornography,	10.1.80.52				HT
http://lifesandsexxx.com/?u=xbepd0x&o=blv0lvu&c	2018-10-19 06:54:23+00				Pornography,	10.1.80.52				HT
http://lazertag73.ru/assets/red/1fugauqzeihgaxidua	2018-10-19 06:48:11+00		Virus dete		Other	10.1.80.52		Mixed Profile		HT
http://46.229.214.238/?MjI3OTgz&NTPTGeU&FiCy=k	2018-10-19 06:40:44+00				Other	10.1.80.52			Medium	HT
http://46.229.214.238/?MjI3OTgz&NTPTGeU&FiCy=k	2018-10-19 06:38:39+00				Other	10.1.80.52			Medium	HT
http://livejasmin24.com/pstool_300_17?cl	2018-10-19 06:35:23+00				Pornography,	10.1.80.52				HT
http://viviking.com/vpp	2018-10-19 06:30:01+00		Virus dete		Other	10.1.80.52				HT
http://oakbaylawncare.com/fzn/	2018-10-19 06:18:32+00		Virus dete		Other	10.1.80.52				HT
http://46.229.214.240/?MTc1NDAz&lOPKr&EtlRj=cor	2018-10-19 06:04:23+00				Other	10.1.80.52			Medium	HT
http://46.229.214.240/?MTc1NDAz&lOPKr&EtlRj=cor	2018-10-19 06:02:18+00				Other	10.1.80.52			Medium	HT
http://livejasmin24.com/pstool_300_17?cl	2018-10-19 05:57:32+00				Pornography,	10.1.80.52				HT
http://46.229.214.240/?MzgwODQ3&Fjek&thfgsf4=r	2018-10-19 05:49:33+00				Other	10.1.80.52			Medium	HT
http://46.229.214.240/?MzgwODQ3&Fjek&thfgsf4=r	2018-10-19 05:47:28+00				Other	10.1.80.52			Medium	HT
http://livejasmin24.com/pstool_300_17?cl	2018-10-19 05:46:08+00				Pornography,	10.1.80.52				HT
http://www.tiaoyinxie.cn/beisiteyulecheng/2018041	2018-10-19 05:35:26+00				Malicious Coc	10.1.80.52				HT
http://www.tiaoyuzhen.cn/saibandaoyuleguibinhui/	2018-10-19 05:23:02+00				Other	10.1.80.52			Medium	HT

Page: 1

Trustwave Secure Web Gateway.

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 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, Ionuţ Răileanu, Chris Stock

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Developer: Lian Sebe

© 2018 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England
Tel: +44 (0)1235 555139 Email: editor@virusbulletin.com
Web: https://www.virusbulletin.com/