JANUARY 2020

virus BULLETIN

Covering the global threat landscape

ISSN 1749-7027

VBWEB COMPARATIVE REVIEW WINTER 2020

Martijn Grooten & Adrian Luca

Together with email[1] the web is one of the two major malware infection vectors through which organizations and individuals get infected with malware. Most organizations use security products to minimize the risk of malware making it onto the network this way, thus avoiding having to rely on security products running on the endpoint.

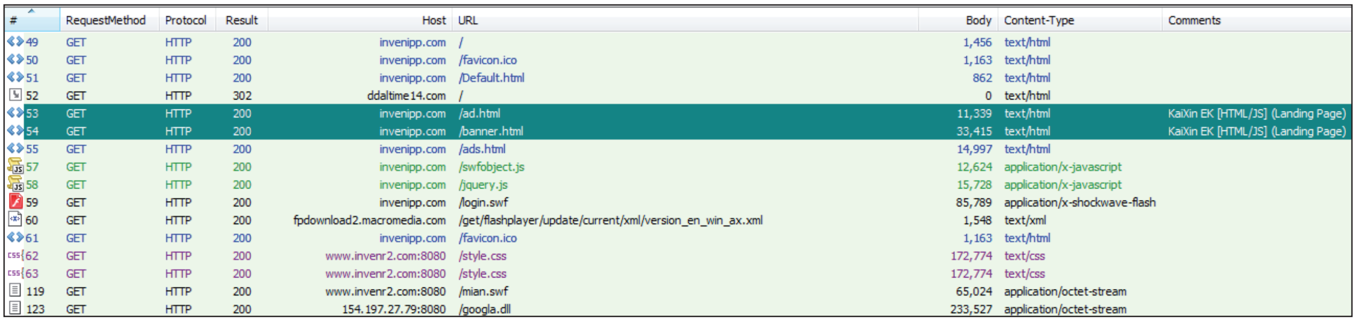
In the VBWeb tests, which form part of *Virus Bulletin*'s test suite, we measure the performance of web security products against a range of live web threats. We publish quarterly reports on the performance of the products that have opted to be included in our public testing. The reports also include an overview of the current state of the web-based threat landscape.

THE WINTER 2019/20 WEB THREAT LANDSCAPE

Winter 2019/20 continues to be more interesting than previous years when it comes to exploit kits, and we are still seeing new kits emerging. At least 11 kits[2] are currently active and in this test we caught eight of them: RIG, Fallout, Spelevo, Underminer, KaiXin, Purplefox, Capesand and Lewd.

The most recent kits to emerge were Capesand[3], found by researchers from *Trend Micro* delivering njRat, and Bottle[4], found by @nao_sec delivering a stealer that targets users in Japan.

Other malware downloaded by the various exploit kits included: Danabot, Smokeloader, Trickbot, Raccoon, Dridex, Hidenbee and Qakbot.



#	RequestMethod	Protocol	Result	Host	URL	Body	Content-Type	Comments
49	GET	HTTP	200	invenipp.com	/	1,456	text/html	
50	GET	HTTP	200	invenipp.com	/favicon.ico	1,163	text/html	
51	GET	HTTP	200	invenipp.com	/Default.html	862	text/html	
52	GET	HTTP	302	ddaltime14.com	/	0	text/html	
53	GET	HTTP	200	invenipp.com	/ad.html	11,339	text/html	KaiXin EK [HTML/JS] (Landing Page)
54	GET	HTTP	200	invenipp.com	/banner.html	33,415	text/html	KaiXin EK [HTML/JS] (Landing Page)
55	GET	HTTP	200	invenipp.com	/ads.html	14,997	text/html	
57	GET	HTTP	200	invenipp.com	/swfobject.js	12,624	application/x-javascript	
58	GET	HTTP	200	invenipp.com	/jquery.js	15,728	application/x-javascript	
59	GET	HTTP	200	invenipp.com	/login.swf	85,789	application/x-shockwave-flash	
60	GET	HTTP	200	fpdownload2.macromedia.com	/get/flashplayer/update/current/xml/version_en_win_ax.xml	1,548	text/xml	
61	GET	HTTP	200	invenipp.com	/favicon.ico	1,163	text/html	
62	GET	HTTP	200	www.invenr2.com:8080	/style.css	172,774	text/css	
63	GET	HTTP	200	www.invenr2.com:8080	/style.css	172,774	text/css	
119	GET	HTTP	200	www.invenr2.com:8080	/mian.swf	65,024	application/octet-stream	
123	GET	HTTP	200	154.197.27.79:8080	/googla.dll	233,527	application/octet-stream	

KaiXin exploit kit traffic.

[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/exploits-and-vulnerabilities/2019/11/exploit-kits-fall-2019-review/.

[3] https://blog.trendmicro.com/trendlabs-security-intelligence/new-exploit-kit-capesand-reuses-old-and-new-public-exploits-and-tools-blockchain-ruse/.

[4] https://nao-sec.org/2019/12/say-hello-to-bottle-exploit-kit.html.

We also saw more than 800 instances of malware downloads from around 90 families including Emotet, Trickbot, Ursnif, Mirai and Ransomshade. Fortunately, the tested products had very few problems blocking malware in any of these categories.

And as was the case in the Autumn 2019 test, products also had few problems blocking phishing pages.

RESULTS

It should be noted that one of the products included in this VBWeb test is a cloud-based product. As with the other products hosted in our lab, we replay previously recorded requests through cloud-based products[5], but as we do not control the connection between the product and the Internet, we cannot replay the response.

Thus it is possible that a request that results in a malicious response in our test lab results in a non-malicious response when replayed through a cloud-based product. We consider such cases full blocks, as this is the user experience, but because a cloud-based product isn't always served the malicious content by the exploit kits, for the purpose of calculating block rates we only count these instances with a weight of 0.5. However, in the case of the particular cloud-based product included this test, all exploit kits were blocked, meaning that the weighting would not have made a difference.

Fortinet FortiGate

Drive-by download rate	100.0%
Malware block rate	99.9%
Phishing block rate	96.1%
Cryptocurrency miner block rate	100.0%
False positive rate	0.0%

Fortinet's *FortiGate* appliance extends its unbroken run of VBWeb awards after having blocked all drive-by download cases (exploit kits) and having missed only one of more than 800 direct malware downloads. With over 96 per cent of phishing sites blocked, this kind of malicious site isn't a significant problem for *FortiGate* either.

iBoss

Drive-by download rate	100.0%
Malware block rate	99.1%
Phishing block rate	96.8%
Cryptocurrency miner block rate	100.0%
False positive rate	3.0%

iBoss once again blocked all drive-by download cases (exploit kits) in this test, as well as all but a few directly downloaded malware samples. *iBoss* also blocked almost 97 per cent of phishing sites. A fourth VBWeb certification is thus fully deserved.

Kaspersky Web Traffic Security

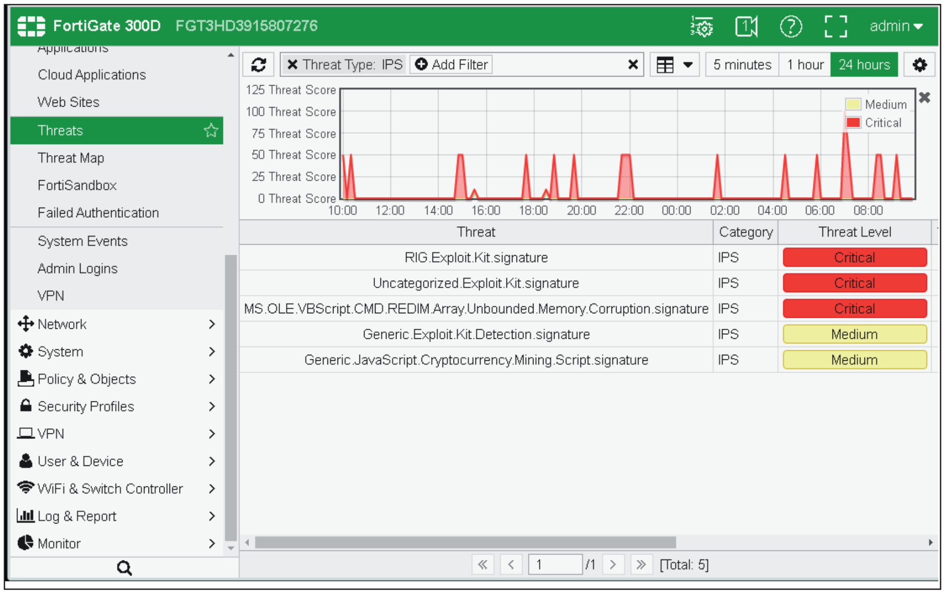
Kaspersky's web security product was also tested. Unfortunately, a routing issue caused by *Virus Bulletin* resulted in the product being unable to download updates – something that wasn't discovered until the end of the test. Indeed, even in this setting *Kaspersky* performed so well it easily achieved another VBWeb certification, but we do not think it fair to include the numbers. We look forward to seeing *Kaspersky*'s real performance in the next test.

APPENDIX: THE TEST METHODOLOGY

The test ran from 15 November to 1 December 2019, 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.

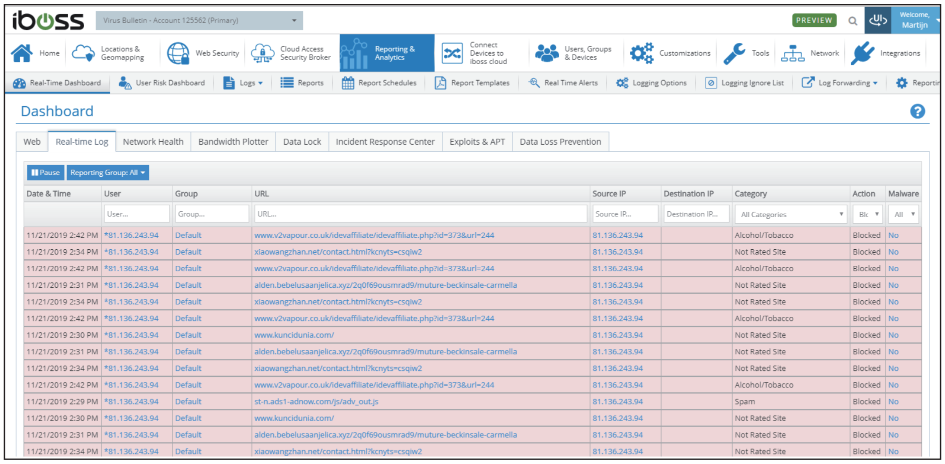
[5] The requests are replayed in near real time.



Threat	Category	Threat Level
RIG.Exploit.Kit.signature	IPS	Critical
Uncategorized.Exploit.Kit.signature	IPS	Critical
MS.OLE.VBScript.CMD.REDIM.Array.Unbounded.Memory.Corruption.signature	IPS	Critical
Generic.Exploit.Kit.Detection.signature	IPS	Medium
Generic.JavaScript.Cryptocurrency.Mining.Script.signature	IPS	Medium

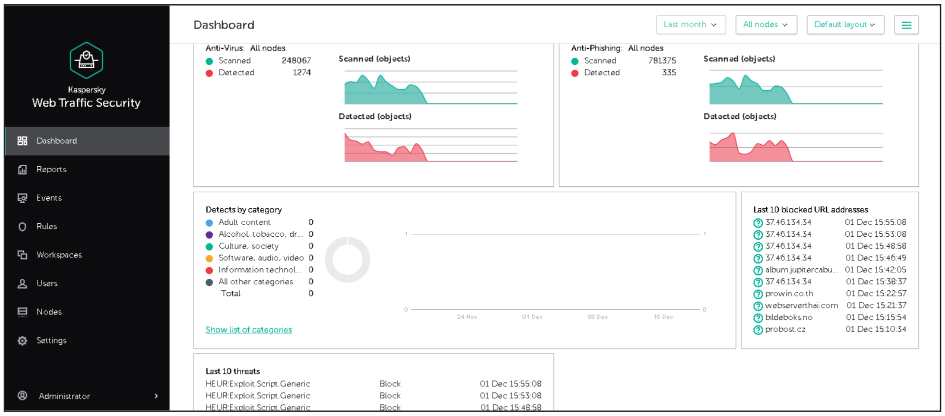
1 /1 [Total: 5]

Fortinet FortiGate.



Date & Time	User	Group	URL	Source IP	Destination IP	Category	Action	Malware
	User...	Group...	URL...	Source IP...	Destination IP...	All Categories	Blc	All
11/21/2019 2:42 PM	*81.136.243.94	Default	www.v2vapour.co.uk/idevaffiliate/idevaffiliate.php?id=373&url=244	81.136.243.94		Alcohol/Tobacco	Blocked	No
11/21/2019 2:34 PM	*81.136.243.94	Default	xiaowangzhan.net/contact.html?kcnyts=csqiw2	81.136.243.94		Not Rated Site	Blocked	No
11/21/2019 2:42 PM	*81.136.243.94	Default	www.v2vapour.co.uk/idevaffiliate/idevaffiliate.php?id=373&url=244	81.136.243.94		Alcohol/Tobacco	Blocked	No
11/21/2019 2:31 PM	*81.136.243.94	Default	alden.bebelusaanjelica.xyz/2q0f69ousmrad9/muture-beckinsale-carmella	81.136.243.94		Not Rated Site	Blocked	No
11/21/2019 2:34 PM	*81.136.243.94	Default	xiaowangzhan.net/contact.html?kcnyts=csqiw2	81.136.243.94		Not Rated Site	Blocked	No
11/21/2019 2:42 PM	*81.136.243.94	Default	www.v2vapour.co.uk/idevaffiliate/idevaffiliate.php?id=373&url=244	81.136.243.94		Alcohol/Tobacco	Blocked	No
11/21/2019 2:30 PM	*81.136.243.94	Default	www.kuncidunia.com/	81.136.243.94		Not Rated Site	Blocked	No
11/21/2019 2:31 PM	*81.136.243.94	Default	alden.bebelusaanjelica.xyz/2q0f69ousmrad9/muture-beckinsale-carmella	81.136.243.94		Not Rated Site	Blocked	No
11/21/2019 2:34 PM	*81.136.243.94	Default	xiaowangzhan.net/contact.html?kcnyts=csqiw2	81.136.243.94		Not Rated Site	Blocked	No
11/21/2019 2:42 PM	*81.136.243.94	Default	www.v2vapour.co.uk/idevaffiliate/idevaffiliate.php?id=373&url=244	81.136.243.94		Alcohol/Tobacco	Blocked	No
11/21/2019 2:29 PM	*81.136.243.94	Default	st-n.ads1-adnow.com/js/adv_out.js	81.136.243.94		Spam	Blocked	No
11/21/2019 2:30 PM	*81.136.243.94	Default	www.kuncidunia.com/	81.136.243.94		Not Rated Site	Blocked	No
11/21/2019 2:31 PM	*81.136.243.94	Default	alden.bebelusaanjelica.xyz/2q0f69ousmrad9/muture-beckinsale-carmella	81.136.243.94		Not Rated Site	Blocked	No
11/21/2019 2:34 PM	*81.136.243.94	Default	xiaowangzhan.net/contact.html?kcnyts=csqiw2	81.136.243.94		Not Rated Site	Blocked	No

iBoss.



Anti-Virus: All nodes

● Scanned	248067
● Detected	1274

Anti-Phishing: All nodes

● Scanned	781375
● Detected	335

Detects by category

● Adult content	0
● Alcohol, tobacco, dr...	0
● Culture, society	0
● Software, audio, video	0
● Information technol...	0
● All other categories	0
Total	0

Last 10 blocked URL addresses

37.46.134.34	01 Dec 15:55:08
37.46.134.34	01 Dec 15:53:08
37.46.134.34	01 Dec 15:48:58
37.46.134.34	01 Dec 15:46:49
album.jupitercabu...	01 Dec 15:42:05
37.46.134.34	01 Dec 15:38:37
prowin.co.th	01 Dec 15:22:57
webserverthai.com	01 Dec 15:21:37
bildeboks.no	01 Dec 15:15:54
probost.cz	01 Dec 15:10:34

Last 10 threats

HEUR:Exploit.Script.Generic	Block	01 Dec 15:55:08
HEUR:Exploit.Script.Generic	Block	01 Dec 15:53:08
HEUR:Exploit.Script.Generic	Block	01 Dec 15:48:58

Kaspersky Web Traffic Security.

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 700 drive-by downloads (exploit kits), 864 direct malware downloads and 441 phishing sites, a category which also includes sites that trick the user into calling a phone number. 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 80%.

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

Data for the test was provided by various public sources as well as an API provided by *Active Defense*[6].

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.

[6] https://www.activedefense.co.jp/adctd-api-spec/.

Head of Testing: Peter Karsai

Security Test Engineers: Gyula Hachbold, Adrian Luca,
Csaba Mészáros, Tony Oliveira, Ionuţ Răileanu

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Tel: +44 20 3920 6348 Email: editorial@virusbulletin.com

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