MARCH 2020

virus BULLETIN

Covering the global threat landscape

VBWEB COMPARATIVE REVIEW SPRING 2020

Adrian Luca

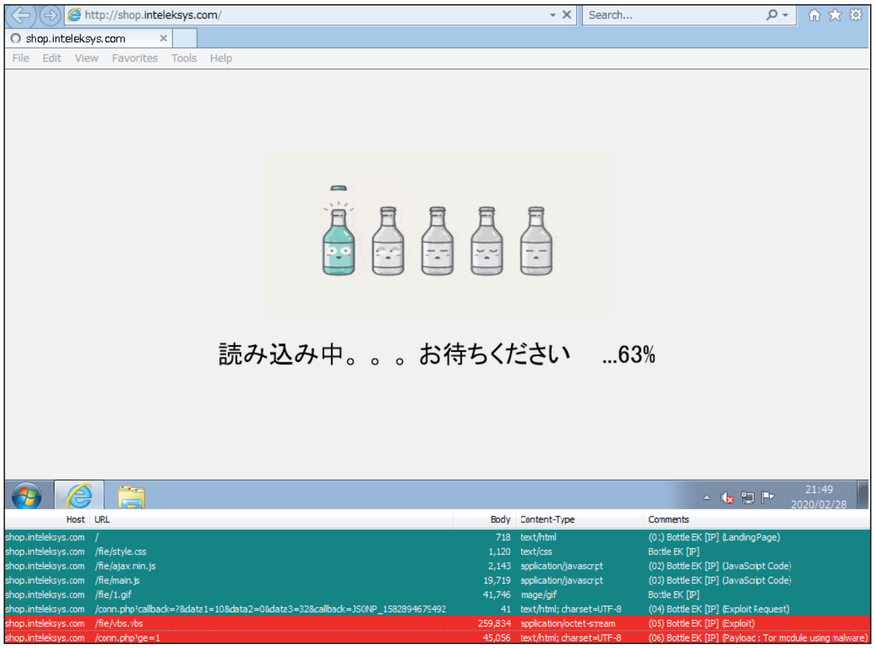
Together with email[1] the web is one of the two major malware infection vectors through which organizations and individuals get infected with malware. For this reason most organizations use security products to minimize the risk of malware making it onto the network in this way, thus avoiding having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

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 have, until now, been publishing quarterly reports on the performance of the products that have opted to be included in our public testing as well as providing an overview of the current state of the web-based threat landscape. Regrettably, the Spring 2020 edition will be the last such report and the VBWeb test is indefinitely suspended.

THE SPRING 2020 WEB THREAT LANDSCAPE

Once again, the most active exploit kit we saw during the test period was RIG, which we typically caught through malvertising. A total of at least eight exploit kits are still active, and during the test itself we saw more than 600 cases of six different exploit kits: RIG, Fallout, Spelevo, Underminer, Lewd and Bottle.

[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/.



読み込み中。。。お待ちください　...63%

Host	URL	Body	Content-Type	Comments
shop.inteleksys.com	/	718	text/html	(01) Bottle EK [IP] (LandingPage)
shop.inteleksys.com	/fie/style.css	1,120	text/css	Bottle EK [IP]
shop.inteleksys.com	/fie/ajax.min.js	2,143	application/javascript	(02) Bottle EK [IP] (JavaScript Code)
shop.inteleksys.com	/fie/main.js	19,719	application/javascript	(03) Bottle EK [IP] (JavaScript Code)
shop.inteleksys.com	/fie/1.gif	41,746	mage/gif	Bottle EK [IP]
shop.inteleksys.com	/conn.php?callback=?&data1=10&data2=0&data3=32&callback=JSONP_1582894679492	41	text/html; charset=UTF-8	(04) Bottle EK [IP] (Exploit Request)
shop.inteleksys.com	/fie/vbs.vbs	259,834	application/octet-stream	(05) Bottle EK [IP] (Exploit)
shop.inteleksys.com	/conn.php?ge=1	45,056	text/html; charset=UTF-8	(06) Bottle EK [IP] (Payload : Tor module using malware)

Bottle Ek traffic.

ISSN 1749-7027

The most recent kit, BottleEK[2], installs a new banking trojan, named Cinobi[3], that targets users in Japan. Other malware we saw downloaded by the various exploit kits included: Dridex, Phorpiex, Raccoon, XMRig, Sodinokibi, Smokeloader, Zloader and Hidenbee.

We also saw almost 500 instances of malware downloads from around 80 families including Emotet, Pony, Troldesh, Ursnif, Azorult and FormBook. Fortunately, the tested products had very few problems blocking malware in any of these categories.

And as was the case in the Winter 2020 VBWeb test[4], 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	99.4%
Phishing block rate	95.4%
False positive rate	0.0%

Fortinet's *FortiGate* appliance extends its unbroken run of VBWeb awards going several years, by blocking all drive-by download cases and missing only three of almost 500 direct malware downloads. With over 95 per cent of phishing sites blocked, this kind of malicious site isn't a big problem for *FortiGate* either. As such, *Fortinet FortiGate* fully deserves another VBWeb award. But besides the product's excellent performance in this test, it is its strong performance over 15 tests that its developers can be truly proud of.

iBoss

Drive-by download rate	100.0%
Malware block rate	100.0%
Phishing block rate	99.3%
False positive rate	2.6%

iBoss extends its impressive VBWeb performance by blocking all drive-by download cases (exploit kits) in this test, as well as all directly downloaded malware samples. *iBoss* also blocked over 99 per cent of phishing sites. The product easily earns its fifth VBWeb certification.

Kaspersky Web Traffic Security

Drive-by download rate	100.0%
Malware block rate	99.0%
Phishing block rate	97.4%
False positive rate	0.0%

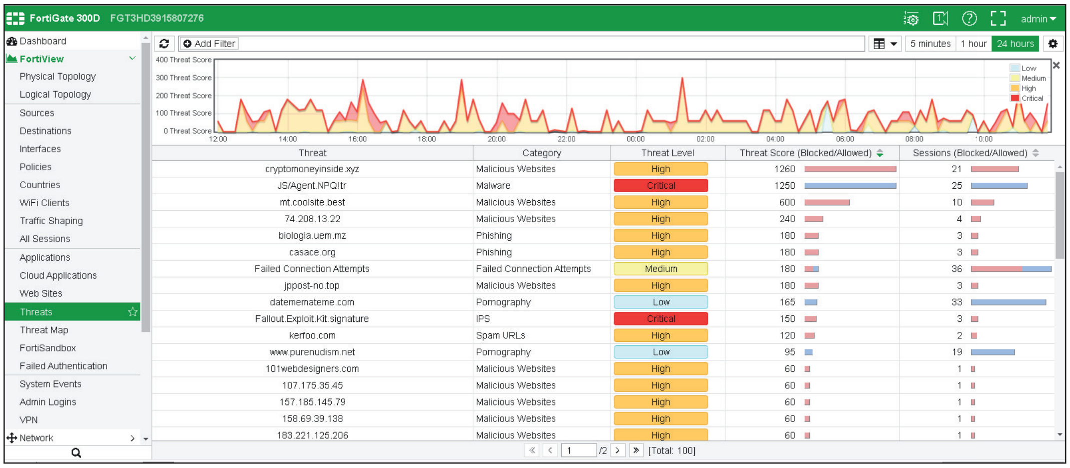
Kaspersky Web Traffic Security blocked all of the more than 650 exploit kits seen in this test. The detection rate of direct malware downloads was very good too, with only a handful of them missed. The product also achieved a good phishing blocking rate of over 97 per cent, thus showing that the gateway product provides an excellent first line of defence for web-based threats and its third VBWeb certification is fully deserved.

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

[3] https://blog.trendmicro.com/trendlabs-security-intelligence/operation-overtrap-targets-japanese-online-banking-users-via-bottle-exploit-kit-and-brand-new-cinobi-banking-trojan/

[4] https://www.virusbulletin.com/virusbulletin/2020/01/vbweb-comparative-review/

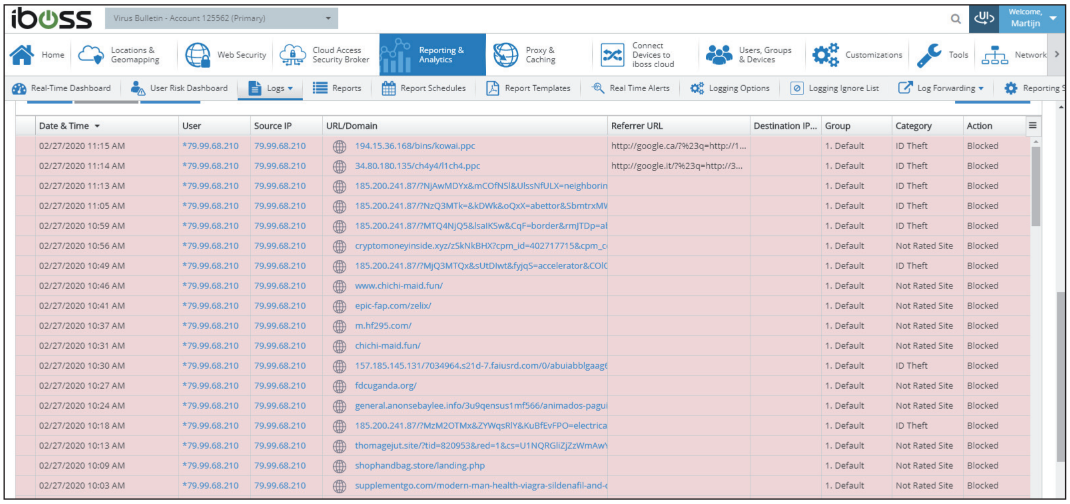
[5] The requests are replayed in near real time.



Threat	Category	Threat Level	Threat Score (Blocked/Allowed)	Sessions (Blocked/Allowed)
cryptomoneyinside.xyz	Malicious Websites	High	1260	21
JS/Agent.NPQ!tr	Malware	Critical	1250	25
mt.coolsite.best	Malicious Websites	High	600	10
74.208.13.22	Malicious Websites	High	240	4
biologia.uem.mz	Phishing	High	180	3
casace.org	Phishing	High	180	3
Failed Connection Attempts	Failed Connection Attempts	Medium	180	36
jppost-no.top	Malicious Websites	High	180	3
datemematerne.com	Pornography	Low	165	33
Fallout.Exploit.Kit.signature	IPS	Critical	150	3
kerfoo.com	Spam URLs	High	120	2
www.purenudism.net	Pornography	Low	95	19
101webdesigners.com	Malicious Websites	High	60	1
107.175.35.45	Malicious Websites	High	60	1
157.185.145.79	Malicious Websites	High	60	1
158.69.39.138	Malicious Websites	High	60	1
183.221.125.206	Malicious Websites	High	60	1

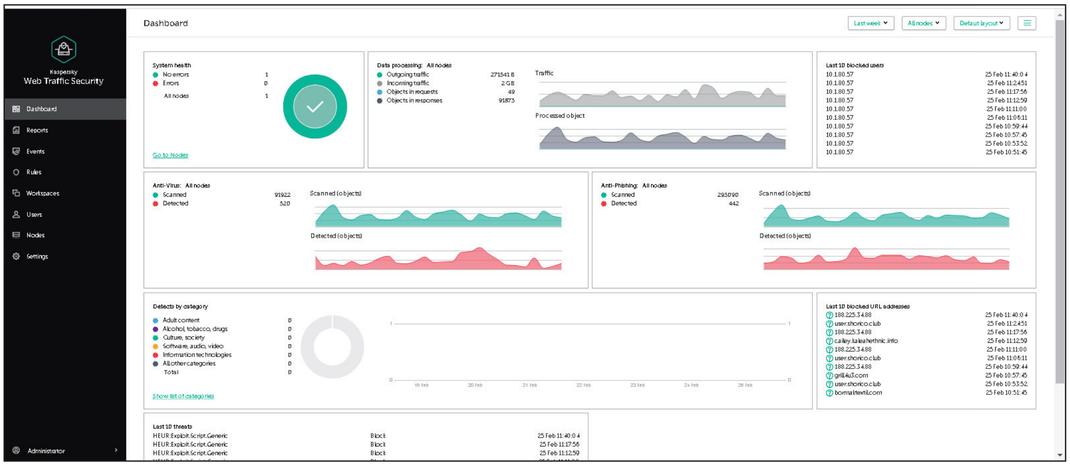
1 /2 [Total: 100]

Fortinet FortiGate.



Date & Time	User	Source IP	URL/Domain	Referrer URL	Destination IP...	Group	Category	Action
02/27/2020 11:15 AM	*79.99.68.210	79.99.68.210	194.15.36.168/bins/kowai.ppc	http://google.ca/?%23q=http://1...		1. Default	ID Theft	Blocked
02/27/2020 11:14 AM	*79.99.68.210	79.99.68.210	34.80.180.135/ch4y4/l1ch4.ppc	http://google.it/?%23q=http://3...		1. Default	ID Theft	Blocked
02/27/2020 11:13 AM	*79.99.68.210	79.99.68.210	185.200.241.87/?NjAwMDYx&mCOfNSl&UlssNfULX=neighborin			1. Default	ID Theft	Blocked
02/27/2020 11:05 AM	*79.99.68.210	79.99.68.210	185.200.241.87/?NzQ3MTk=&kDWk&oQxX=abettor&SbmtrxMV			1. Default	ID Theft	Blocked
02/27/2020 10:59 AM	*79.99.68.210	79.99.68.210	185.200.241.87/?MTQ4NjQ5&lsalKSw&CqF=border&rmJTDp=al			1. Default	ID Theft	Blocked
02/27/2020 10:56 AM	*79.99.68.210	79.99.68.210	cryptomoneyinside.xyz/zSkNkBHX?cpm_id=402717715&cpm_c			1. Default	Not Rated Site	Blocked
02/27/2020 10:49 AM	*79.99.68.210	79.99.68.210	185.200.241.87/?MjQ3MTQx&sUtDlwt&fyjqS=accelerator&COlC			1. Default	ID Theft	Blocked
02/27/2020 10:46 AM	*79.99.68.210	79.99.68.210	www.chichi-maid.fun/			1. Default	Not Rated Site	Blocked
02/27/2020 10:41 AM	*79.99.68.210	79.99.68.210	epic-fap.com/zelix/			1. Default	Not Rated Site	Blocked
02/27/2020 10:37 AM	*79.99.68.210	79.99.68.210	m.hf295.com/			1. Default	Not Rated Site	Blocked
02/27/2020 10:31 AM	*79.99.68.210	79.99.68.210	chichi-maid.fun/			1. Default	Not Rated Site	Blocked
02/27/2020 10:30 AM	*79.99.68.210	79.99.68.210	157.185.145.131/7034964.s21d-7.faiusrd.com/0/abuiabblgaag6			1. Default	ID Theft	Blocked
02/27/2020 10:27 AM	*79.99.68.210	79.99.68.210	fdcuganda.org/			1. Default	Not Rated Site	Blocked
02/27/2020 10:24 AM	*79.99.68.210	79.99.68.210	general.anonsebaylee.info/3u9qensus1mf566/animados-pagui			1. Default	Not Rated Site	Blocked
02/27/2020 10:18 AM	*79.99.68.210	79.99.68.210	185.200.241.87/?MzM2OTMx&ZYWqsRlY&KuBfEvFPO=electrica			1. Default	ID Theft	Blocked
02/27/2020 10:13 AM	*79.99.68.210	79.99.68.210	thomagejut.site/?tid=820953&red=1&cs=U1NQRGliZjZzWmAwY			1. Default	Not Rated Site	Blocked
02/27/2020 10:09 AM	*79.99.68.210	79.99.68.210	shophandbag.store/landing.php			1. Default	Not Rated Site	Blocked
02/27/2020 10:03 AM	*79.99.68.210	79.99.68.210	supplementgo.com/modern-man-health-viagra-sildenafil-and-c			1. Default	Not Rated Site	Blocked

iBoss.



System health

No errors	1
Errors	0
All nodes	1

Data processing: All nodes

Outgoing traffic	271541 B
Incoming traffic	2 GB
Objects in requests	49
Objects in responses	91873

Last 10 blocked users

10.1.80.57	25 Feb 11:40:04
10.1.80.57	25 Feb 11:24:51
10.1.80.57	25 Feb 11:17:56
10.1.80.57	25 Feb 11:12:59
10.1.80.57	25 Feb 11:11:00
10.1.80.57	25 Feb 11:06:11
10.1.80.57	25 Feb 10:59:44
10.1.80.57	25 Feb 10:57:45
10.1.80.57	25 Feb 10:53:52
10.1.80.57	25 Feb 10:51:45

Anti-Virus: All nodes

Scanned	91922
Detected	520

Anti-Phishing: All nodes

Scanned	293090
Detected	442

Detects by category

Adult content	0
Alcohol, tobacco, drugs	0
Culture, society	0
Software, audio, video	0
Information technologies	0
All other categories	0
Total	0

Last 10 blocked URL addresses

188.225.34.88	25 Feb 11:40:04
user.shorico.club	25 Feb 11:24:51
188.225.34.88	25 Feb 11:17:56
cailey.kaleahethnic.info	25 Feb 11:12:59
188.225.34.88	25 Feb 11:11:00
user.shorico.club	25 Feb 11:06:11
188.225.34.88	25 Feb 10:59:44
grill4u3.com	25 Feb 10:57:45
user.shorico.club	25 Feb 10:53:52
bormaktextil.com	25 Feb 10:51:45

Last 10 threats

HEUR:Exploit.Script.Generic	Block	25 Feb 11:40:04
HEUR:Exploit.Script.Generic	Block	25 Feb 11:17:56
HEUR:Exploit.Script.Generic	Block	25 Feb 11:12:59

Kaspersky Web Traffic Security.

APPENDIX: THE TEST METHODOLOGY

The test ran from 14 February 2020 to 29 February 2020, 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 654 drive-by downloads (exploit kits), 482 direct malware downloads and 416 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 from 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

© 2020 Virus Bulletin Ltd, Manor House - Office 6, Howbery Business Park, Wallingford OX10 8BA, UK

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

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