JULY 2019

virus BULLETIN

Covering the global threat landscape

VBWEB COMPARATIVE REVIEW SUMMER 2019

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 SUMMER 2019 THREAT LANDSCAPE

Recent months have seen some interesting developments when it comes to web-based malware. On the one hand, the shutdown of Coinhive in March 2019 led to a sharp decline in illicit in-browser mining activity, though it will be interesting to see if the recent increase in cryptocurrency values will lead malicious authors to return to mining for such currencies in users' browsers.

At the same time, exploit kits are making some kind of comeback. Just after this test ended, the GreenFlash Sundown kit[2] became very active during a large malvertising campaign. During the test itself, we saw hundreds of cases of six different exploit kits: Rig, Spelevo, Fallout, Kaixin, Underminer and the Router exploit kit, which targets vulnerable routers rather than attempting to infect the endpoint.

We saw these exploit kits deliver ransomware such as Sodinokibi and Buran, banking trojans such as IcedID

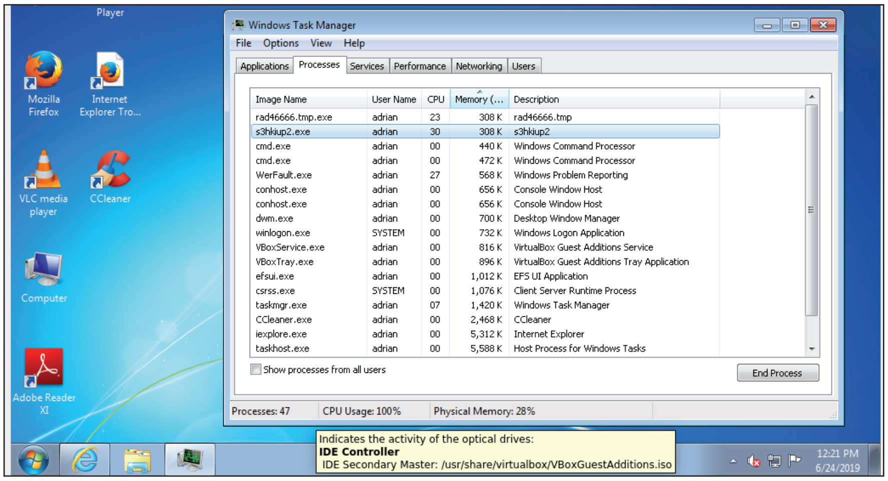


Image Name	User Name	CPU	Memory (...	Description
rad46666.tmp.exe	adrian	23	308 K	rad46666.tmp
s3hkiup2.exe	adrian	30	308 K	s3hkiup2
cmd.exe	adrian	00	440 K	Windows Command Processor
cmd.exe	adrian	00	472 K	Windows Command Processor
WerFault.exe	adrian	27	568 K	Windows Problem Reporting
conhost.exe	adrian	00	656 K	Console Window Host
conhost.exe	adrian	00	656 K	Console Window Host
dwm.exe	adrian	00	700 K	Desktop Window Manager
winlogon.exe	SYSTEM	00	732 K	Windows Logon Application
VBoxService.exe	adrian	00	816 K	VirtualBox Guest Additions Service
VBoxTray.exe	adrian	00	896 K	VirtualBox Guest Additions Tray Application
efsui.exe	adrian	00	1,012 K	EFS UI Application
csrss.exe	SYSTEM	00	1,076 K	Client Server Runtime Process
taskmgr.exe	adrian	07	1,420 K	Windows Task Manager
CCleaner.exe	adrian	00	2,468 K	CCleaner
iexplore.exe	adrian	00	5,312 K	Internet Explorer
taskhost.exe	adrian	00	5,588 K	Host Process for Windows Tasks

Processes: 47 CPU Usage: 100% Physical Memory: 28%

Indicates the activity of the optical drives:
IDE Controller
IDE Secondary Master: /usr/share/virtualbox/VBoxGuestAdditions.iso

12:21 PM
6/24/2019

Infection attempt following successful execution of the Rig exploit kit.

[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/2019/06/greenflash-sundown-exploit-kit-expands-via-large-malvertising-campaign/.

ISSN 1749-7027

and Kronos, as well as other kinds of malware such as the AZORult information stealer and the Pitou spambot.

We also saw a wide variety of direct malware downloads, including Emotet, GandCrab, Pony, Nanobot and Troldesh. Thankfully, tested products had very few problems blocking malware in any of these categories.

New in this test is the category of phishing websites. Such sites aren't malicious in a strict sense – in that they won't infect a user's computer – but the stealing of credentials is an important cybercriminal activity. Despite the lack of any malicious code making these kinds of sites inherently harder to block, we were pleased to see products block over 95 per cent of them.

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[3], 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	99.5%
Phishing block rate	95.2%
Cryptocurrency miner block rate	100.0%
False positive rate	0.0%

Fortinet's *FortiGate* appliance continued its unbroken run of VBWeb awards that goes back several years, blocking all drive-by download cases and almost all direct malware downloads. With over 95 per cent of phishing sites blocked, this kind of malicious site doesn't pose a big problem for *FortiGate* either.

iBoss

Drive-by download rate	100.0%
Malware block rate	99.3%
Phishing block rate	96.9%
Cryptocurrency miner block rate	100.0%
False positive rate	0.5%

iBoss showed that its impressive performance in its debut test was no exception, blocking all drive-by download cases (exploit kits) in this test, as well as all directly downloaded malware. *iBoss* also blocked almost 97 per cent of phishing sites. The product's second VBWeb certification is thus well deserved.

APPENDIX: THE TEST METHODOLOGY

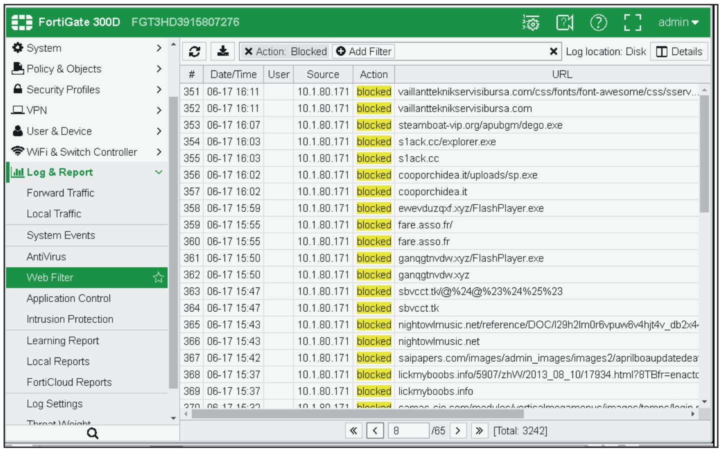
The test ran from 7 June 2019 to 24 June 2019 during which period we gathered a large number of URLs (most of which were found through public sources) which we had reason to believe could serve a malicious response. We opened the URLs in one of our test browsers, selected at random.

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.

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 224 drive-by downloads (exploit kits), 1,338 direct malware downloads

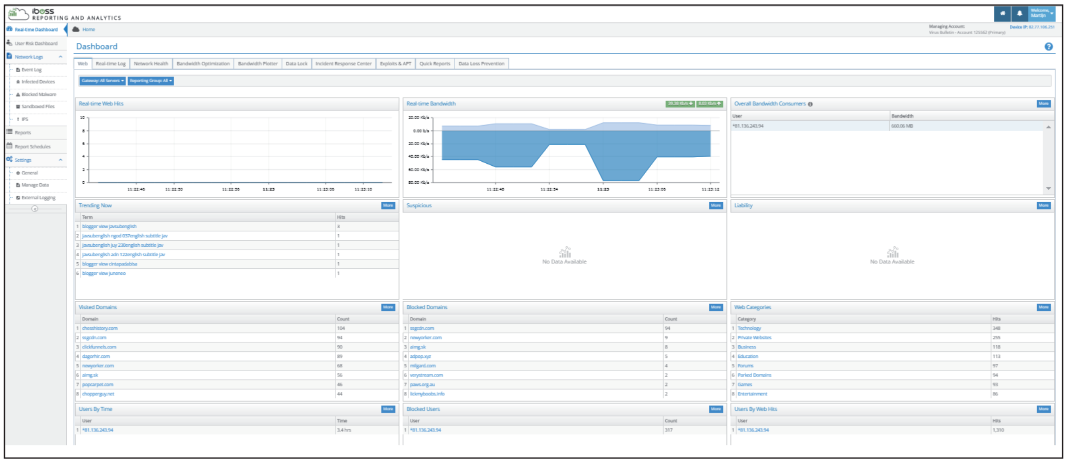
[3] The requests are replayed in near real time.



#	Date/Time	User	Source	Action	URL
351	06-17 16:11		10.1.80.171	blocked	vaillantteknikservisibursa.com/css/fonts/font-awesome/css/sserv...
352	06-17 16:11		10.1.80.171	blocked	vaillantteknikservisibursa.com
353	06-17 16:07		10.1.80.171	blocked	steamboat-vip.org/apubgm/dego.exe
354	06-17 16:03		10.1.80.171	blocked	s1ack.cc/explorer.exe
355	06-17 16:03		10.1.80.171	blocked	s1ack.cc
356	06-17 16:02		10.1.80.171	blocked	cooporchidea.it/uploads/sp.exe
357	06-17 16:02		10.1.80.171	blocked	cooporchidea.it
358	06-17 15:59		10.1.80.171	blocked	ewevduzqxf.xyz/FlashPlayer.exe
359	06-17 15:55		10.1.80.171	blocked	fare.asso.fr/
360	06-17 15:55		10.1.80.171	blocked	fare.asso.fr
361	06-17 15:50		10.1.80.171	blocked	ganqgtnvdw.xyz/FlashPlayer.exe
362	06-17 15:50		10.1.80.171	blocked	ganqgtnvdw.xyz
363	06-17 15:47		10.1.80.171	blocked	sbvcct.tk/@%24@%23%24%25%23
364	06-17 15:47		10.1.80.171	blocked	sbvcct.tk
365	06-17 15:43		10.1.80.171	blocked	nightowlmusic.net/reference/DOC/l29h2lm0r6vpuw6v4hjt4v_db2x4
366	06-17 15:43		10.1.80.171	blocked	nightowlmusic.net
367	06-17 15:42		10.1.80.171	blocked	saipapers.com/images/admin_images/images2/aprilboaupdatedea
368	06-17 15:37		10.1.80.171	blocked	lickmyboobs.info/5907/zhW/2013_08_10/17934.html?8TBfr=enactc
369	06-17 15:37		10.1.80.171	blocked	lickmyboobs.info
370	06-17 15:32		10.1.80.171	blocked	camas-cic.com/modules/verticalmegamenus/images/temps/login

« < 8 /65 > » [Total: 3242]

Fortinet FortiGate.



Overall Bandwidth Consumers

User	Bandwidth
*81.136.243.94	660.06 MB

Trending Now

	Term	Hits
1	blogger view javsubenglish	3
2	javsubenglish ngod 037english subtitle jav	1
3	javsubenglish juy 230english subtitle jav	1
4	javsubenglish adn 122english subtitle jav	1
5	blogger view cintapadabisa	1
6	blogger view juneneo	1

Visited Domains

	Domain	Count
1	chesshistory.com	104
2	ssgcdn.com	94
3	clickfunnels.com	90
4	dagorhir.com	89
5	newyorker.com	68
6	aimg.sk	56
7	popcarpet.com	46
8	chopperguy.net	44

Blocked Domains

	Domain	Count
1	ssgcdn.com	94
2	newyorker.com	9
3	aimg.sk	8
4	adpop.xyz	5
5	milgard.com	4
6	verystream.com	2
7	paws.org.au	2
8	lickmyboobs.info	2

Web Categories

	Category	Hits
1	Technology	348
2	Private Websites	255
3	Business	118
4	Education	113
5	Forums	97
6	Parked Domains	94
7	Games	93
8	Entertainment	86

Users By Time

	User	Time
1	*81.136.243.94	3.4 hrs

Blocked Users

	User	Count
1	*81.136.243.94	317

Users By Web Hits

	User	Hits
1	*81.136.243.94	1,310

iBoss.

and 547 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 the first two of these categories, with weights of 90% and 10% respectively, needed to be at least 80%.

The 'potentially malicious' cases that were included in previous reports have been removed from the public test reports.

The test focused on both HTTP and HTTPS 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: Gyula Hachbold, Adrian Luca, Csaba Mészáros, Tony Oliveira, Ionuţ Răileanu
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin

© 2019 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/