FEBRUARY 2019

virus BULLETIN

Covering the global threat landscape

VBWEB COMPARATIVE REVIEW WINTER 2019

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. Most organizations use web security products to minimize the risk of malware making it onto the network this way, thus avoiding having to rely solely on security products that run on the endpoint.

In the VBWeb tests we measure the performance of web security products against a wide 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 THREAT LANDSCAPE

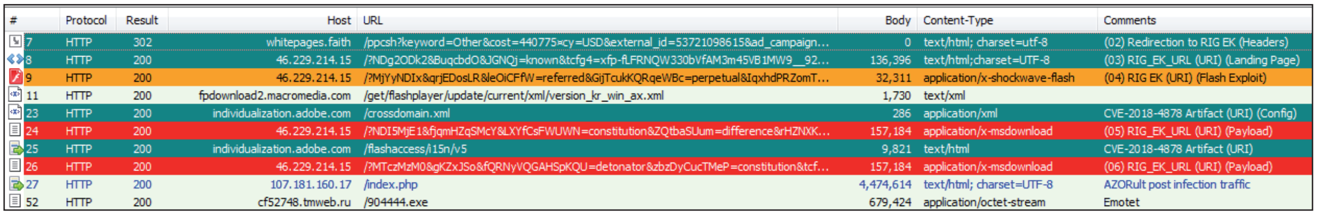
Though cybercrime is a global phenomenon, a significant number of malware campaigns are run by individuals who take a break during the Russian Orthodox Christmas holidays. Indeed, we saw a decline in activity during this period, with many exploit kits either reducing or stopping their activity altogether.

We believe that a number of exploit kits continued to be active during this period, but we only observed two, Rig and Fallout, during our test, with Fallout not delivering a full payload. This means that all 277 of the exploit kits observed were part of Rig, which uses a number of different gates.

The Gandcrab ransomware continues to be a payload commonly delivered by exploit kits, while we also saw infostealers like AZORult and Vidar being delivered, the latter of which is fairly new[2], as well as some adware families. We observed at least one case where a download of AZORult was followed by a download of the infamous Emotet malware.

Emotet was also seen regularly as the payload of direct malware downloads, which is not surprising given that it is often served via links in spam emails. Other payloads we observed included Ramnit, Hancitor and Mirai. We should note that it is likely that some of these malware samples would have gone on to install further payloads in a real-world scenario.

As we have seen in the past, the products in our test performed extremely well against drive-by downloads and the related, but less severe threat of in-browser cryptocurrency mining, with both of the products in this public report blocking 100% of the cases in both categories. Block rates of direct malware downloads were not quite as impressive, but still very high.



#	Protocol	Result	Host	URL	Body	Content-Type	Comments
7	HTTP	302	whitepages.faith	/ppcsh?keyword=Other&cost=440775¤cy=USD&external_id=53721098615&ad_campaign…	0	text/html; charset=utf-8	(02) Redirection to RIG EK (Headers)
8	HTTP	200	46.229.214.15	/?NDg2ODk2&BuqcbdO&JGNQj=known&tcfg4=xfp-fLFRNQW330bVfAM3m45VB1MW9__92…	136,396	text/html;charset=UTF-8	(03) RIG_EK_URL (URI) (Landing Page)
9	HTTP	200	46.229.214.15	/?MjYyNDIx&qrjEDosLR&leOiCFfW=referred&GijTcukKQRqeWBc=perpetual&IqxhdPRZomT…	32,311	application/x-shockwave-flash	(04) RIG EK (URI) (Flash Exploit)
11	HTTP	200	fpdownload2.macromedia.com	/get/flashplayer/update/current/xml/version_kr_win_ax.xml	1,730	text/xml	
23	HTTP	200	individualization.adobe.com	/crossdomain.xml	286	application/xml	CVE-2018-4878 Artifact (URI) (Config)
24	HTTP	200	46.229.214.15	/?NDI5MjE1&fjqmHZqSMcY&LXYfCsFWUWN=constitution&ZQtbaSUum=difference&rHZNXK…	157,184	application/x-msdownload	(05) RIG_EK_URL (URI) (Payload)
25	HTTP	200	individualization.adobe.com	/flashaccess/i15n/v5	9,821	text/html	CVE-2018-4878 Artifact (URI)
26	HTTP	200	46.229.214.15	/?MTczMzM0&gKZxJSo&fQRNyVQGAHSpKQU=detonator&zbzDyCucTMeP=constitution&tcf…	157,184	application/x-msdownload	(06) RIG_EK_URL (URI) (Payload)
27	HTTP	200	107.181.160.17	/index.php	4,474,614	text/html; charset=UTF-8	AZORult post infection traffic
52	HTTP	200	cf52748.tmweb.ru	/904444.exe	679,424	application/octet-stream	Emotet

Post-infection traffic following a successful infection attempt by the Rig exploit kit serving first AZORult and then Emotet (traffic highlighted with EKFiddle in Fiddler).

[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://fumik0.com/2018/12/24/lets-dig-into-vidar-an-arkei-copycat-forked-stealer-in-depth-analysis/

ISSN 1749-7027

RESULTS

Fortinet FortiGate

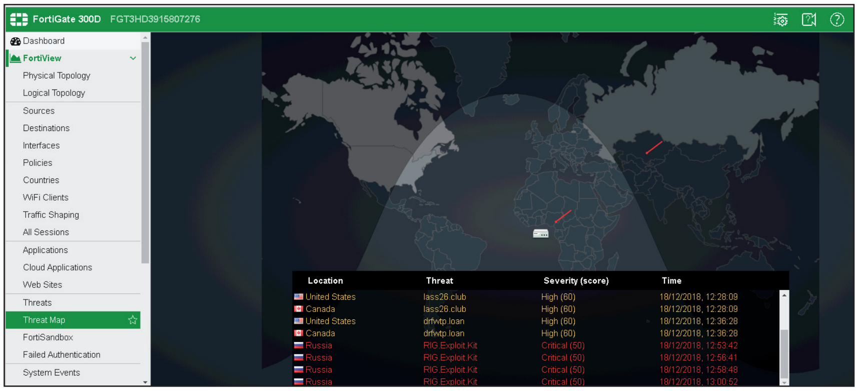
Drive-by download rate	100.0%
Malware block rate	98.5%
Weighted average	99.9%
Potentially malicious rate	99.3%
Cryptocurrency miner block rate	100.0%
False positive rate	0.00%

A long test period didn't pose any problems for *Fortinet's FortiGate* appliance, which blocked all drive-by downloads and all instances of in-browser mining we observed in our test. It also blocked all but a handful of direct malware downloads, meaning that *Fortinet* easily achieves its eighth VBWeb certification.

Trustwave Secure Web Gateway

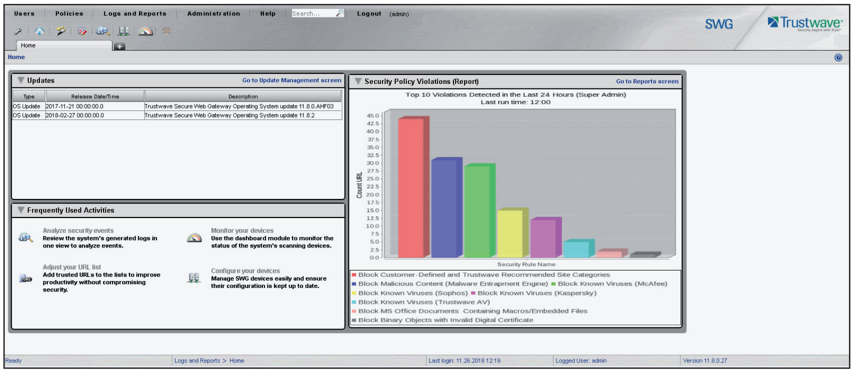
Drive-by download rate	100.0%
Malware block rate	96.5%
Weighted average	99.7%
Potentially malicious rate	88.9%
Cryptocurrency miner block rate	100.0%
False positive rate	0.00%

The last test saw *Trustwave*'s web security product catch up quickly with new threats, so we weren't surprised to see it block all drive-by downloads and all instances of in-browser mining in this test. A small number of direct malware downloads slipped through, but in practice such misses would be mitigated by security products running on the endpoint. *Trustwave* is thus fully deserving of its seventh VBWeb certification.



Location	Threat	Severity (score)	Time
United States	lass26.club	High (60)	18/12/2018, 12:28:09
Canada	lass26.club	High (60)	18/12/2018, 12:28:09
United States	drfwtp.loan	High (60)	18/12/2018, 12:36:28
Canada	drfwtp.loan	High (60)	18/12/2018, 12:36:28
Russia	RIG.Exploit.Kit	Critical (50)	18/12/2018, 12:53:42
Russia	RIG.Exploit.Kit	Critical (50)	18/12/2018, 12:56:41
Russia	RIG.Exploit.Kit	Critical (50)	18/12/2018, 12:58:48
Russia	RIG.Exploit.Kit	Critical (50)	18/12/2018, 13:00:52

Fortinet FortiGate.



Type	Release Date/Time	Description
OS Update	2017-11-21 00:00:00.0	Trustwave Secure Web Gateway Operating System update 11.8.0.AHF03
OS Update	2018-02-27 00:00:00.0	Trustwave Secure Web Gateway Operating System update 11.8.2

🟥 Block Customer-Defined and Trustwave Recommended Site Categories
🟦 Block Malicious Content (Malware Entrapment Engine) 🟩 Block Known Viruses (McAfee)
🟨 Block Known Viruses (Sophos) 🟪 Block Known Viruses (Kaspersky)
■ Block Known Viruses (Trustwave AV)
■ Block MS Office Documents Containing Macros/Embedded Files
■ Block Binary Objects with Invalid Digital Certificate

Analyze security events
Review the system's generated logs in one view to analyze events.

Monitor your devices
Use the dashboard module to monitor the status of the system's scanning devices.

Adjust your URL list
Add trusted URLs to the lists to improve productivity without compromising security.

Configure your devices
Manage SWG devices easily and ensure their configuration is kept up to date.

Ready | Logs and Reports > Home | Last login: 11.26.2018 12:19 | Logged User: admin | Version 11.8.0.27

Trustwave Secure Web Gateway.

APPENDIX: THE TEST METHODOLOGY

The test ran from 26 November 2018 to 13 January 2019 (with a short break taken around the holiday season), 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 277 drive-by downloads (exploit kits) and 1,067 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 289 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.

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 include it in this report 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: 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/