MAY 2019

virus BULLETIN

Covering the global threat landscape

VBWEB COMPARATIVE REVIEW SPRING 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 SPRING 2019 THREAT LANDSCAPE

Though, as noted in previous VBWeb reports, the exploit kit landscape is nowhere near as active as it was half a decade ago, a number of exploit kits are still active and new ones continue to appear – for example the Spelevo kit, which was first spotted early in March[2], not long before this test started. It was also spotted in our lab during the test.

The most active kit during the test period continued to be Rig, which we typically caught through malvertising and which typically linked to the Fobos or Hookads campaigns. Interestingly, we spotted cases of the latter campaign where, depending on the location from which the request was made (we use a distributed network of IP addresses for our tests), the user was redirected to either Rig or Spelevo[3].

As a reminder that it wasn't just *Flash Player* that was being exploited, we spotted cases of CVE-2018-8174[4], a vulnerability in *Internet Explorer* patched last year, which installed the lesser-known Golden Axe ransomware. We also recorded instances of the Fallout exploit kit during this test.

Among the direct malware downloads, we found a wide range of malware including Emotet, Trickbot, Pony, AZORult and Mirai.

RESULTS

For the first time, a cloud-based product was included in this VBWeb test. 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.

[1] See the regular VBSpam reports on the email-based threat landscape and email security products' ability to protect email accounts.
[2] https://twitter.com/kafeine/status/1103649040800145409.
[3] See also https://twitter.com/nao_sec/status/1108388558539087873.
[4] https://securelist.com/root-cause-analysis-of-cve-2018-8174/85486/.
[5] The requests are replayed in near real time.

ISSN 1749-7027

Fortinet FortiGate

Drive-by download rate	100.0%
Malware block rate	99.0%
Weighted average	99.9%
Cryptocurrency miner block rate	100.0%
False positive rate	0.0%

Fortinet's *FortiGate* appliance once again blocked all the drive-by downloads and in-browser mining observed during the test. It also blocked all but a handful of direct malware downloads and did not block any legitimate URLs. The product deservedly earns its eleventh VBWeb certification.

iBoss

Drive-by download rate	100.0%
Malware block rate	99.5%
Weighted average	99.9%
Cryptocurrency miner block rate	100.0%
False positive rate	0.7%

iBoss is a cloud-based web security solution that makes its debut in this VBWeb test. *Virus Bulletin* does not express a view as to whether it is better to use a cloud-based or a locally hosted solution, but when it comes to performance, customers should not expect any difference. We were thus pleased to see the product block 100% of all exploit kits and all but a few direct malware downloads. With this performance the product earns its first VBWeb award.

We should note that the product did erroneously block three legitimate URLs in our test. Though we do not think this number is sufficiently high to deny the product an award, it is worth noting that some customers may want to choose slightly different settings from those we used in our test.

Trustwave Secure Web Gateway

Drive-by download rate	100.0%
Malware block rate	98.4%
Weighted average	99.8%
Cryptocurrency miner block rate	100.0%
False positive rate	0.0%

Trustwave's 100% block rate of both drive-by downloads and cryptocurrency miners won't come as a surprise for regular readers of this report, neither will its very high block rate when it comes to direct malware downloads. *Trustwave* easily achieves its tenth VBWeb certification.

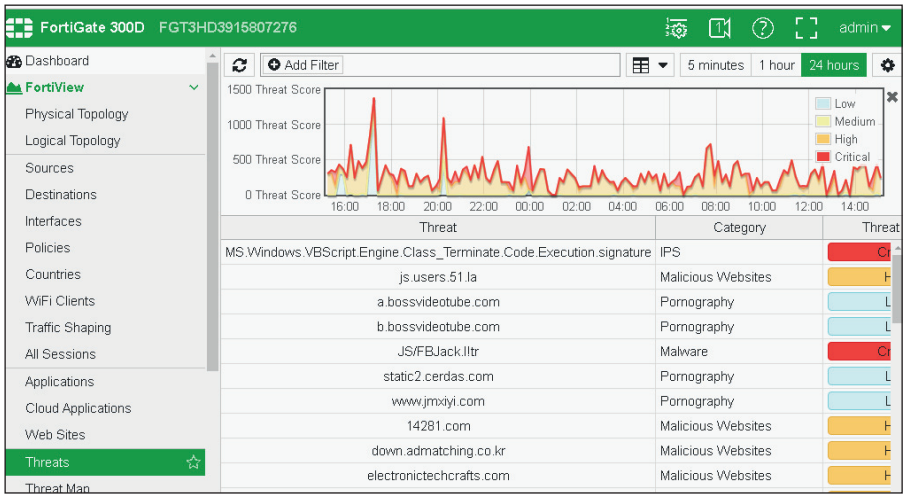
APPENDIX: THE TEST METHODOLOGY

The test ran from 11 March to 2 April 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.

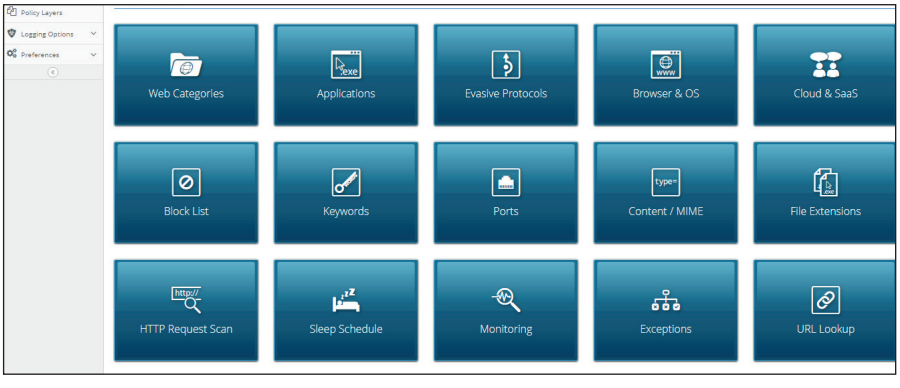
When our systems deemed the response sufficiently likely to fit one of various definitions of 'malicious', we made the same request in the same browser a number of times, each with one of the participating products in front of it. The traffic to the filters was replayed from our cache within seconds 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.

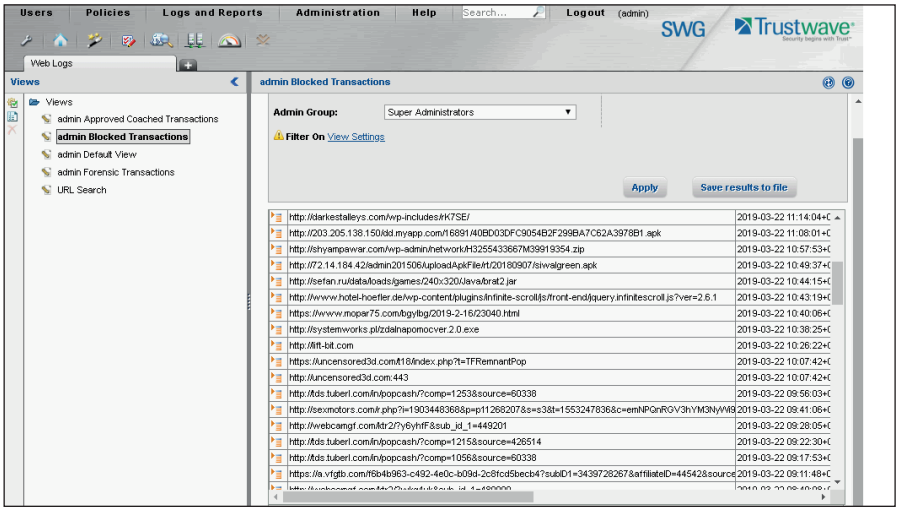
In this test, we checked products against 355 drive-by downloads (exploit kits) and 1,561 direct malware downloads. To qualify for a VBWeb award, the weighted



Fortinet FortiGate.



iBoss.



Trustwave Secure Web Gateway.

average catch rate of these two 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

Tel: +44 (0)1235 555139 Email: editor@virusbulletin.com

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