

## VBWEB COMPARATIVE REVIEW SUMMER 2019

*Martijn Grooten & Adrian Luca*

Together with email<sup>1</sup>, 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.

<sup>1</sup> 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/>.

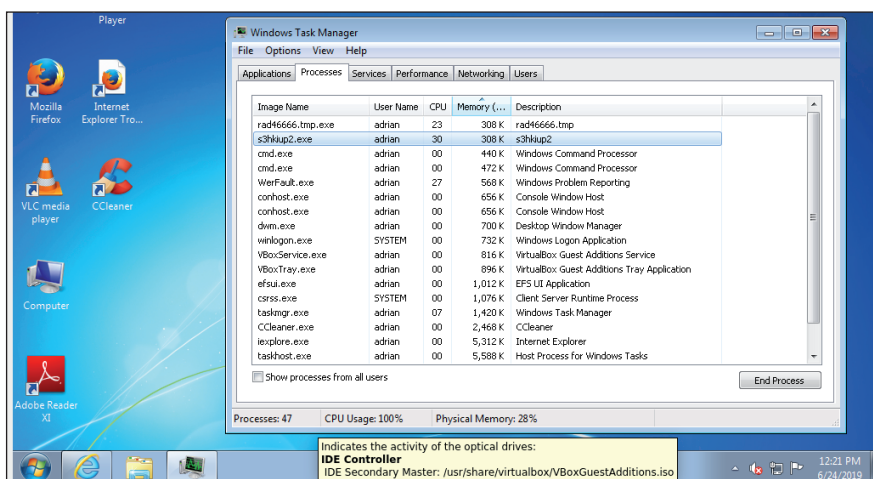
## THE SUMMER 2019 THREAT LANDSCAPE

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<sup>2</sup> 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

<sup>2</sup> <https://blog.malwarebytes.com/threat-analysis/2019/06/greenflash-sundown-exploit-kit-expands-via-large-malvertising-campaign/>.



*Infection attempt following successful execution of the Rig exploit kit.*

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 Trolldesh. 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<sup>3</sup>, 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 in this test, all exploit kits were blocked, meaning that the weighting would not have made a difference.

### Fortinet FortiGate

|                                        |        |
|----------------------------------------|--------|
| <b>Drive-by download rate</b>          | 100.0% |
| <b>Malware block rate</b>              | 99.5%  |
| <b>Phishing block rate</b>             | 95.2%  |
| <b>Cryptocurrency miner block rate</b> | 100.0% |
| <b>False positive rate</b>             | 0.0%   |



<sup>3</sup> The requests are replayed in near real time.

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

|                                        |        |
|----------------------------------------|--------|
| <b>Drive-by download rate</b>          | 100.0% |
| <b>Malware block rate</b>              | 99.3%  |
| <b>Phishing block rate</b>             | 96.9%  |
| <b>Cryptocurrency miner block rate</b> | 100.0% |
| <b>False positive rate</b>             | 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.

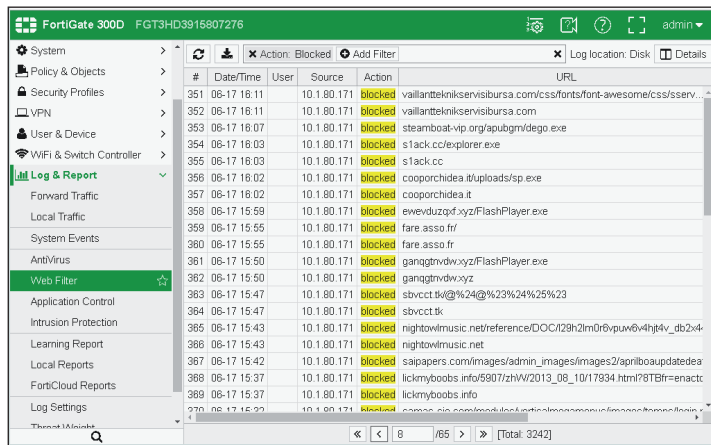
## APPENDIX: THE TEST METHODOLOGY

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.

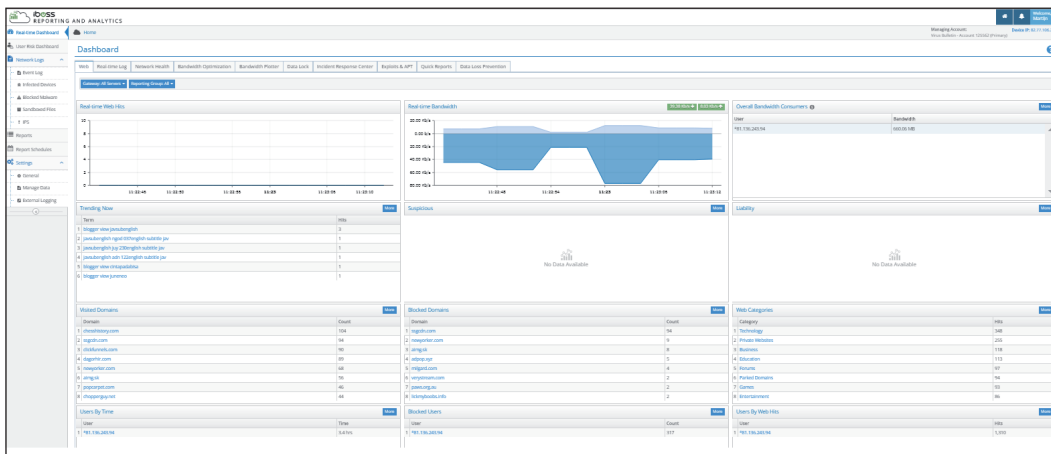
When our systems deemed the response sufficiently likely to fit one of various definitions of 'malicious', we made the same request in the same browser a number of times, each with one of the participating products in front of it. The traffic to the filters was replayed from our cache within seconds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



*Fortinet FortiGate.*

*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, Ionuț 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](mailto:editor@virusbulletin.com)**

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