JUNE 2018

virus BULLETIN

Covering the global threat landscape

VBWEB COMPARATIVE REVIEW SUMMER 2018

Martijn Grooten & Adrian Luca

Together with email[1], web is one of the major vectors through which organizations and individuals get infected with malware. Despite a decline in activity, exploit kits remain the most prominent web-based threat and are a reminder that browsers and browser plug-ins should take absolute priority when it comes to patching: exploit kits almost always exploit vulnerabilities for which a patch has been made available.

But because people do make mistakes, and organizations find it hard always to patch software right away, web security products provide an important extra layer of defence.

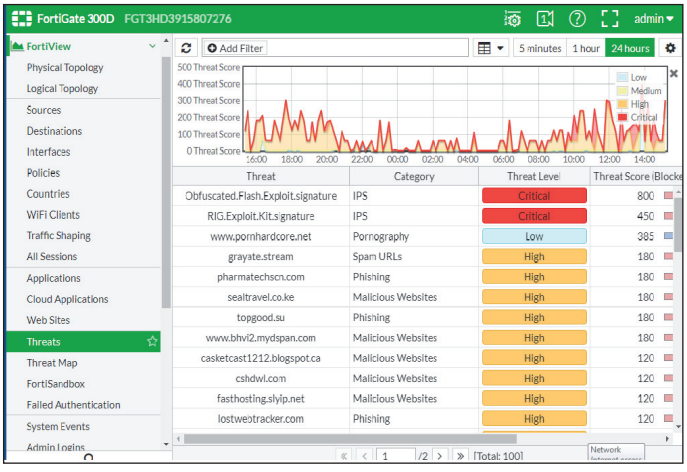
[1] See the regular VBSpam reports on the email-based threat landscape and email security products' ability to protect email accounts: https://www.virusbulletin.com/testing/vbspam/.

THE MAY 2018 THREAT LANDSCAPE

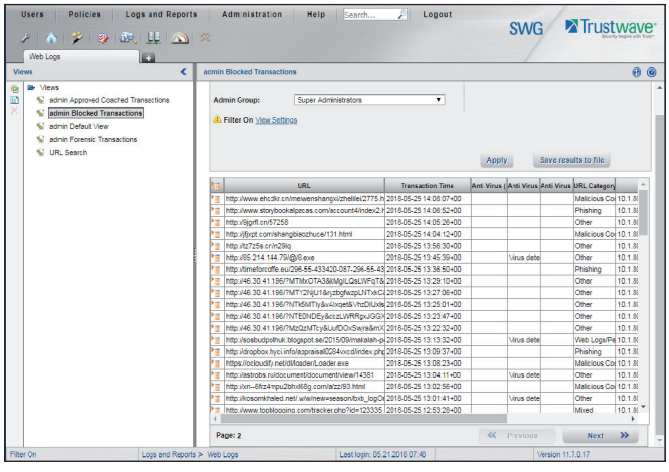
Two kits continue to dominate the global exploit kit landscape: Rig and Grandsoft, both of which are served via a number of different campaigns. A single campaign often serves different kinds of malware to different victims, and though cryptocurrency miners remain popular among cybercriminals, we continue to see more traditional and more serious threats, such as banking trojans and ransomware, being served.

Of course, cryptocurrency mining is also performed via malicious and/or compromised websites. We do not make the blocking of such threats a requirement to achieve VBWeb certification as there are legitimate sites that perform this kind of activity; nevertheless, we were pleased to find that all solutions in our test (including those being tested privately) blocked 100% of cryptocurrency miners.

As in the previous report, we continue to see threats being delivered via HTTPS. Though the privacy implications of an organization intercepting HTTPS for its employees should be well understood, it is important to note that not doing so



FortiGate interface.



Trustwave Secure Web Gateway interface.

ISSN 1749-7027

would result in a not insignificant amount of malicious web traffic bypassing the security product in place.

RESULTS

Fortinet FortiGate

Drive-by download rate	100.0%
Malware block rate	98.7%
Weighted average	99.9%
Potentially malicious rate	97.9%
Cryptocurrency miner block rate	100.0%
False positive rate	0.00%

In yet another test, *Fortinet*'s *FortiGate* appliance blocked every one of the hundreds of drive-by downloads it was served, showing continued excellence when it comes to blocking this type of threat.

With a weighted average block rate of 99.9%, we are pleased to award *Fortinet* its eighth VBWeb award.

Trustwave Secure Web Gateway

Drive-by download rate	100.0%
Malware block rate	98.9%
Weighted average	99.9%
Potentially malicious rate	93.8%
Cryptocurrency miner block rate	100.0%
False positive rate	0.00%

Trustwave's *Secure Web Gateway* continues its excellent performance on our test bed, once again blocking all exploit kits – no trivial achievement given how such kits constantly evolve in an attempt to stay one step ahead of the security vendors.

With a weighted average block rate of 99.9%, yet another VBWeb award is well deserved by *Trustwave*.

APPENDIX 1: THE TEST METHODOLOGY

The test ran from 16 to 31 May 2018, 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 291 drive-by downloads (exploit kits) and 1419 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 243 URLs that we deemed '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 decided to include it in this 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.

APPENDIX 2: 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: Scott James, Tony Oliveira, Adrian Luca, Ionuţ Răileanu, Chris Stock

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Developer: Lian Sebe

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

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