APRIL 2018

virus BULLETIN

Covering the global threat landscape

VBWEB COMPARATIVE REVIEW SPRING 2018

Martijn Grooten & Adrian Luca

Exploit kits are making a bit of a comeback. Certainly, they aren't as prevalent as they were a few years ago, during the days of Blackhole and later Angler, but there are a number of active kits exploiting vulnerabilities in browsers and browser plug-ins (most notably *Adobe*'s *Flash Player*) to infect users with various kinds of malware.

In recent months, a second trend has widely been reported where, rather than websites attempting to serve malware, they run JavaScript inside the browser to mine for cryptocurrencies, most often Monero.

Though far less damaging than actual malware attacks, such in-browser mining costs electricity and slows down devices and is thus considered undesirable by many users and organizations.

Most security products thus aim to (and claim to) block such attacks, and we were pleased to find, when running the spring 2018 VBWeb test, that this was indeed the case for almost all cases of cryptocurrency mining – showing that web security products also protect the end-user against this type of threat.

FILTERING HTTP AND HTTPS TRAFFIC

Until now, the VBWeb test reports have looked at products' ability to scan and, if deemed necessary, block unencrypted HTTP traffic. Blocking this kind of traffic at the gateway level is technically easy and hardly controversial.

Yet there is a growing trend for websites – including many sites that deliver malware – to be served over HTTPS, which ensures an end-to-end encrypted connection between the browser and the server. That doesn't mean that it is impossible for a security product positioned in between the browser and the web server to scan the network traffic, but it does require a 'tweak' in the browser or the operating system[1].

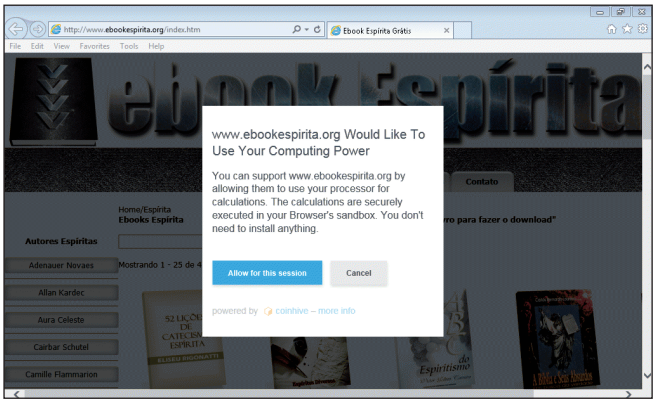
All the products we tested supported the scanning of HTTPS, and we managed to integrate HTTPS scanning into the various proxies in our test network. This allowed us to include encrypted traffic in our tests and thus cover an even wider range of attacks.

The decision as to whether it is right for an organization to scan HTTPS traffic is not for us to make. The security case is fairly clear, but there is privacy to consider too. We think that, if the employee is informed about the scanning and if they have alternative ways of accessing the internet[2], then it is certainly permissible for an organization to install the relevant root certificates on company devices and thus have a security product that scans even the encrypted web traffic.

IN-BROWSER CRYPTOCURRENCY MINING

The main trend in cybercrime over the last few months has been the massive increase in various kinds of cryptocurrency mining on the desktop, on mobile devices and, through

[1] More specifically, the addition of a root certificate.
[2] Personal mobile devices make this an easily satisfied criterion.



A site asks the user's permission to perform mining.

ISSN 1749-7027

JavaScript, in the browser. While there are cases where this is done with the explicit permission of the user (for example as an alternative way for a site or service to generate income), when done without the user's permission it is considered by many to be a malicious activity.

The case against in-browser cryptocurrency mining is subtle though, especially given that the activity stops when the browser or tab is closed and given that no personal data is stolen. As such, while we found many cases of in-browser mining, we decided not to include them in the 'drive-by download' or 'malware' categories, which we reserve for more harmful activities.

However, we were pleased to note that in all but a few cases, the products participating in both the public and private tests blocked in-browser mining activity.

THE SPRING 2018 THREAT LANDSCAPE

Rig has been the most active exploit kit for quite some time – in this test we recorded no fewer than four different Rig campaigns, delivering various kinds of malware including Bunitu, Ramnit and Ursnif, as well as various cryptocurrency miners. Unlike in-browser miners, such miners do stay on the system even after a connection has been closed[3].

We also saw instances of the Kaixin and Bloodlust campaigns, delivering malware like Quantloader and Gh0st RAT.

As before, the test also included malware downloaded directly, as well as 'potentially malicious' cases where, for one of various reasons, a malicious payload wasn't served, but enough of the delivery took place to reason that a malicious payload was likely to have been served under different circumstances. This also included the download of some malicious *Office* documents sent as links in spam emails; our system isn't set up to execute the full infection chain, which often requires human interaction.

[3] This is not the only reason we include them in the drive-by download category though: most drive-by downloads deliver the payload to the machine encrypted (and, in some cases, no file ever exists on the machine). We reason that if an exploit kit is able to run code on a machine, it is 'game over'.

RESULTS

Fortinet FortiGate

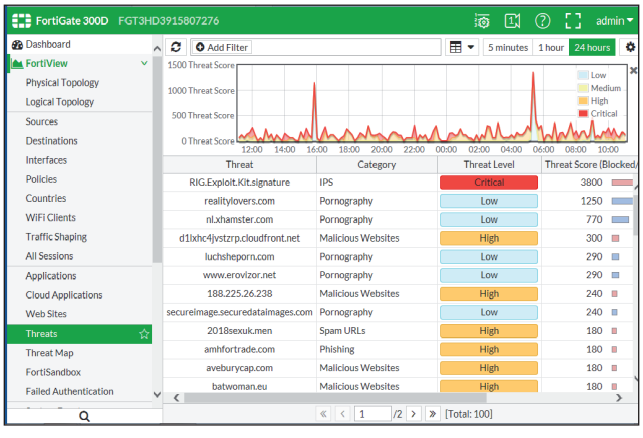
Drive-by download rate: 100.0%
Malware block rate: 98.3%
Weighted average: 99.8%
Potentially malicious rate: 98.5%
False positive rate: 0.0%

Once again, *Fortinet*'s *FortiGate* appliance blocked all of the almost 600 drive-by download cases, showing that even if some browsers within an organization are slightly behind in patching vulnerabilities, *FortiGate* is there to prevent infections from happening. It also blocked almost all of the direct malware downloads before they made it onto the endpoint – thus taking a significant load off an endpoint anti-virus product.

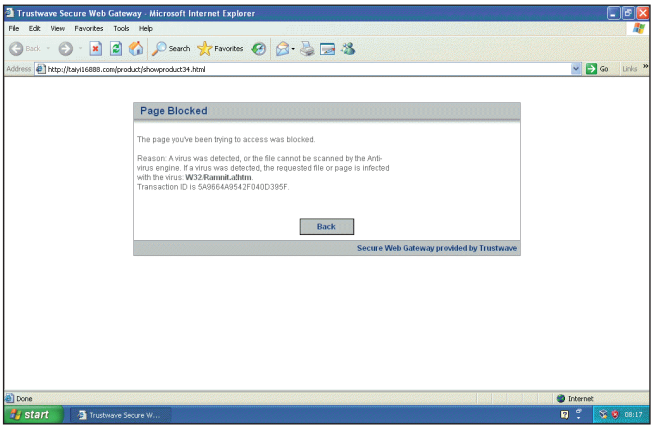
With a weighted average block rate of 99.8%, we are pleased to award *Fortinet* its seventh VBWeb award.

Trustwave Secure Web Gateway

Drive-by download rate: 100.0%
Malware block rate: 98.8%
Weighted average: 99.9%
Potentially malicious rate: 90.7%
False positive rate: 0.0%



FortiGate interface.



Trustwave Secure Web Gateway interface.

The small comeback made by exploit kits didn't cause any problems for *Trustwave*'s *Secure Web Gateway*: whether it was one of the various Rig campaigns, Kaixin or Bloodlust, *Trustwave* blocked them all. The same was true for almost all direct malware downloads, resulting in a 99.9% average block rate.

As such, yet another VBWeb award is well deserved by *Trustwave*'s developers.

APPENDIX: THE TEST METHODOLOGY

The test ran from 19 February to 7 March 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 571 drive-by downloads (exploit kits) and 423 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 335 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.

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, Ionuț 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/