DECEMBER 2017

virus BULLETIN

Covering the global threat landscape

VBWEB COMPARATIVE REVIEW AUTUMN 2017

Martijn Grooten & Adrian Luca

Recently, researchers[1] reported continued activity of the Kaixin exploit kit – a threat that had gone unnoticed for some time, no doubt in part due to its specific geo-targeting of China.

Kaixin is notable because it still exploits vulnerable versions of the Java browser plug-in – something which other exploits stopped doing after modern browsers essentially killed the plug-in[2]. But, as we have seen repeatedly this year, not every individual or organization patches their systems – and at least in the case of some organizations, where there is a need to support legacy systems, the reasons for not doing so may arguably be valid.

This is why it's important for organizations to have reliable protection of their HTTP traffic: to guard against attackers exploiting those imperfections in our networks.

Once again, this VBWeb test demonstrates that there are multiple solutions available that will provide ample protection of HTTP traffic and do a great job of protecting against both drive-by downloads and direct malware downloads that could do serious damage to the network behind it.

MULTIPLE SOLUTIONS TO THE SAME THREAT

During November 2017, a number of web security products were run in *Virus Bulletin*'s test lab and exposed to various real-time, web-based threats, including exploit kits and direct malware downloads. *Virus Bulletin* applies the same rule to all of its tests: each participating vendor must decide prior to the start of the test whether they want the results of the test to be made public, or whether they want to keep the results private, for internal use as quality assurance. In this test two vendors opted to go public with their results, while another four were tested privately.

The products blocked between 90 and 100 per cent of both exploit kits and direct malware downloads. While this demonstrates that products are doing a great job of blocking malware, the details show that there are differences between them: a web security gateway can help a lot, but some can help more than others.

THE WEB THREAT LANDSCAPE, AUTUMN 2017

Throughout 2017, RIG has remained the most prevalent exploit kit by some distance, with others either having disappeared or, as in the case of Kaixin, having become very localized threats. If you did get infected through an exploit kit this year, it was most likely to have been RIG.

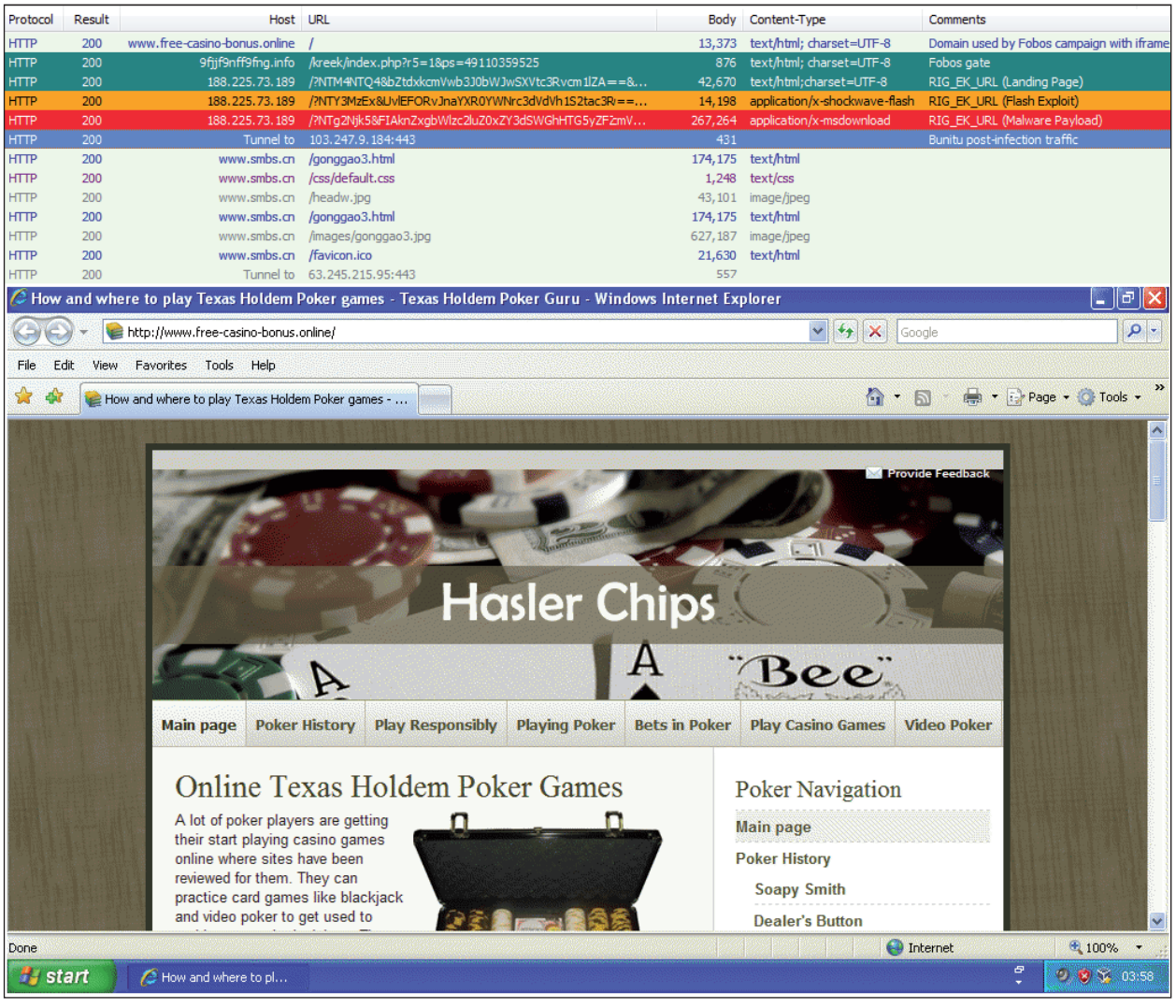
RIG uses various campaigns though, each with slightly different characteristics, thus making it far more than a single threat. This was reflected in the variety of payloads we saw, which included various kinds of ransomware and other kinds of malware.

Since a successful exploit kit often delivers malware that is only decrypted locally, the actual payload wouldn't make a difference to the tested products, and different victims of the same threat may receive different payloads. Examples of payloads seen in this test include the Ramnit banking trojan and the Bunitu proxy trojan. In keeping with its targeting of long unpatched machines, among the malware Kaixin was seen to deliver was the older Symmi trojan.

One new 'threat' that has emerged this autumn is that of in-browser cryptocurrency mining, sometimes also referred to as 'drive-by mining'[3]. This uses JavaScript embedded in

[1] http://www.malware-traffic-analysis.net/2017/11/17/index.html; http://www.nao-sec.org/2017/11/analyzing-kaixin-exploit-kit.html.
[2] https://www.theverge.com/2016/1/28/10858250/oracle-java-plugin-deprecation-jdk-9.
[3] https://blog.malwarebytes.com/cybercrime/2017/11/a-look-into-the-global-drive-by-cryptocurrency-mining-phenomenon/.

ISSN 1749-7027



RIG's Fobos campaign surreptitiously delivering the Bunitu malware.

a website to mine for a cryptocurrency (typically monero, which can be mined effectively in JavaScript) while the user is visiting the website.

The quotes around 'threat' are intentional: from a security point of view, nothing bad happens; the only detrimental effects for the user are extra CPU usage and, with that, the cost of both electricity and wear and tear. Drive-by mining is performed on compromised sites as well as by sites whose owners see it as an extra way to generate income from visitors.

There is an ongoing debate among security vendors as to whether this activity should be blocked. For this reason, as well as the lack of actual malicious activity taking place, we decided that drive-by mining was not suitable for this test report. We did, however, check a few instances of websites performing drive-by mining and noticed that products (those tested both publicly and privately) are not currently blocking them uniformly.

RESULTS

Fortinet FortiGate

Drive-by download rate: 100.0%

Malware block rate: 98.3%

Weighted average: 99.8%

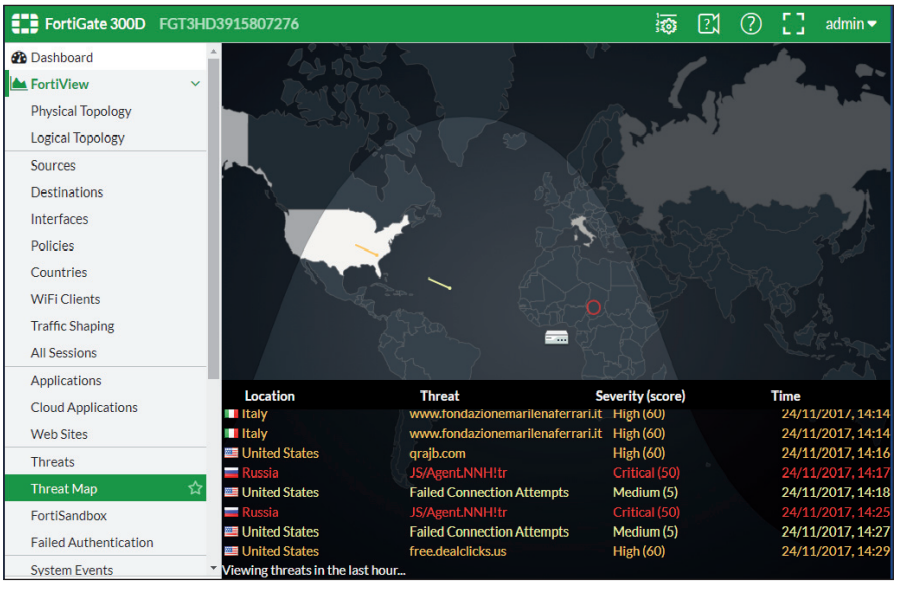
Potentially malicious rate: 97.5%

Fortinet's *FortiGate* appliance once again blocked all of the more than 500 exploit kits seen in this test, thus showing that the gateway product continues to provide an excellent first line of defence. The detection rate of direct malware downloads was very good too, with only a handful of them missed.

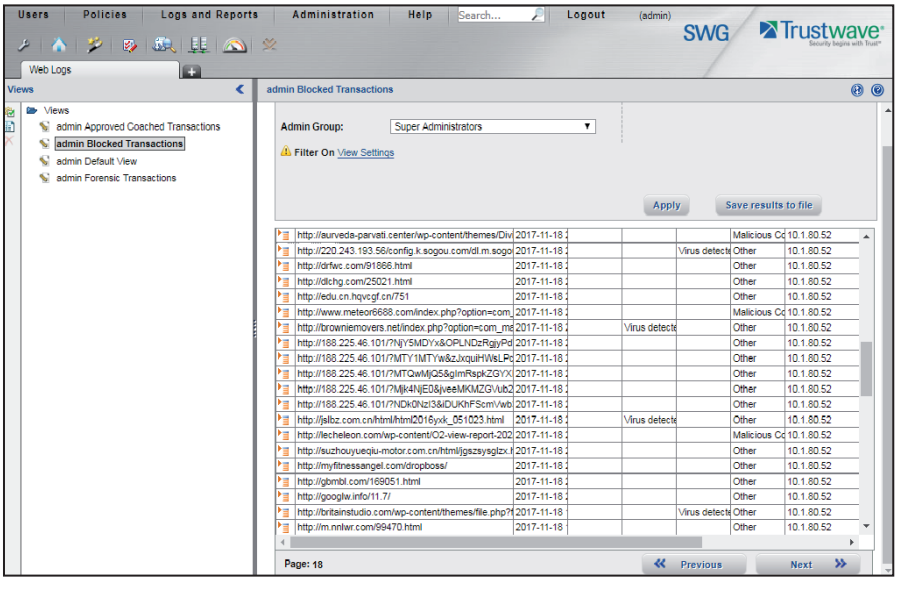
Thus, for keeping up with the threat landscape and for the continued protection it offers, *Fortinet* is well deserving of another VBWeb award and we are pleased to strongly recommend the product to organizations looking to mitigate web-based threats.

Trustwave Secure Web Gateway

Drive-by download rate: 100.0%
Malware block rate: 97.1%
Weighted average: 99.7%
Potentially malicious rate: 97.7%



FortiGate interface.



Trustwave interface.

Exploit kits remain no problem for *Trustwave*'s *Secure Web Gateway*: once again, not a single one was missed by the product, while more than 97% of direct malware downloads – where a web gateway is the first line of defence before an endpoint security product will try to block the threat – were blocked too. But more than its excellent performance in this test, it is the product's strong performance over several tests that the product's developers should be proud of.

As such, *Trustwave* fully deserves another VBWeb award and we are pleased to strongly recommend the product to organizations looking to mitigate web-based threats.

APPENDIX: THE TEST METHODOLOGY

The test ran from 10 November to 24 November 2017, 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 534 drive-by downloads (exploit kits) and 962 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 440 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 machines 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/