OCTOBER 2019

virus BULLETIN

Covering the global threat landscape

VBWEB COMPARATIVE REVIEW AUTUMN 2019

Martijn Grooten & Adrian Luca

Together with email[1], 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.

[1] See the regular VBSpam reports on the email-based threat landscape and email security products' ability to protect email accounts.

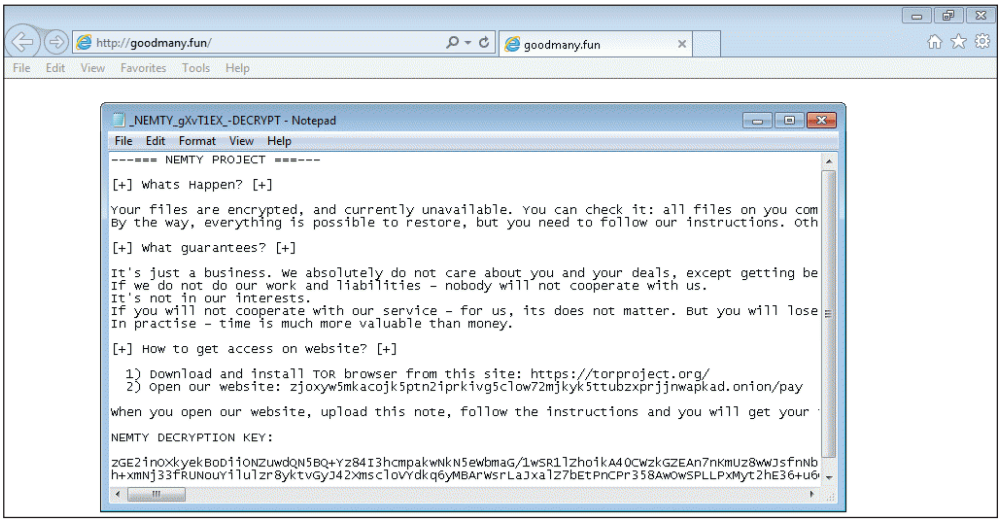
THE AUTUMN WEB 2019 THREAT LANDSCAPE

2019 continues to be more interesting than previous years when it comes to exploit kits. More than half a dozen kits are currently active. In this test, we caught six active exploit kits: Rig, Spelevo, Fallout, Underminder, Radio and Lewd.

Radio is a new kit that was first discovered by *nao_sec* in July[2], while Lewd was first reported on *Twitter* in September[3]. There is a good chance that Lewd, like the Lord exploit kit discovered by *Virus Bulletin* earlier this year[4], is not actually an exploit kit but a standalone use of an exploit to facilitate a drive-by download. We saw this push the Quasar RAT.

Other malware downloaded by the various exploit kits included Nemty, Vidar, Smokeloader, PsiXBot and DanaBot.

[2] https://nao-sec.org/2019/07/weak-dbd-attack-with-radioek.html
[3] https://twitter.com/tkanalyst/status/1171818815493201925
[4] https://www.virusbulletin.com/blog/2019/08/virus-bulletin-researcher-discovers-new-lord-exploit-kit/



The Nemty ransomware as downloaded by the Radio exploit kit.

ISSN 1749-7027

We also saw more than 900 instances of malware downloads, including Emotet, Locky, Nanobot, Ursnif and Remcos RAT. Thankfully, the tested products had very few problems blocking malware in any of these categories.

As in the Summer 2019 report[5], the test also confirmed that products had few problems blocking phishing pages.

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[6], 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.

Fortinet FortiGate

Drive-by download rate	100.0%
Malware block rate	99.1%
Phishing block rate	98.1%
Cryptocurrency miner block rate	100.0%
False positive rate	0.0%

Fortinet's *FortiGate* appliance continues its unbroken run of VBWeb awards going several years. It blocked all drive-by download cases, missing fewer than one in 100 direct malware downloads, and with over 98 per cent of phishing sites blocked, this kind of malicious site isn't a big problem for *FortiGate* either.

iBoss

Drive-by download rate	100.0%
Malware block rate	99.6%
Phishing block rate	98.6%
Cryptocurrency miner block rate	100.0%
False positive rate	2.0%

iBoss continues its impressive VBWeb performance by blocking all drive-by download cases (exploit kits) in this test, as well as all but a few directly downloaded malware samples. *iBoss* also blocked almost 99 per cent of phishing sites. A third VBWeb certification is thus well deserved.

APPENDIX: THE TEST METHODOLOGY

The test ran from 29 August 2019 to 15 September 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.

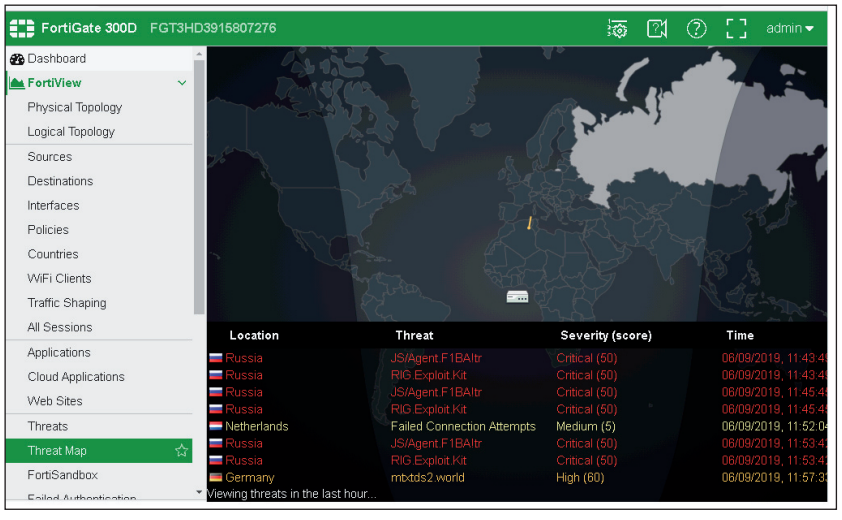
When our systems deemed the response sufficiently likely to fit one of various definitions of 'malicious', we made the same request in the same browser a number of times, each with one of the participating products in front of it. The traffic to the filters was replayed from our cache within seconds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

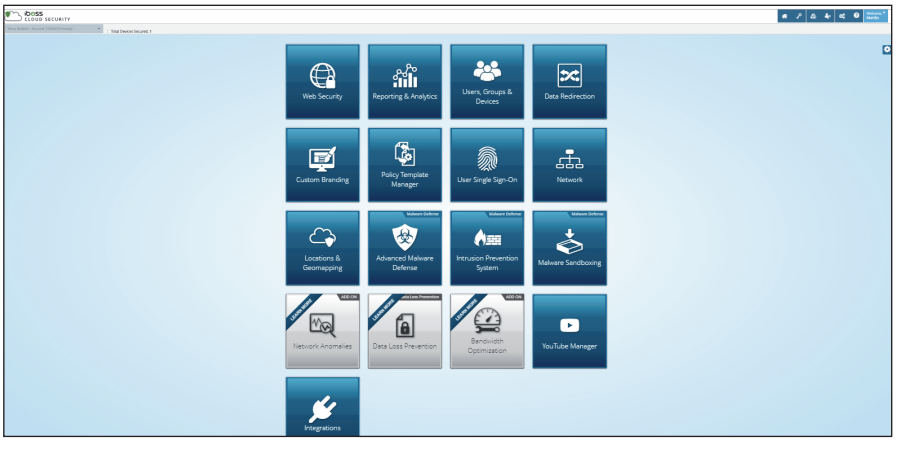
In this test, we checked products against 609 drive-by downloads (exploit kits), 926 direct malware downloads and 364 phishing sites, a category which also includes sites that

[5] https://www.virusbulletin.com/virusbulletin/2019/07/vbweb-comparative-review/

[6] The requests are replayed in near real time.



Fortinet FortiGate.



iBoss.

trick the user into calling a phone number. 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 80%.

The test focused on both HTTP and HTTPS traffic. It did not look at extremely targeted attacks or possible vulnerabilities in the products themselves.

Data from the test was provided by various public sources as well as an API provided by *Active Defense*.

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

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

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