FEBRUARY 2017

virus BULLETIN

Covering the global threat landscape

VBWEB COMPARATIVE REVIEW FEBRUARY 2017

Martijn Grooten & Adrian Luca

Malicious websites continue to be one of the most important infection vectors for malware, which today often means ransomware. A recent study showed that 70 per cent of businesses affected with ransomware ended up paying the ransom, which in many cases cost tens of thousands of dollars[1].

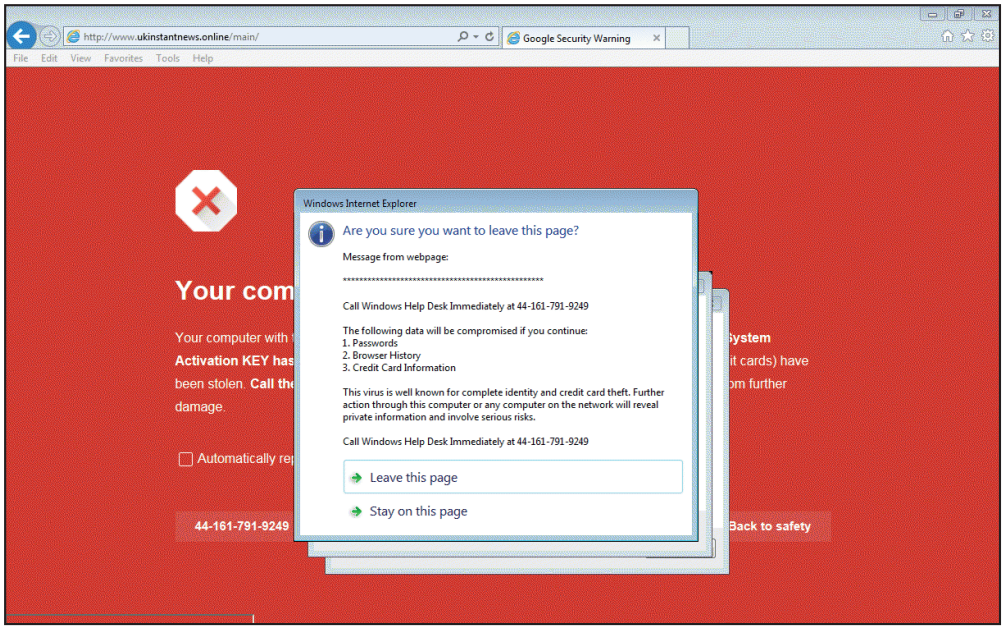
However, the same study also showed that half of businesses were not hit by ransomware at all – suggesting that these organizations must be doing something right.

[1] https://www.virusbulletin.com/blog/2017/01/ransomware-not-problem-half-businesses/

This report looks at one important thing all businesses can do to make their users more secure: install a web security product.

Virus Bulletin does not suggest that the use of a web security solution – or any other security product for that matter – alone will work as some kind of silver bullet against all threats. It is also essential that businesses ensure that their browsers and their add-ons are fully up to date. User education can also go a long way towards improving an organization's security. However, no matter how hard one tries, there will always one browser that falls a patch behind, or one user who stubbornly insists on downloading that free program to make their job easier.

For such all-too-real scenarios, web security products can offer important protection – and this report demonstrates that there are products on the market that are very good at this.



Scam seen during the test period (November 2016).

ISSN 1749-7027

ONE THREAT, MULTIPLE SOLUTIONS

During November and December 2016, 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. While some vendors elected to be privately tested (with the results for these products not being made public), this report features those who submitted to the public test. (For obvious reasons, once a test has started, participants may not switch from 'public' to 'private' testing or vice versa.)

There were two vendors that opted to enter their products publicly, and their decision proved to be justified. Both *Fortinet*'s *FortiGate* appliance and *Trustwave*'s *Secure Web Gateway* product blocked all the live exploit kits they were exposed to, as well as all but a handful of direct malware downloads. (It should be noted that the latter threat is less of an issue in both qualitative[2] and quantitative terms, hence such cases are given a lower weight in the test.)

Products were also exposed to a number of malicious URLs that ended up not delivering a payload – a not uncommon occurrence in the complicated world of web-based malware. Of course, it is not essential for products to block these failed infection attempts, yet blocking them indicates a good level of proactive detection. Both *FortiGate* and *Trustwave SWG* blocked more than 98 per cent of such failed attempts, and there is reason to believe that they would have blocked the remaining cases had they resulted in actual malicious traffic. On top of this, neither product mistakenly alerted on any of the legitimate sites we exposed them to. Both products earn the VBWeb certification and we are happy to recommend either of them to organizations looking to mitigate web-based threats.

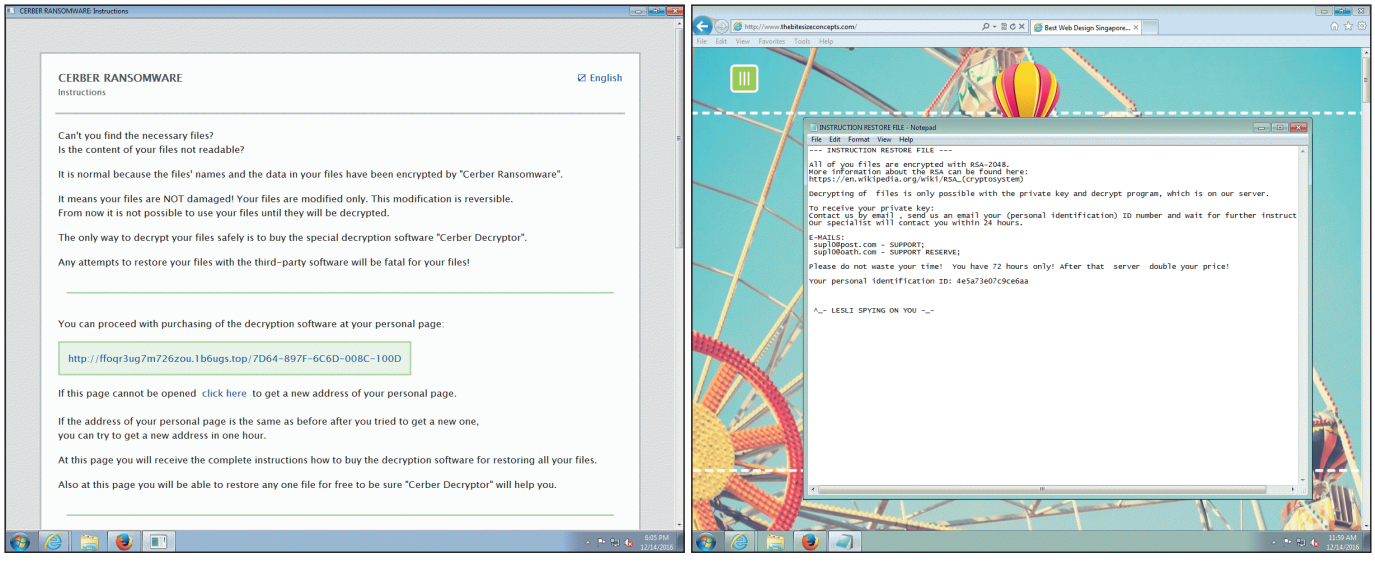
[2] Because the malware is stored on the local disk before being opened, there is a better chance of an endpoint security product blocking the threat.

THE CHANGING WEB THREAT LANDSCAPE

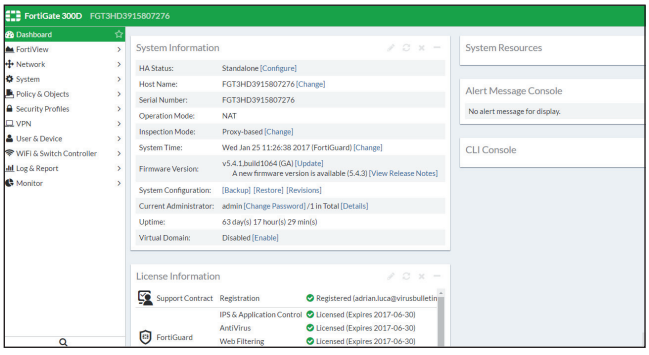
Since we last published a web security product review in April 2016, the exploit kit landscape has changed significantly. Some of the exploit kits commonly seen back then have disappeared – some more mysteriously than others (Angler, most notably, disappeared last spring when its authors were arrested as part of a law enforcement action against the authors of the Lurk trojan).

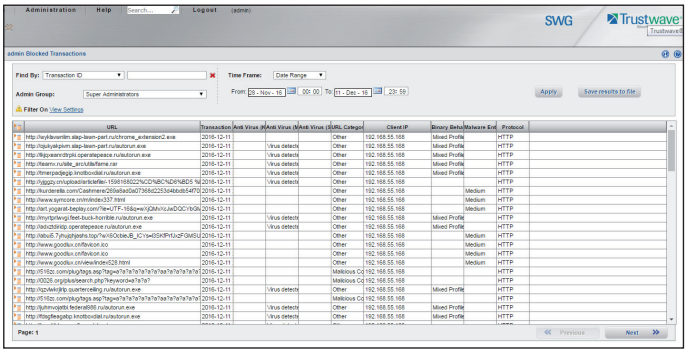
These days, RIG (which comes in a number of variants) and Sundown are known to be the most prominent kits, and this was what we observed in our tests. The payloads delivered by these exploit kits continue to vary and may depend, among other things, on the victim's location. More often than not in our test, this payload was ransomware, with Cerber, Locky and CryptoMix all seen on numerous occasions.

Drive-by downloads are the main component of our 'VBWeb' tests, as at the moment they are by far the most prevalent and most dangerous threats on the web. They are not the only threat though: occasionally, people are tricked into downloading a file directly from the Internet which subsequently turns out to be malicious. Such 'direct



Examples of machines being infected with the Cerber (left) and CryptoMix (right) ransomware. In both cases, they were infected on 14 December 2016, via the Pseudodarkleech campaign of the RIG-V exploit kit.





download' cases were counted with a total weight of 10 per cent in this test – among the malware downloaded this way were Ramnit, Pony and Nitrol, as well as various kinds of ransomware (including Locky).

RESULTS

Fortinet FortiGate

Drive-by download rate: 100.0%
Malware block rate: 99.3%
Weighted average: 99.9%
Potentially malicious rate: 98.5%

We know that *Fortinet* dedicates a lot of resources to threat research – research that undoubtedly is used to help keep its range of products, including the *FortiGate* appliance, up to date with the changes in the threat landscape.

Indeed, the recent changes in the exploit landscape posed no problem for the appliance: the product blocked all 108 infection attempts through drive-by downloads, giving it a 100% catch rate. It also blocked all but three direct malware downloads, and proactively it blocked more than 98% of potentially malicious cases – it would likely also have blocked the remaining cases had actual malicious traffic been sent.

As such, *Fortinet* is well deserving of its third VBWeb award.

Trustwave Secure Web Gateway

Drive-by download rate: 100.0%
Malware block rate: 96.7%
Weighted average: 99.7%
Potentially malicious rate: 98.1%

Trustwave's *SpiderLabs* blog is a very important source of information on the latest research on exploit kits – and of course, the research the company performs contributes to keeping its products, including the *Secure Web Gateway* virtual appliance, up to date.

Having already performed exceptionally well the last time we put it to the test, this time *SWG* blocked all infection attempts via exploit kits. It also blocked all but a handful of direct malware downloads and, proactively, more than 98% of potentially malicious cases – it would likely also have blocked the remaining cases had actual malicious traffic been sent.

Trustwave is thus the deserving recipient of its second VBWeb award.

APPENDIX: THE TEST METHODOLOGY

The test ran from 28 November to 14 December 2016, 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 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 108 drive-by downloads (exploit kits) and 274 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 268 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.

We found that, in practice, we were far more likely to receive a malicious response for the *Windows 7* machines using either version of *Internet Explorer*; hence most cases that ended up in the test used this configuration. Of course that does not mean that *Windows XP* is more secure – on the contrary, it has not received any security updates since April 2014 – rather that exploit kit authors consider infecting the more modern operating systems to be of greater value.

Editor: Martijn Grooten

Chief of Operations: John Hawes

Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Ionuţ Răileanu, Chris Stock

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Developer: Lian Sebe

Consultant Technical Editor: Dr Morton Swimmer

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

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