AUGUST 2016

virus BULLETIN

Covering the global threat landscape

VBWEB REVIEW: TRUSTWAVE SECURE WEB GATEWAY

Martijn Grooten & Adrian Luca

Rig, Angler, Nuclear, Magnitude. Few people outside security circles will have heard of them, yet they are behind what is possibly the worst large-scale malware plague ever: encryption ransomware. In particular, these are exploit kits which, when embedded into websites (often through compromised ads), check your browser for vulnerabilities and exploit them to push malicious software onto your computer.

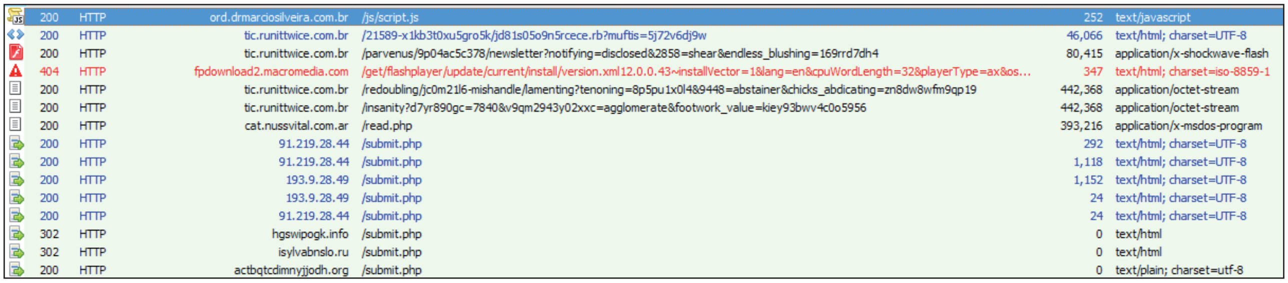
Indeed, when, during our tests, we made requests to websites serving exploit kits, we found our test machines infected with ransomware such as Locky, Teslacrypt and Cerber, as well as other kinds of malware, including Bedep and Zbot variants. Many individuals and organizations have found themselves infected with malware in this way, and many have ended up paying hefty ransoms to attackers to get their files back.

Patching remains a great way to reduce the chances of being infected, but in decades of IT security we've learned that users often don't do what's best for them or their employer. As a result, many organizations rely on web security products that run on the gateway and filter web content for malicious responses.

In *Virus Bulletin*'s VBWeb tests we measure how effective products are at blocking malicious web traffic. In this report we focus on one particular product: *Trustwave*'s *Secure Web Gateway*.

THE TEST METHODOLOGY

During the test period, which ran from 1 to 11 April 2016, we used a number of public sources, combined with the results of our own research, to open URLs that we had reason to believe could serve a malicious response in one of our test browsers, selected at random. When our systems deemed the response likely enough to fit one of various definitions of 'malicious', we made the same request in the same browser a number of times, each time with one of the participating products in front of it. The traffic to the filters was replayed from our cache. Note that we did not need to know at this point whether the response was actually malicious, meaning that our test didn't depend on instances already known to the industry or community. During the review of the corpus days later, we analysed the responses and only included cases in which the traffic was indeed malicious.



```
200  HTTP      ord.drmarciosilveira.com.br  /js/script.js                                                                                          252  text/javascript
200  HTTP          tic.runittwice.com.br  /21589-x1kb3t0xu5gro5k/jd81s05o9n5rcece.rb?muftis=5j72v6dj9w                                           46,066  text/html; charset=UTF-8
200  HTTP          tic.runittwice.com.br  /parvenus/9p04ac5c378/newsletter?notifying=disclosed&2858=shear&endless_blushing=169rrd7dh4               80,415  application/x-shockwave-flash
404  HTTP     fpdownload2.macromedia.com  /get/flashplayer/update/current/install/version.xml12.0.0.43~installVector=1&lang=en&cpuWordLength=32&playerType=ax&os...     347  text/html; charset=iso-8859-1
200  HTTP          tic.runittwice.com.br  /redoubling/jc0m21l6-mishandle/lamenting?tenoning=8p5pu1x0l4&9448=abstainer&chicks_abdicating=zn8dw8wfm9qp19  442,368  application/octet-stream
200  HTTP          tic.runittwice.com.br  /insanity?d7yr890gc=7840&v9qm2943y02xxc=agglomerate&footwork_value=kiey93bwv4c0o5956                    442,368  application/octet-stream
200  HTTP           cat.nussvital.com.ar  /read.php                                                                                         393,216  application/x-msdos-program
200  HTTP                   91.219.28.44  /submit.php                                                                                           292  text/html; charset=UTF-8
200  HTTP                   91.219.28.44  /submit.php                                                                                         1,118  text/html; charset=UTF-8
200  HTTP                    193.9.28.49  /submit.php                                                                                         1,152  text/html; charset=UTF-8
200  HTTP                    193.9.28.49  /submit.php                                                                                            24  text/html; charset=UTF-8
200  HTTP                   91.219.28.44  /submit.php                                                                                            24  text/html; charset=UTF-8
302  HTTP                 hgswipogk.info  /submit.php                                                                                             0  text/html
302  HTTP                  isylvabnslo.ru  /submit.php                                                                                             0  text/html
200  HTTP        actbqtcdimnyjjodh.org  /submit.php                                                                                             0  text/plain; charset=utf-8
```

Nuclear traffic followed by Locky traffic.

ISSN 1749-7027

While we registered various types of malicious responses, including spam/scam sites and phishing pages, we decided to concentrate only on drive-by downloads, where the URL was an HTML page that forced the browser to download and/or install malware in the background. This is by far the biggest threat at the moment and makes unprotected web browsing more dangerous than ever.

In this test, we checked products against 439 cases, including 105 drive-by downloads (exploit kits) and 100 direct malware downloads that were all served in real time, while the malicious server was live. We also checked the product against 234 URLs that we call 'potentially malicious'. These are URLs for which we have 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.

The test focused on unencrypted HTTP traffic. It did not look at very targeted attacks or vulnerabilities in the products themselves.

TEST MACHINES

We used two virtual machines, selected at random, from which to make requests. On each machine, an available browser was also selected at random.

We found that, in practice, we were far more likely to receive a malicious response for the *Windows 7* machine using either version of *Internet Explorer*, hence most of the cases that ended up in the test used this configuration.

Windows XP Service Pack 3 Home Edition 2002 (x86)

This machine had the following software installed:

- *Adobe Flash Player 12 Active X* 12.0.0.38
- *Adobe Flash Player 12* plug-in 12.0.0.43
- *Adobe Reader XI* 11.0.0.0
- *Apple Application Support* 2.0.1
- *Apple QuickTime* 7.70.80.34
- *Oracle Java 7* update 51 7.0.510
- *VLC* media player 2.1.3

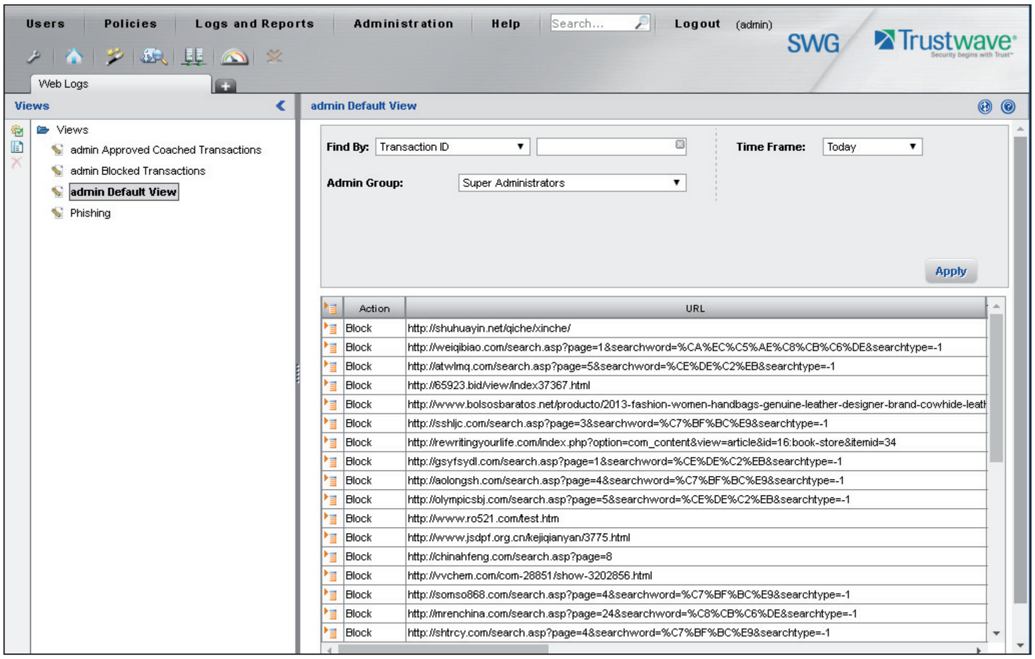
The following browsers were installed:

- *Windows Internet Explorer* 8 (8.0.6001.18072)
- *Mozilla Firefox* 28.0

Windows 7 Service Pack 1 Ultimate 2009 (x86)

This machine had the following software installed:

- *Adobe Flash Player 13 Active X* 13.0.0.182
- *Adobe Flash Player 13* plug-in 13.0.0.182



Find By: Transaction ID

Time Frame: Today

Admin Group: Super Administrators

Action	URL
Block	http://shuhuayin.net/qiche/xinche/
Block	http://weiqibiao.com/search.asp?page=1&searchword=%CA%EC%C5%AE%C8%CB%C6%DE&searchtype=-1
Block	http://atwlmq.com/search.asp?page=5&searchword=%CE%DE%C2%EB&searchtype=-1
Block	http://65923.bid/view/index37367.html
Block	http://www.bolsosbaratos.net/producto/2013-fashion-women-handbags-genuine-leather-designer-brand-cowhide-leath
Block	http://sshljc.com/search.asp?page=3&searchword=%C7%BF%BC%E9&searchtype=-1
Block	http://rewritingyourlife.com/index.php?option=com_content&view=article&id=16:book-store&itemid=34
Block	http://gsyfsydl.com/search.asp?page=1&searchword=%CE%DE%C2%EB&searchtype=-1
Block	http://aolongsh.com/search.asp?page=4&searchword=%C7%BF%BC%E9&searchtype=-1
Block	http://olympicsbj.com/search.asp?page=5&searchword=%CE%DE%C2%EB&searchtype=-1
Block	http://www.ro521.com/test.htm
Block	http://www.jsdpf.org.cn/kejiqianyan/3775.html
Block	http://chinahfeng.com/search.asp?page=8
Block	http://vvchem.com/com-28851/show-3202856.html
Block	http://somso868.com/search.asp?page=4&searchword=%C7%BF%BC%E9&searchtype=-1
Block	http://mrenchina.com/search.asp?page=24&searchword=%C8%CB%C6%DE&searchtype=-1
Block	http://shtrcy.com/search.asp?page=4&searchword=%C7%BF%BC%E9&searchtype=-1

Trustwave: excellent protection.

- *Adobe Reader XI* 11.0.0.0
- *Apple Application Support* 2.0.1
- *Apple QuickTime* 7.70.80.34
- *Piriform CCleaner* 5.0.4
- *Oracle Java 7* update 51 7.0.510
- *Microsoft* .NET framework 4.5.2 (4.5.51.209)
- *Microsoft Silverlight* 5.1.10411.0
- *VLC* media player 2.1.3

The following browsers were installed:

- *Windows Internet Explorer* 11 (11.0.09600.17843 update 11.0.20)
- *Windows Internet Explorer* 9 (9.0.8112.16421 update 9.0.37)
- *Mozilla Firefox* 28.0

Trustwave Secure Web Gateway

Drive-by download rate: 95.2%

Potentially malicious rate: 95.3%

Trustwave is one of the industry leaders when it comes to web security. Indeed, *Trustwave*'s *SpiderLabs* blog is one of the resources we turn to for the latest research on exploit kits, so we were expecting the company's *Secure Web Gateway* product to do a very good job at blocking these threats.

vb VERIFIED WEB virusbtn.com

We were not disappointed. The appliance, set up as an explicit proxy in our test lab, blocked more than 95 per cent of exploit kits – and did equally well at blocking potentially malicious URLs proactively. Given how quickly exploit kits change, and how difficult it is for organizations to make sure all endpoints are fully patched, this is a big deal.

There are many things users can and should do to mitigate drive-by downloads, patching being the most important. But for those organizations that cannot trust their users always to follow best security practice (which is probably all organizations), *Trustwave*'s *Secure Web Gateway* removes 95 per cent of drive-by downloads. And that makes a huge difference.

Of course, *Trustwave* earns a very well deserved VBWeb award for its performance.

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 Fax: +44 (0)1865 543153

Email: editorial@virusbtn.com Web: https://www.virusbtn.com/