MAY 2017

virus BULLETIN

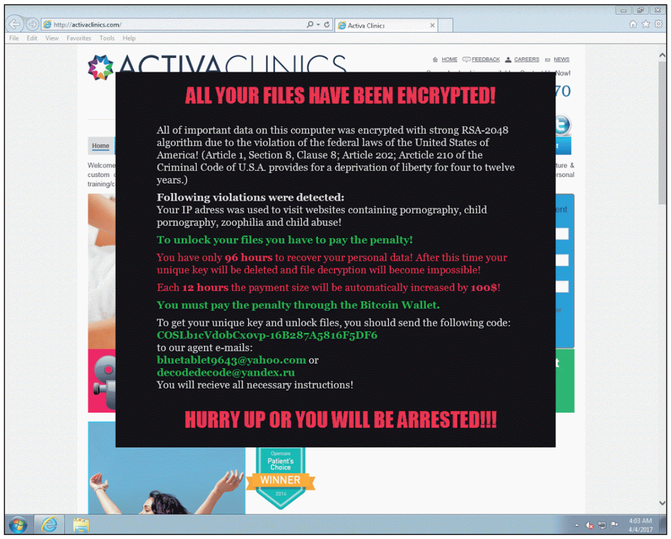
Covering the global threat landscape

VBWEB COMPARATIVE REVIEW SPRING 2017

Martijn Grooten & Adrian Luca

With a few notable exceptions (such as the infamous WannaCry[1] 'ransomworm' spread via SMB), users get infected with malware either via malicious emails or via malicious websites, both of which delivery methods come with their own advantages for the attacker: malicious emails work well against a fully patched system, but if a browser or its plug-ins are vulnerable, malicious websites have the advantage of not requiring any user interaction.

In recent months, many security researchers have noted a decrease in the use of malicious websites as a malware delivery system, attackers instead tending to favour email – a trend we have also observed in our lab at *Virus Bulletin*.



ALL YOUR FILES HAVE BEEN ENCRYPTED!

All of important data on this computer was encrypted with strong RSA-2048 algorithm due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Arcticle 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:
Your IP adress was used to visit websites containing pornography, child pornography, zoophilia and child abuse!

To unlock your files you have to pay the penalty!

You have only **96 hours** to recover your personal data! After this time your unique key will be deleted and file decryption will become impossible!

Each **12 hours** the payment size will be automatically increased by **100$**!

You must pay the penalty through the Bitcoin Wallet.

To get your unique key and unlock files, you should send the following code:
COSLb1cVdobCxovp-16B287A5816F5DF6
to our agent e-mails:
bluetablet9643@yahoo.com or
decodedecode@yandex.ru
You will recieve all necessary instructions!

HURRY UP OR YOU WILL BE ARRESTED!!!

Matrix ransomware infection.

However, such trends are rarely, if ever, permanent, and they do not mean the web has all of a sudden become safe. There are still exploits out there (RIG in particular remains very active), and 'unprotected' browsing remains as bad an idea as ever.

We thus continue to recommend patching operating systems, browsers and plug-ins as the first and most important step in fending off web-based malware. But, as this test shows, web security products are an important second layer of protection that, in a world where things are never perfect, can make a huge difference.

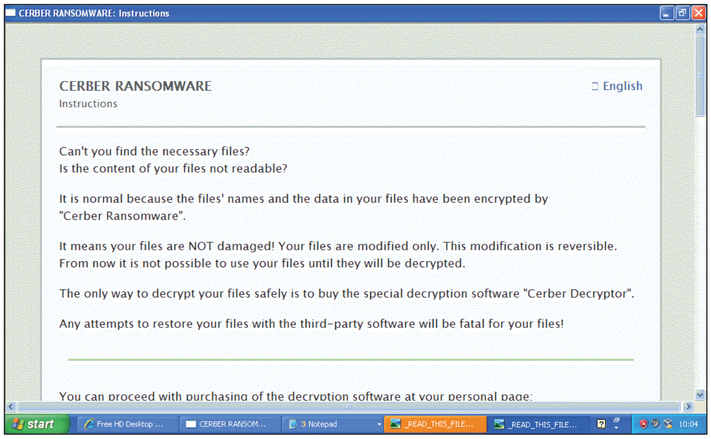
ONE THREAT, MULTIPLE SOLUTIONS

During March and April 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. While some vendors elected to be tested privately (with the results for these products not being made public), this report features those that 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.)

As on previous occasions, there were two vendors that opted to enter their products publicly, and once again their decision proved to be justified. Both *Fortinet*'s *FortiGate* appliance and *Trustwave*'s *Secure Web Gateway* (*SWG*) 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 and quantitative terms – since the malware is stored on the local disk before being opened, there is a better chance of an endpoint security product blocking the threat – hence such cases are given a lower weight in the test.) While we will not comment publicly on the individual performances of those products that opted to be tested privately, we note that not all of them managed to block all the live exploit kits they were exposed to, thus underlining

[1] https://www.virusbulletin.com/blog/2017/may/modern-security-software-not-powerless-against-threats-wannacry/

ISSN 1749-7027


CERBER RANSOMWARE: Instructions

CERBER RANSOMWARE
Instructions

Can't you find the necessary files?
Is the content of your files not readable?

It is normal because the files' names and the data in your files have been encrypted by "Cerber Ransomware".

It means your files are NOT damaged! Your files are modified only. This modification is reversible. From now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "Cerber Decryptor".

Any attempts to restore your files with the third-party software will be fatal for your files!

You can proceed with purchasing of the decryption software at your personal page:

Cerber ransomware infection.

the fact that a 100% block rate was no trivial achievement for the two products in the public 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, and not doing so is not taken as a sign that the product wouldn't have blocked the attempts in the real world. However, blocking them indicates a good level of proactive detection, which is an interesting data point for those trying to understand the way web-based threats are fought.

Both *FortiGate* and *Trustwave SWG* blocked the overwhelming majority 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 thus earn the VBWeb certification and we are happy to recommend either of them to organizations looking to mitigate web-based threats.

THE WEB THREAT LANDSCAPE, SPRING 2017

The disappearance of prominent exploit kits such as Angler, Nuclear and (at least temporarily) Sundown has made RIG the most prominent exploit kit by far. All the exploit kit cases in our test were RIG; they used the EITest and PseudoDarkleech campaigns and the Seamless, GoodMan and HookAds gates. We recorded a few failed cases of the Terror exploit kit in the category of potentially malicious cases.

Web-based threats continue to spread ransomware: we noticed various exploit kits dropping ransomware such as Cerber, Matrix and Ransomlocker, as well as the downloader Smoke Loader, which in turn would have downloaded other malware.

The direct malware downloads included dozens of different malware families such as Ramnit, Sality and Bladabindi, as well as several downloaders, which in turn would have downloaded other kinds of malware.

RESULTS

Fortinet FortiGate

Drive-by download rate: 100.0%

Malware block rate: 97.8%

Weighted average: 99.8%

Potentially malicious rate: 98.6%

False positives: 0.0%

vb VERIFIED WEB virusbtn.com

With three VBWeb awards already under its belt, *Fortinet*'s *FortiGate* appliance seems, so far, to have had little problem in keeping apace with the changes in the threat landscape.

Indeed, this month the *FortiGate* appliance once again blocked all infection attempts through drive-by downloads, resulting in a 100% catch rate. It also blocked all but six direct malware downloads – and proactively it blocked more than 98% of potentially malicious cases.

Of course, this means *Fortinet* is well deserving of its fourth VBWeb award.

Trustwave Secure Web Gateway

Drive-by download rate: 100.0%

Malware block rate: 97.8%

Weighted average: 99.8%

Potentially malicious rate: 96.4%

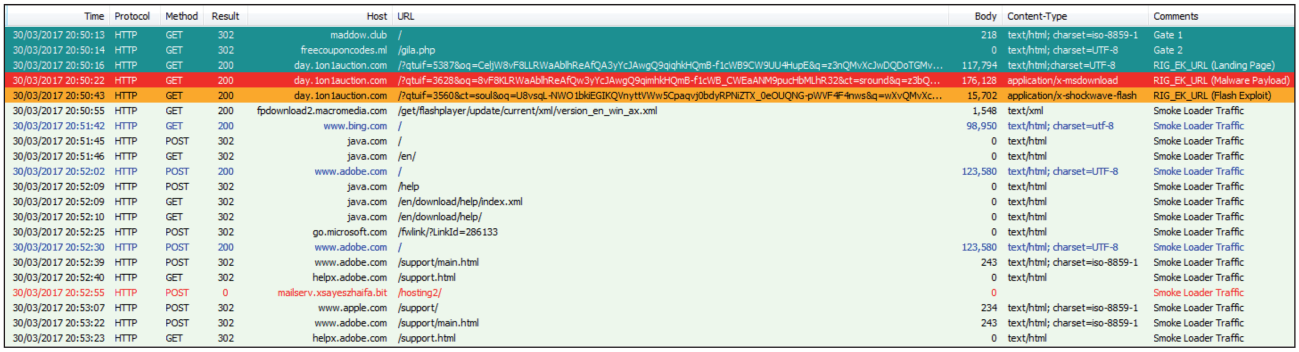
False positives: 0.0%

vb VERIFIED WEB virusbtn.com

Trustwave's *Secure Web Gateway* virtual appliance has only appeared twice before in our public tests, but has put in exceptional performances and earned VBWeb awards on both occasions.

On this occasion, *SWG* once again blocked all infection attempts via exploit kits. What's more, it also blocked all but six direct malware downloads – and proactively it blocked more than 96% of potentially malicious cases.

Trustwave is therefore once again a worthy winner of a VBWeb award.



Time	Protocol	Method	Result	Host	URL	Body	Content-Type	Comments
30/03/2017 20:50:13	HTTP	GET	302	maddow.club	/	218	text/html; charset=iso-8859-1	Gate 1
30/03/2017 20:50:14	HTTP	GET	302	freecouponcodes.ml	/gila.php	0	text/html; charset=UTF-8	Gate 2
30/03/2017 20:50:16	HTTP	GET	200	day.1on1auction.com	/?qtuif=5387&oq=CeljW8vF8LLRWaAblhReAfQA3yYcJAwgQ9qiqhkHQmB-f1cWB9CW9UU4HupE&q=z3nQMvXcJwDQDoTGMv...	117,794	text/html;charset=UTF-8	RIG_EK_URL (Landing Page)
30/03/2017 20:50:22	HTTP	GET	200	day.1on1auction.com	/?qtuif=3628&oq=8vF8KLRWaAblhReAfQw3yYcJAwgQ9qimhkHQmB-f1cWB_CWEaANM9pucHbMLhR32&ct=sround&q=z3bQ...	176,128	application/x-msdownload	RIG_EK_URL (Malware Payload)
30/03/2017 20:50:43	HTTP	GET	200	day.1on1auction.com	/?qtuif=3560&ct=soul&oq=U8vsqL-NWO1bkiEGIKQVnyttVWw5Cpaqvj0bdyRPNiZTX_0eOUQNG-pWVF4F4nws&q=wXvQMvXc...	15,702	application/x-shockwave-flash	RIG_EK_URL (Flash Exploit)
30/03/2017 20:50:55	HTTP	GET	200	fpdownload2.macromedia.com	/get/flashplayer/update/current/xml/version_en_win_ax.xml	1,548	text/xml	Smoke Loader Traffic
30/03/2017 20:51:42	HTTP	GET	200	www.bing.com	/	98,950	text/html; charset=utf-8	Smoke Loader Traffic
30/03/2017 20:51:45	HTTP	POST	302	java.com	/	0	text/html	Smoke Loader Traffic
30/03/2017 20:51:46	HTTP	GET	302	java.com	/en/	0	text/html	Smoke Loader Traffic
30/03/2017 20:52:02	HTTP	POST	200	www.adobe.com	/	123,580	text/html; charset=UTF-8	Smoke Loader Traffic
30/03/2017 20:52:09	HTTP	POST	302	java.com	/help	0	text/html	Smoke Loader Traffic
30/03/2017 20:52:09	HTTP	GET	302	java.com	/en/download/help/index.xml	0	text/html	Smoke Loader Traffic
30/03/2017 20:52:10	HTTP	GET	302	java.com	/en/download/help/	0	text/html	Smoke Loader Traffic
30/03/2017 20:52:25	HTTP	POST	302	go.microsoft.com	/fwlink/?LinkId=286133	0	text/html	Smoke Loader Traffic
30/03/2017 20:52:30	HTTP	POST	200	www.adobe.com	/	123,580	text/html; charset=UTF-8	Smoke Loader Traffic
30/03/2017 20:52:39	HTTP	POST	302	www.adobe.com	/support/main.html	243	text/html; charset=iso-8859-1	Smoke Loader Traffic
30/03/2017 20:52:40	HTTP	GET	302	helpx.adobe.com	/support.html	0	text/html	Smoke Loader Traffic
30/03/2017 20:52:55	HTTP	POST	0	mailserv.xsayeszhaifa.bit	/hosting2/	0		Smoke Loader Traffic
30/03/2017 20:53:07	HTTP	POST	302	www.apple.com	/support/	234	text/html; charset=iso-8859-1	Smoke Loader Traffic
30/03/2017 20:53:22	HTTP	POST	302	www.adobe.com	/support/main.html	243	text/html; charset=iso-8859-1	Smoke Loader Traffic
30/03/2017 20:53:23	HTTP	GET	302	helpx.adobe.com	/support.html	0	text/html	Smoke Loader Traffic

RIG EK followed by Smoke Loader traffic.

APPENDIX: THE TEST METHODOLOGY

The test ran from 27 March to 10 April 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 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 116 drive-by downloads (exploit kits) and 270 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 244 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 be given a malicious response for the *Windows 7* machine using *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 regular 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

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

Consultant Technical Editor: Dr Morton Swimmer

© 2017 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England

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

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