

Covering the global threat landscape

VBWEB REVIEW: FORTINET FORTIGATE

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 thus 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

#	Result	Protocol	Host URL	Bod	Content-Type					
<>	200	HTTP	hec5f.gca0b.p8c4e1ebi.tf0p.9765d26.g1afy.0005o.la.zi14osu39k6n.copiesout.link /	1,16	1 text/html					
X	200	HTTP	5e956.1f7f.m7c.0889.ld048fao.d514ai.w1c3caj.v6i.zi14osu39k6n.copiesout.link /	71	5 application/x-shockwa					
Ż	200	HTTP	5e956.1f7f.m7c.0889.ld048fao.d514ai.w1c3caj.v6i.zi14osu39k6n.copiesout.link /	71	5 application/x-shockwa					
<>	200	HTTP	2a32i.t56.70190.pcdt.i0852v.ka6611o.b73ax.ed.b75d.zi14osu39k6n.copiesout.link /	23,25	9 text/html					
Z	200	HTTP	hec5f.gca0b.p8c4e1ebi.tf0p.9765d26.g1afy.0005o.la.zi14osu39k6n.copiesout.link /5943942e3		5 application/x-shockwa					
Ż	200	HTTP	hec5f.gca0b.p8c4e1ebi.tf0p.9765d26.g1afy.0005o.la.zi14osu39k6n.copiesout.link /5943942e3		5 application/x-shockwa					
<>	200	HTTP	hec5f.gca0b.p8c4e1ebi.tf0p.9765d26.g1afy.0005o.la.zi14osu39k6n.copiesout.link /favicon.ico) text/html					
<>	200	HTTP	148.251.205.98 /b7caf32376	148.251.205.98 /b7caf3237e7b3bbdacdea5ab/f6d9d345 64,932 text/html 148.251.205.98 /457354611a6253872890bc3c4c310d3 595,456 text/html 148.251.205.98 /457354611a6253872890bc3c4c310d3 595,456 text/html 148.251.205.98 /b7caf3237e7b3bbdacdea5ab/f6d9d345 64,932 text/html 148.251.205.98 /b7caf3237e7b3bbdacdea5ab/f6d9d345 64,932 text/html tele-channel.com /wp-admin/maint/wcspng.php 10 text/html multbrandphone.com /wp-content/t/temes/storefront/wcspng.php 10 text/html vtechehop.net /wcspng.php 10 text/html						
<>	200	HTTP	148.251.205.98 /45f354611	1a62538f2af90bc8c4c310d3 595,45	5 text/html					
<>	200	HTTP								
<>	200	HTTP								
	200	HTTP		/maint/wcspng.php 1) text/html; charset=U					
3	200	HTTP		it/themes/storefront/wcspng.php 1) text/html; charset=U					
	200	HTTP								
	200	HTTP								
	200	HTTP	shirongfeng.cn /images/lurd) text/html					
Tra	nsformer	r Heade	rs TextView SyntaxView ImageView HexView WebView Auth 📆 F	FiddlerScript 📃 Log 📃 Filters	🔄 🔄 Timeline					
Ca	hing	Cookies	Raw JSON XML Sta	atistics 🕺 Inspectors 🖉 AutoResponder	Compos					
I			Headers	TextView SyntaxView WebForms HexView Auth	Cookies Raw					
dody> JSON XML										
			27cdb6e-ae6d-11cf-96b8-444553540000" allowScriptAccess="always" width="389" ame="movie" Request I	Request Headers (Raw1 Header Defin						
val	ue="http	://5e956.1f	7f.m7c.0889.ld048fao.d514ai.w1c3caj.v6i.zi14osu39k6n.copiesout.link/"> <param get="" htt<="" td=""/> <td colspan="7">GET / HTTP/1.1</td>	GET / HTTP/1.1						
			e">	Client						
			n/x-shockwave-flash" :m7c.0889.ld048fao.d514ai.w1c3cai.v6i.zi14osu39k6n.copiesout.link/" Accept:	Accept: text/html, application/xhtml+xml, */*						
allo	wScript/	Access="alv	ays" width="389" height="351"> <param accept-<="" name="movie" td=""/> <td colspan="7">Accept-Encoding: gzip, deflate</td>	Accept-Encoding: gzip, deflate						
			7f.m7c.0889.ld048fao.d514ai.w1c3caj.v6i.zi14osu39k6n.copiesout.link/"> <param accept-<="" td=""/> <td colspan="7">Accept-Language: en-US</td>	Accept-Language: en-US						
			e"> ment_iiz = function(iocsdd){var oietwp = "",ngihxn = iocsdd.match(/()/g),for (var i = 0; i < User-Ag	User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)						
			p += String fromCharCode(parseInt(ngihxn[i], 21));return oietwp};isfbf[ijz("5e59505b4h")] Miscelland	Miscellaneous						
(jjz				Referer: http://www.sproutgamesz.net/						
				Transport						
			24462029409724404024462020402490090272805080529219220592447955790405856 5555045554455445241932311354251134255504154252312225550415944544524193222052244755572045544554452419322	Connection: Keep-Alive						

Magnitude Exploit Kit traffic followed by Teslacrypt.



we focus on one particular product: *Fortinet*'s *FortiGate* appliance.

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 included cases in which the traffic was indeed malicious.

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.

VBWEB

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.

While one can have a very good web security product that doesn't block any of these, we do believe that blocking them could serve as an indication of a product's ability to block threats proactively, without inspecting the traffic. For some customers this could matter, 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 very targeted attacks or vulnerabilities in the product themselves.

F CRTINET Fort	iGate 3								2:0 Wizard	Video	Help	Logo	
System	C	Add Filter								Log log	cation: Dis	sk 🙋	
Router	# 0	Date/Time	e Severity	Source	Protoco	l User	Action	Count		Attack N	Jame		
Policy & Objects	▶1	08-03 01:48		185.158.152.7	tep		dropped		RIG.Ex	ploit.Kit			
Security Profiles	2	08-02 22:07		74.208.234.19	tcp		dropped		Obfusc	ated.Flas	sh.Exploit		
	3	3 08-02 22:00 ••••• 5.2		5.200.35.239 tcp dropped				RIG.Exploit.Kit					
PN	4	08-02 21:49		185.30.232.53	tcp		dropped		Obfuso	ated.Flas	sh.Exploit		
Iser & Device	5	08-02 21:40		185.30.232.53	top		dropped		Magnit	ude.Explo	oit.Kit		
/iEi Controller	6	08-02 21:08		185.30.232.53	tcp		dropped	ed Magnitude.Exploit.K			oit.Kit		
	7	08-02 17:51		185.158.152.7	tcp		dropped Obfuscated.F			ated.Flas	sh.Exploit		
og & Report	8	08-02 16:42		5.200.35.239	tcp		dropped		RIG.Ex	ploit.Kit			
📲 Traffic Log	9	08-02 16:12		185.30.232.53	tcp		dropped		Obfuse	ated.Flas	sh.Exploit		
- Forward Traffic	10	08-02 13:48		185.30.232.53	tcp		dropped		Magnit	ude.Explo	oit.Kit		
- • Local Traffic	11	08-02 13:36		185.30.232.53	tcp		dropped		Magnitude.Exploit.Kit				
Sniffer Traffic	12	08-02 06:37		188.227.18.241	tep		dropped	RIG.Exploit.Kit					
Event Log	13	08-02 05:01		188.227.18.241	tcp		dropped	pped RIG.Exploit.Kit					
I Security Log													
- AntiVirus													
- • Web Filter												_	
- • Application Control				K 📢 1	/ 1 🚺	🕅 [те	otal: 13]					
	#		1		A	ction		Iropped				_	
📲 Report	Attac	k ID	38920 08-03 01:48 port4		A	Destination		RIG.Exploit.Kit 192.168.55.168 43224					
- • Local	Date/												
- • FortiCloud													
🕎 Log Config	Destin	nation Interface			D								
Monitor	Direct	ion	incoming			Event Type signature							
		ame	tree.goodmoja					72179002					

FortiGate: excellent all-round protection.

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
- 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

Fortinet FortiGate

Drive-by download rate: 87.6% Malware block rate: 98.9% Potentially malicious rate: 96.1%

FortiGate was the only participant in the last VBWeb report and easily achieved a VBWeb award, not least thanks to a near perfect blocking of direct downloads



of malicious files. It did the same again in this test, blocking all but one of these files, thus protecting users and organizations well against supposedly helpful programs that turn out to be a real hindrance.

The product also blocked the vast majority of driveby downloads, missing fewer than one in eight of the exploit kits it was served, and performed really well on blocking potentially malicious URLs too. All in all, a great performance and the appliance fully deserves its second VBWeb award.

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 © 2016 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153 Email: editorial@virusbtn.com Web: https://www.virusbtn.com/