

Bad Sites Botnets CTO Insights Exploits Internet of Things Mac Malware Mobile Social Spam Targeted Attacks Vulnerabilities

[blog.trendmicro.com Sites](#) > [TrendLabs Security Intelligence Blog](#) > [Malware](#) > Fiesta Exploit Kit Spreading Crypto-Ransomware – Who Is Affected?

Apr20 [Fiesta Exploit Kit Spreading Crypto-Ransomware – Who Is Affected?](#)

2:56 am (UTC-7) | by [Brooks Li and Joseph C. Chen \(Threats Analysts\)](#)

[f Share](#) [Recommend 36](#) [Tweet](#)

Exploits kits have long been used to deliver threats to users, but they seem to have gone retro: it was recently being used to deliver fake antivirus malware.

We closely monitor exploit kit activity because of their widespread use (we discussed [their use in malvertising](#) recently), so it was no great surprise to see the Fiesta exploit kit being used to deliver crypto-ransomware. The choice of exploits delivered is broadly in line with other exploit kits. Flash, Internet Explorer, Adobe Reader/Acrobat, and Silverlight are all targeted. (It's worth noting that as is the case in recent attacks, Java is no longer a favored infection vector).

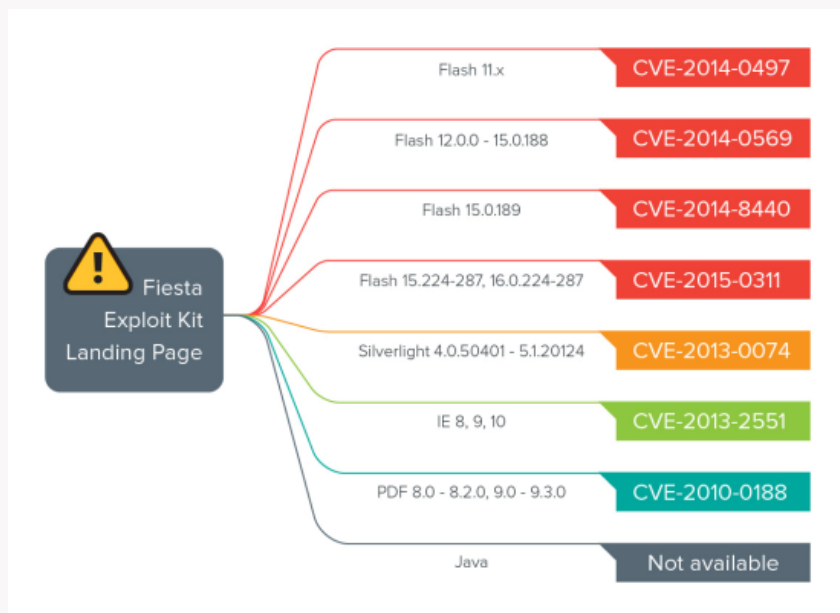


Figure 1. Exploits used by Fiesta

What is interesting is that after March 19, we noticed a change in the malware payloads delivered to victims. Before that date, crypto-ransomware was being delivered to end users. Aside from encrypting the user's files, this particular variant terminates some running processes (Process Explorer, Task Manager, the Command Prompt, Regedit, and Msconfig) so that it cannot be terminated by the user easily. (We detect this as [TROJ\\_CRYPTESLA.CAG.](#))



Search our blog:

## Targeted Attacks

- Operation Pawn Storm Ramps Up its Activities; Targets NATO, White House
- How Targeted Attacks Changed in 2014
- Kjw0rm VBS Malware Tied To Attacks on French TV Station TV5Monde

Bookmark the [Threat Intelligence Resources](#) site to stay updated on valuable information you can use in your APT defense strategy

## Recent Posts

- Latest Flash Exploit in Angler EK Might Not Really Be CVE-2015-0359
- IIS At Risk: The HTTP Protocol Stack Vulnerability
- Resurrection of the Living Dead: The "Redirect to SMB" Vulnerability

## Calendar

April 2015						
S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

« Mar

## Email Subscription

Email Subscription

Your email here

About us





Figure 2. Screenshot of crypto-ransomware

After March 19, Fiesta served up a threat best known from previous years: fake antivirus. Again, it disables some common system tools such as Task Manager, Process Explorer, and Internet Explorer, so that this fake antivirus cannot be easily shut down. It's not clear why the attackers chose to return to this older kind of threat. (This is detected as [TROJ\\_FAKEAV.YSXF.](#))



Figure 3. Screenshot of fake antivirus

#### Who's affected?

Exploit kits are frequently used to spread various threats, so the use of Fiesta to spread both crypto-ransomware and the (seemingly) reborn fake antivirus should not be a great surprise. We decided to use this incident to check trends in exploit kit activity, particularly the levels and distribution of this specific usage of the Fiesta exploit kit in the month of March.

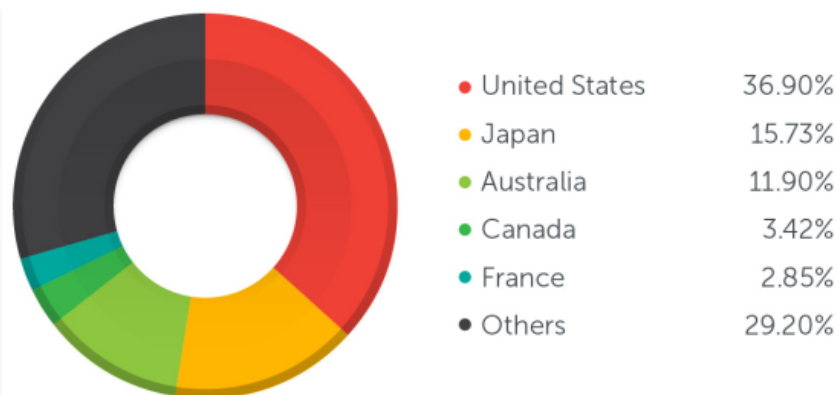


Figure 4. Global distribution of Fiesta Exploit Kit victims in March

In terms of distribution, three countries account for almost two-thirds of the traffic related to this attack: the United States, Japan, and Australia. The United States by itself accounts for more than a third of the traffic, making it the country most affected by this threat.

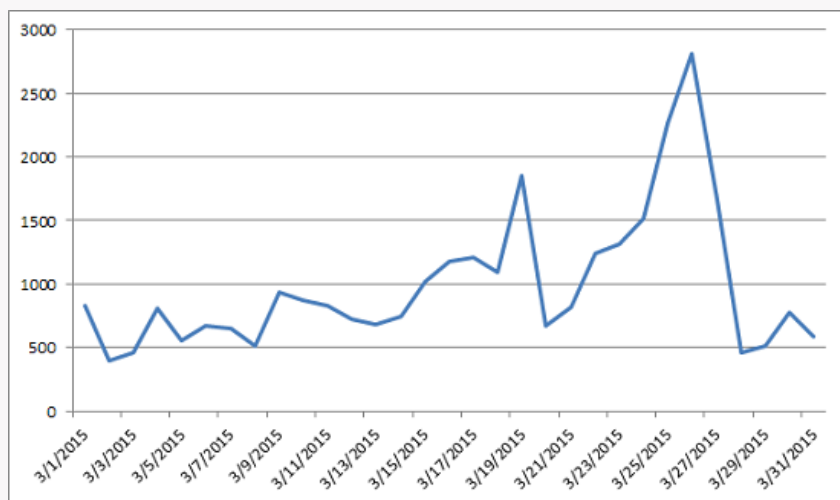


Figure 5. Number of machines affected by Fiesta per day

As for threat activity over time, the overall trend for activity of this exploit kit was gradually upwards. However, this growth was punctuated by several spikes in the month of March. However, the overall threat picture is indicative of a growing crypto-ransomware threat; as we [noted earlier](#) the first quarter of the year has seen many changes in this part of the threat landscape.

#### Best practices

The first step to defend against these attacks is: keep software up to date. By removing the vulnerabilities that an exploit kit targets, users can prevent themselves from becoming the next victims of these attacks.

The Browser Exploit Prevention feature in our endpoint products such as [Trend Micro™ Security](#), [OfficeScan](#), and [Worry-Free Business Security](#) blocks exploits from running at the browser level. In addition, [Trend Micro™ Security](#) software safeguards against malware, phishing, and other Internet threats. Businesses are also protected with Endpoint Security in [Trend Micro™ Smart Protection Suite](#) as it offers multiple layers of protection.

#### Share this article



Get the latest on malware protection from [TrendLabs](#)











This entry was posted on Monday, April 20th, 2015 at 2:56 am and is filed under [Malware](#) . You can [leave a response](#), or [trackback](#) from your own site.



Disqus seems to be taking longer than usual. [Reload?](#)

Without a Trace: Fileless Malware Spotted in the Wild  
Operation Pawn Storm Ramps Up its Activities; Targets NATO, White House

#### Other Trend Micro blogs

-  CTO Insights
-  CounterMeasures Blog
-  Cloud Security Blog
-  Consumerization Blog
-  Fearless Web
-  Internet Safety for Kids & Families
-  Simply Security News
-  Trend Micro Blog [German]
-  TrendLabs Security Blog [Japan]
-  Cloud Security APAC



Do you have a product-related question? [Visit our eSupport website.](#)