TREND MICRO | TrendLabs SECURITY INTELLIGENCE Blog

SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Blog of News Site “The Independent” Hacked, Leads to TeslaCrypt Ransomware

- Posted on:December 8, 2015 at 9:04 am
- Posted in:Bad Sites, Malware
- Author:
  Joseph C Chen (Fraud Researcher)

3

Updated on December 9, 2015, 6:14 PM PST (UTC -8): *We have edited this entry to include more technical details on the incident, including another infection chain.*

As of this writing, the blog portion of the site is now redirecting all users to the main site. A spokesperson for The Independent *has stated that “an advert appearing on that blogsite may have included malware.” They have also added that the the affected site was a “legacy” system that was rarely visited.*

Updated on December 8, 2015, 7:15 PM PST (UTC -8): *We have edited this entry to reflect the current status of communications with* The Independent *and the current threat. As of this writing, the site is still compromised and serving various malware threats to users.*

The blog page of one of the leading media sites in the United Kingdom, *The Independent* has been compromised, which may put its readers at risk of getting infected with ransomware. We have already informed *The Independent* about this security incident. However, the site is still currently compromised and users are still at risk.

It should be noted that only the blog part of the website–which uses WordPress–is impacted; the rest of The Independent's online presence seem unaffected. WordPress is a very popular blogging platform that has seen more than its fair share of attacks and compromises from threat actors and cybercriminals looking to infect users. Other security researchers have noted that this is part of a larger campaign involving compromised WordPress sites.

I stumbled upon this while monitoring the activity of Angler Exploit Kit. Based on my investigation, since at least November 21, the compromised blog page redirected users to pages hosting the said exploit kit. If a user does not have an updated Adobe Flash Player, the vulnerable system will download the Cryptesla 2.2.0 ransomware (detected by Trend Micro as RANSOM_CRYPTESLA.YYSIX).

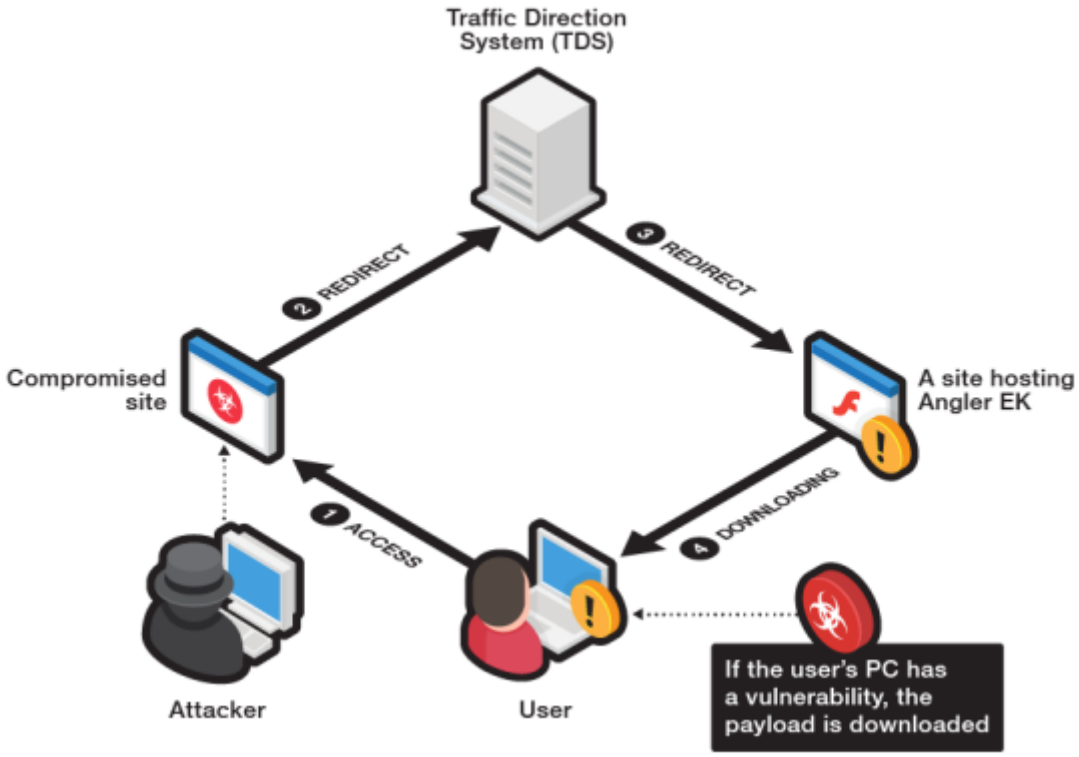

Figure 1. Infection diagram

The malware then changes the extension of encrypted files to ".vvv".

The vulnerability involved in this particular instance is discovered to be CVE-2015-7645. This is also the latest vulnerability we detect to be added to Angler's repertoire.

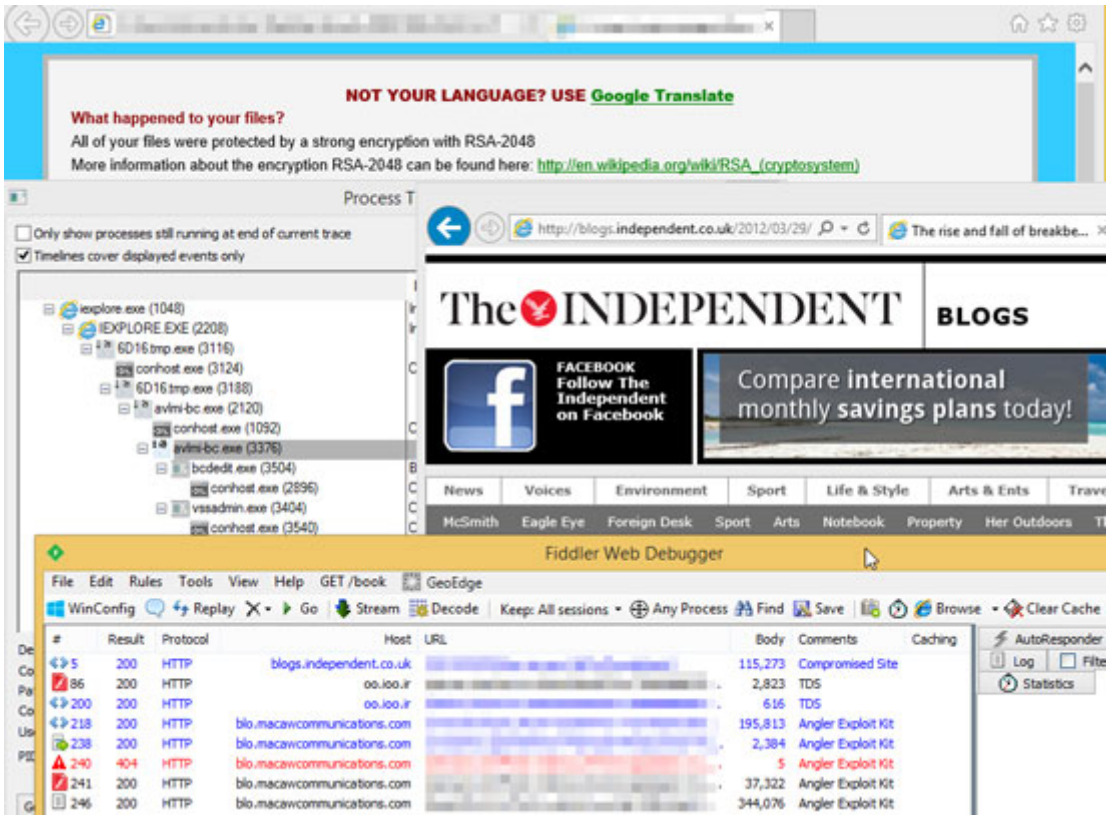

Figure 2. Our analysis showing the compromised blog page of The Independent

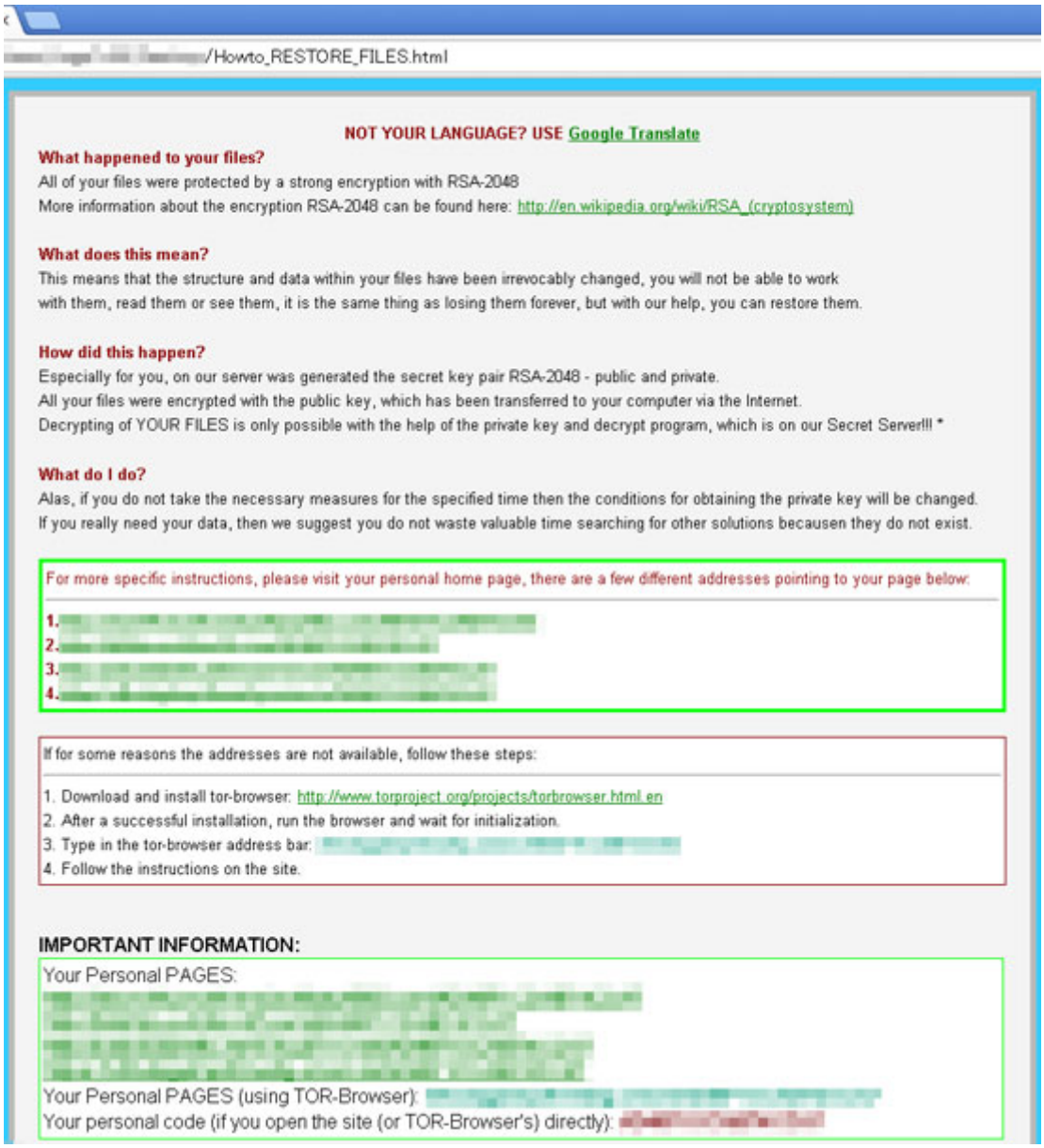

Figure 3. Screenshot of the ransom note

Angler Exploit Kit is the most active exploit kit to date that integrated Abobe Flash zero-day vulnerabilities related to the Hacking Team leak. In our 3Q threat roundup report, we observed a spike in the number of Angler-hosting links from May to September 2015.

We also tracked the number of hits to the TDS between compromised sites leading to Angler EK (not just The Independent blog) and have seen as many as 4,000 hits a day. The real number could be bigger.

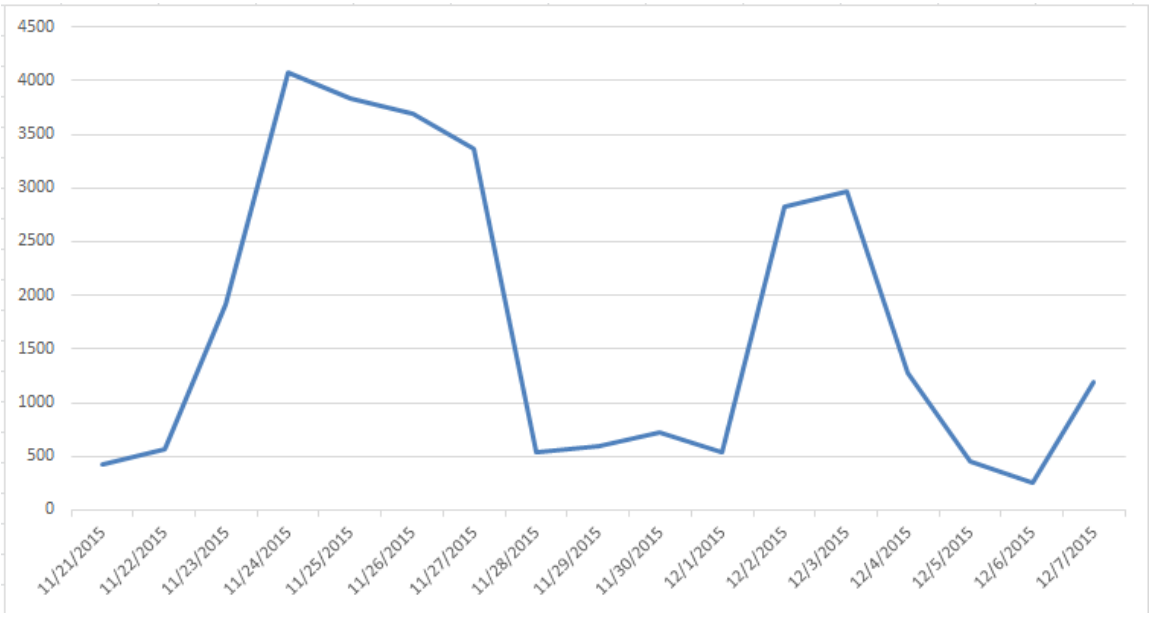

Figure 4. Number of users redirected from compromised sites leading to Angler EK

Continuous monitoring of this incident has revealed another infection chain. Rather than immediately downloading TeslaCrypt ransomware to the affected system, the exploit kit first downloads BEDEP malware.

First spotted in 2014, BEDEP became more prominent early this year due to its in use in exploit kit attacks. We even noted that it was the final payload for an attack involving the Angler Exploit Kit at the start of the year. In our BEDEP Security Brief, we pointed out that "BEDEP and its strains are known to skirt detection because of its heavy encryption. It also comes manipulated Microsoft file properties to make it appear legitimate upon inspection." In this particular infection chain, the BEDEP variant arrives via fileless infection in an effort to avoid detection.

BEDEP malware is known to download other malware—a routine demonstrated in this particular incident. The BEDEP variant downloads ransomware into the affected system. But instead of TeslaCrypt, it downloads another notorious ransomware, CryptoLocker. This malware demands that the user pay a fee of US$499 for decryption; the fee increases after a certain period has lapsed.

It's hard to determine the exact reason behind adding BEDEP to the infection chain but it's highly possible that the cybercriminals wanted to take advantage of the different features of the malware, which include information theft and backdoor capabilities.

We at Trend Micro have provided protection to user systems by blocking all known related malicious websites and detecting the final payload.

*Additional insights and analysis by **Feike Hacquebord**, **Brooks Li**, **David Agni**, and **Anthony Melgarejo**.*

*Hat tip to **Jérôme Segura** of MalwareBytes for his research on the compromised WordPress sites campaign.*

Related Posts:

- **BEDEP Malware Tied To Adobe Zero-Days**
- **BEDEP: Backdoors Brought Into The Light By Flash Zero-Days**
- **CTB-Locker Ransomware Spoofs Chrome and Facebook Emails as Lures, Linked to Phishing**
- **MERS News Used in Targeted Attack against Japanese Media Company**

Tags: mediaTeslaCryptoThe IndependentUnited Kingdomwebsite

Featured Stories

- 2016 Predictions: The Fine Line Between Business and Personal
- Pawn Storm Targets MH17 Investigation Team
- FBI, Security Vendors Partner for DRIDEX Takedown
- Japanese Cybercriminals New Addition To Underground Arena
- Follow the Data: Dissecting Data Breaches and Debunking the Myths

Recent Posts

- New Targeted Attack Group Buys BIFROSE Code, Works in Teams
- Adobe Flash Player Fixes 79 Bugs; Microsoft Issues 12 Patches in December Patch Tuesday
- Blog of News Site "The Independent" Hacked, Leads to TeslaCrypt Ransomware
- The German Underground: Buying and Selling Goods via Droppers
- Out in the Open: Accessibility in the North American Underground

2016 Security Predictions

- From new extortion schemes and IoT threats to improved cybercrime legislation, Trend Micro predicts how the security landscape is going to look like in 2016.
  Read more

Popular Posts

High-Profile Mobile Apps At Risk Due to Three-Year-Old Vulnerability
Trend Micro, NCA Partnership Leads to Arrests and Shutdown of Refud.me and Cryptex Reborn
Blog of News Site “The Independent” Hacked, Leads to TeslaCrypt Ransomware
Siri’s Flaw: Apple’s Personal Assistant Leaks Personal Data
Cybercriminals Improve Android Malware Stealth Routines with OBAD

Latest Tweets

- The Independent blogsite closed, now redirects to main site bit.ly/1HU0kcZ
  about 8 hours ago
- @Scardanelli1748 You can check the paper here bit.ly/1QcLFMs
  about 10 hours ago
- The Independent hack sees new infection chain with #CryptoLocker #ransomware bit.ly/1HU0kcZ
  about 21 hours ago

Stay Updated

Email Subscription

Your email here

Subscribe