TREND MICRO | TrendLabs SECURITY INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity

- Posted on:June 22, 2016 at 8:47 am
- Posted in:Exploits, Malware, Ransomware
- Author:
  Joseph C Chen (Fraud Researcher)

0

Early this year, we reported that in 2015, Angler came out as the top exploit kit, having contributed 59.5% in the total exploit kit activity for the year. Now, there's barely any pulse left.

After the arrest of 50 people accused of using malware to steal US$25 million, it is interesting to note that Angler basically stopped functioning. With Angler's reported inactivity, it appears that cybercriminals are scrambling to find new exploit kits to deliver malware. Angler had been the exploit kit of choice because it was the most aggressive in terms of including new exploits and it was able to apply a lot of antivirus evasion techniques such as payload encryption and fileless infection.

We saw a significant decline in overall exploit kit activity after the fall of Angler. We did see increased activity in other exploit kits, but they were no match to Angler. It appears that not all threat activity previously tied to Angler has migrated to other exploit kits.

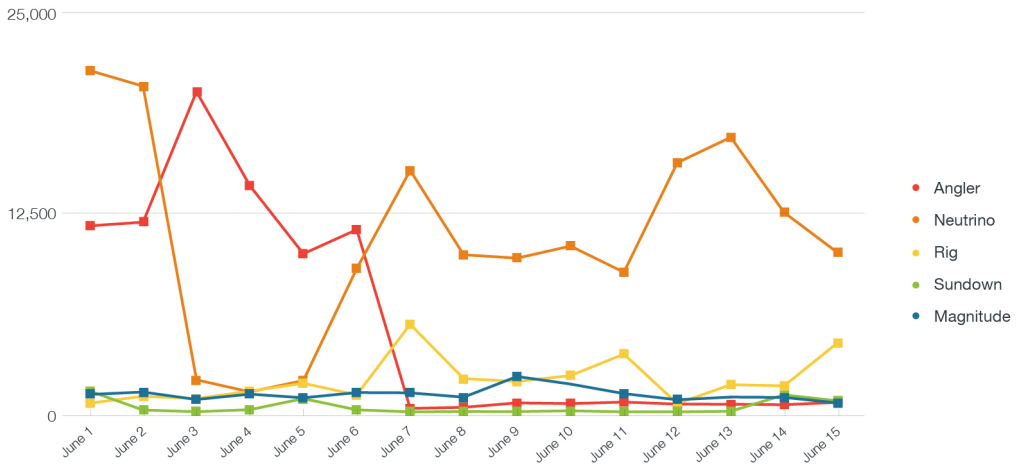


Figure 1. Exploit Kit activity from May 15-June 15, 2016

As a common tool used to drop ransomware, would Angler's inactivity affect ransomware at all? The answer seems to be "not really". We have seen Magnitude push Cerber since March this year and Rig spreading CryptoWall and TeslaCrypt last year. With Angler now out of the picture, we've seen CryptXXX campaigns, which was previously tied to the former, switching to Neutrino. New families have also emerged using the abovementioned Rig and Sundown–arguably the exploit kit "underdogs"–as their delivery mechanism.

Underdogs

Rig exploit kit employs a zero-day vulnerability disclosed from the Hacking Team leak, as well as other Adobe Flash Player vulnerabilities, among others. Rig has been spotted in a recent malvertising campaign that has affected almost 40 countries but is mainly targeting Japan.

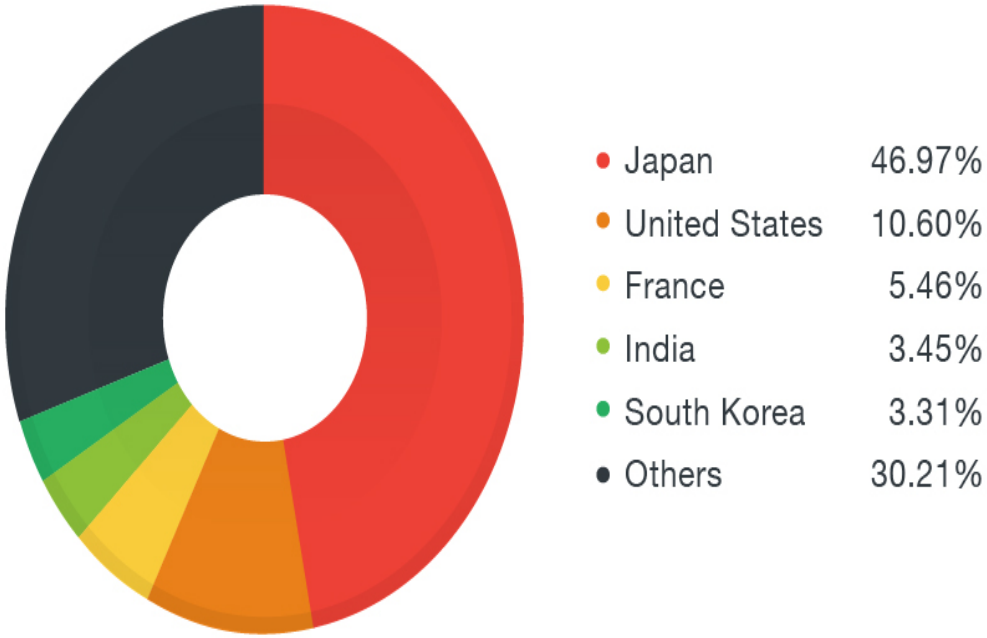


Figure 2. Distribution of Rig detections from June 1 – 16, 2016

On the other hand, Sundown employs use-after-free vulnerabilities in Adobe Flash Player. Similar to Rig, Sundown is also widely affecting Japan. Keep in mind that not all of these attacks involves Sundown dropping ransomware.

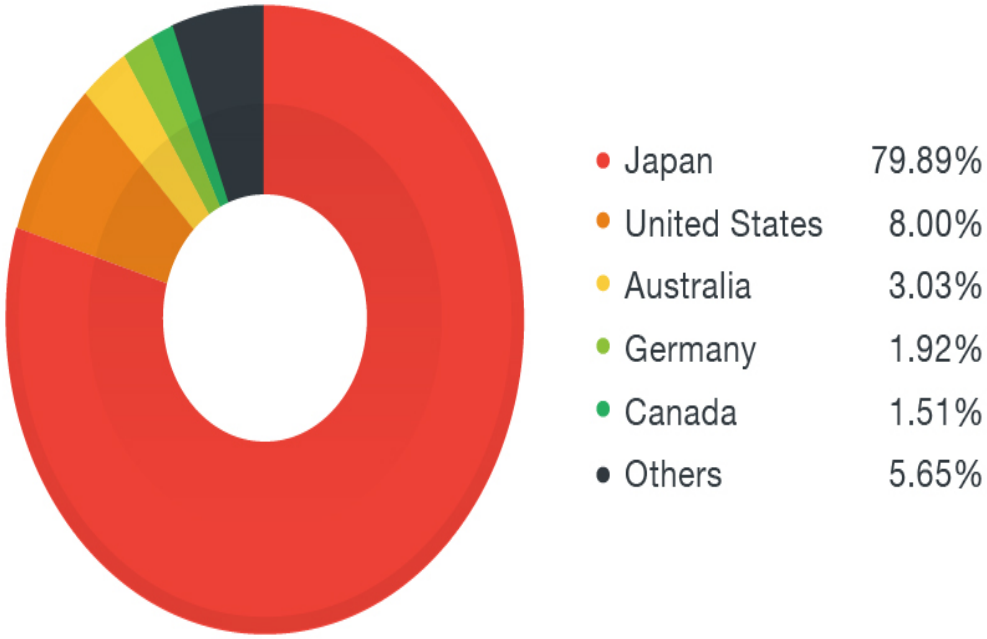


Figure 3. Distribution of Sundown detections from June 1 – 16, 2016

Dropping new ransomware

Recent Rig exploit kit activities showed that it was dropping a new family of ransomware detected as RANSOM_GOOPIC.A. This ransomware asks for US$500 payment and has a very sleek, professionally-

designed interface.

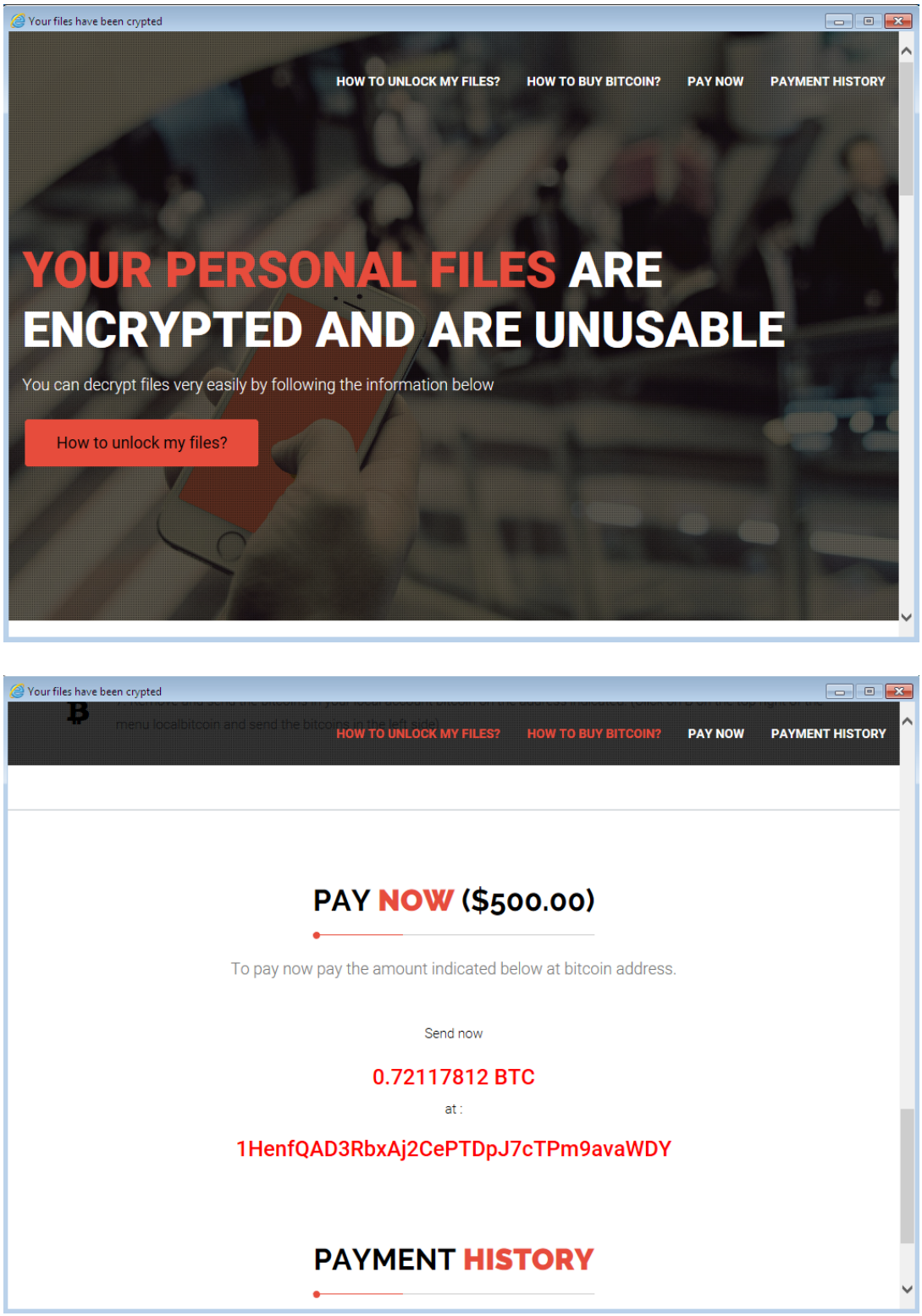


Figure 4. GOOPIC ransomware interface

Another peculiar thing about this ransomware is that provides its victims a longer time limit to pay up before it permanently locks the encrypted data. Previously, ransomware typically gives victims anywhere from 24 to 72 hours to pay the ransom; even notable families such as CryptXXX only gave users up to 90 hours to pay the ransom.

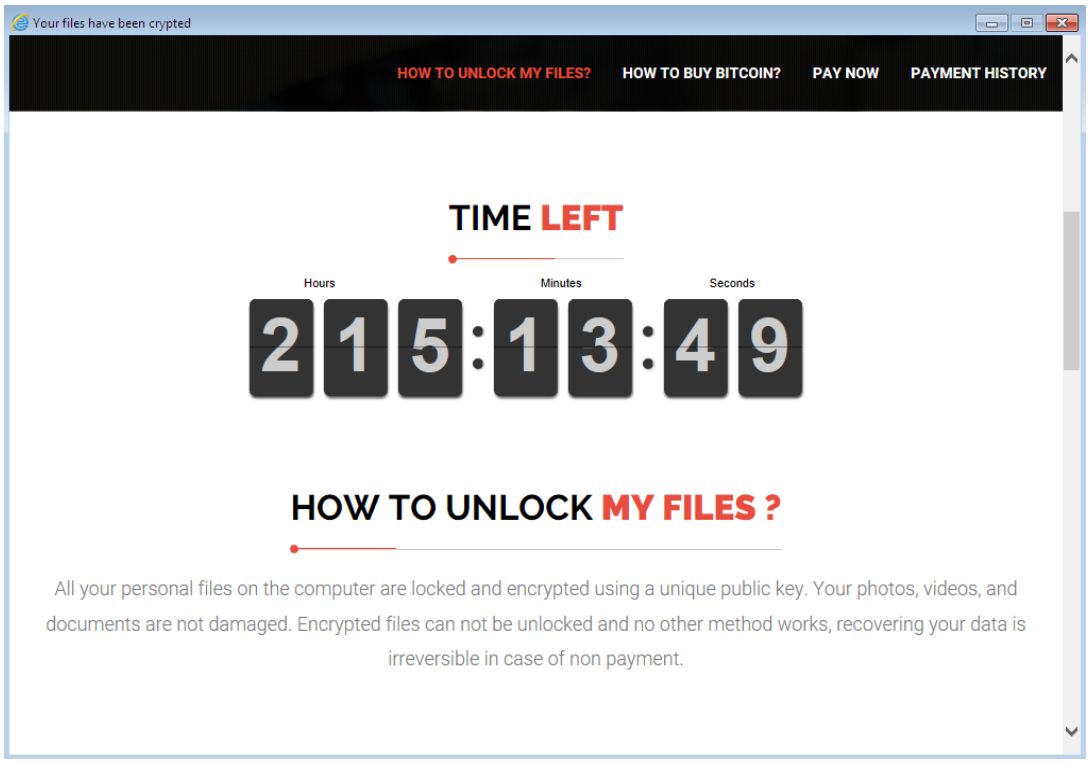


Figure 5. Over 200 hours for victims to pay

Sundown, meanwhile, delivers CryptoShocker (detected as RANSOM_CRYPSHOCKER.A), although it is not as alarming as it sounds. It charges victims US$200 and even advertises bitcoin exchange services, complete with their logos.

Figure 7. CryptoShocker ransom note

Outdated and unpatched systems and applications are the primary gateways for exploit kits to affect users. We advise users to update their systems to the latest versions of their installed applications to avoid getting victimized by exploit kits that drop ransomware. Likewise, it is unwise for users to click links from unknown sources as they may lead to malicious sites.

Trend Micro Solutions

Trend Micro offers different solutions to protect enterprises, small businesses, and home users to help minimize the risk of getting affected by crypto-ransomware.

Enterprises can benefit from a multi-layered, step-by-step approach in order to best mitigate the risks brought by these threats. Email and web gateway solutions such as Trend Micro™ Deep Discovery™ Email Inspector and InterScan™ Web Security prevents ransomware from ever reaching end users. At the endpoint level, Trend Micro Smart Protection Suites deliver several capabilities like behavior monitoring and application control, and vulnerability shielding that minimize the impact of this threat. Trend Micro Deep Discovery Inspector detects and blocks ransomware on networks, while Trend Micro Deep Security™ stops ransomware from reaching enterprise servers–whether physical, virtual or in the cloud.

For small businesses, Trend Micro Worry-Free Services Advanced offers cloud-based email gateway security through Hosted Email Security. Its endpoint protection also delivers several capabilities such as behavior monitoring and real-time web reputation in order detect and block ransomware.

For home users, Trend Micro Security 10 provides robust protection against ransomware, by blocking malicious websites, emails, and files associated with this threat.

Users can likewise take advantage of our free tools such as the Trend Micro Lock Screen Ransomware Tool, which is designed to detect and remove screen-locker ransomware; as well asTrend Micro Crypto-Ransomware File Decryptor Tool, which can decrypt certain variants of crypto-ransomware without paying the ransom or the use of the decryption key.

Hashes for related files:

- d6bbf02ec922ba035d863ec813221f15ab4c2bfb – RANSOM_GOOPIC.A
- 02126b0f507d38b03624599e782931e43c5e7141 – RANSOM_CRYPSHOCKER.A

With additional analysis by Jaaziel Carlos

Related Posts:

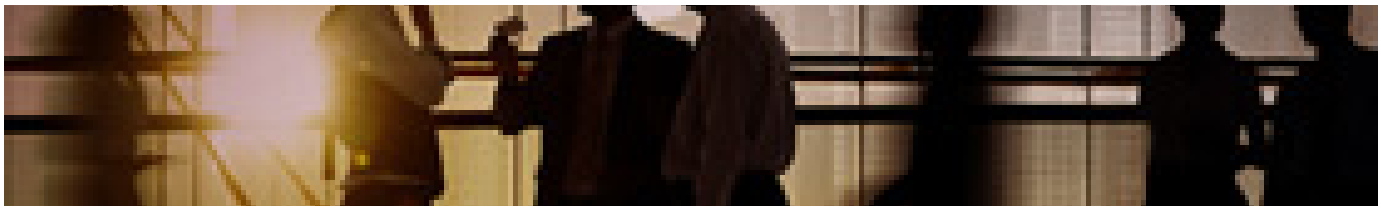
- **Angler and Nuclear Exploit Kits Integrate Pawn Storm Flash Exploit**
- **CERBER: Crypto-ransomware that Speaks, Sold in Russian Underground**
- **PETYA Crypto-ransomware Overwrites MBR to Lock Users Out of Their Computers**
- **Chimera Crypto-Ransomware Wants You (As the New Recruit)**

Tags: Angler Exploit Kitcrypto-ransomwareexploit kitransomware

Featured Stories

- FLocker Mobile Ransomware Crosses to Smart TV
- JIGSAW Crypto-Ransomware Turns Customer-Centric, Uses Chat for Ransom Attempts
- FastPOS: Quick and Easy Credit Card Theft
- IXESHE Derivative IHEATE Targets Users in America
- Company CFOs Targeted The Most By BEC Schemes

Business Email Compromise



- How can a sophisticated email scam cause more than $2.3 billion in damages to businesses around the world?
  See the numbers behind BEC

Latest Ransomware Posts

- MIRCOP Crypto-Ransomware Channels Guy Fawkes, Claims To Be The Victim Instead
- After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity
- JScript-toting Ransomware Can Steal Your Passwords and Bitcoin Wallets, Too
- Why Ransomware Works: Tactics and Routines Beyond Encryption
- FLocker Mobile Ransomware Crosses to Smart TV

Recent Posts

- MIRCOP Crypto-Ransomware Channels Guy Fawkes, Claims To Be The Victim Instead
- After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity
- 'GODLESS' Mobile Malware Uses Multiple Exploits to Root Devices
- JScript-toting Ransomware Can Steal Your Passwords and Bitcoin Wallets, Too
- Banking Trojans as a Service—Theft Made Easy in Brazil

Ransomware 101

- 

This infographic shows how ransomware has evolved, how big the problem has become, and ways to avoid being a ransomware victim.
Check the infographic

Popular Posts

Flashlight App Spews Malicious Ads
'GODLESS' Mobile Malware Uses Multiple Exploits to Root Devices
FLocker Mobile Ransomware Crosses to Smart TV
Kernel Waiter Exploit from the Hacking Team Leak Still Being Used
Unsupported TeamViewer Versions Exploited For Backdoors, Keylogging

Latest Tweets

Error: Rate limit exceeded

Stay Updated

Email Subscription

Your email here

Subscribe