TrendLabs SECURITY INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

New Bizarro Sundown Exploit Kit Spreads Locky

- Posted on:November 4, 2016 at 2:04 am
- Posted in:Bad Sites, Exploits, Ransomware
- Author:
  Brooks Li and Joseph C. Chen (Threats Analysts)

0

A new exploit kit has arrived which is spreading different versions of Locky ransomware. We spotted two cases of this new threat, which is based on the earlier Sundown exploit kit. Sundown rose to prominence (together with Rig) after the then-dominant Neutrino exploit kit was neutralized.

Called Bizarro Sundown, the first version was spotted on October 5 with a second sighting two weeks later, on October 19. Users in Taiwan and Korea made up more than half of the victims of this threat. Bizarro Sundown shares some features with its Sundown predecessor but added anti-analysis features. The October 19 attack also changed its URL format to closely resemble legitimate web advertisements. This second version is called GreenFlash Sundown. Both versions were used exclusively by the ShadowGate/WordsJS campaign.

First identified in 2015, the ShadowGate campaign targeted Revive and OpenX's open-source advertising servers that have been locally installed. Once compromised, the servers act as gateways to the exploit kit for malware distribution. Some of the domains associated with this campaign were taken down. Recently, we saw the campaign using 181 compromised sites to deliver ransomware. In September we saw ShadowGate using the Neutrino exploit kit to drop a variant of Locky (with the encrypted files having the *.zepto* extension). On October 5, the campaign shifted to Bizarro Sundown. Two weeks later (October 19), a modified version of Bizarro Sundown (GreenFlash Sundown) was spotted.

Scale and Distribution of the Attacks

The number of Bizarro Sundown victims leads to an interesting finding right away: the number of victims drops to zero on weekends.

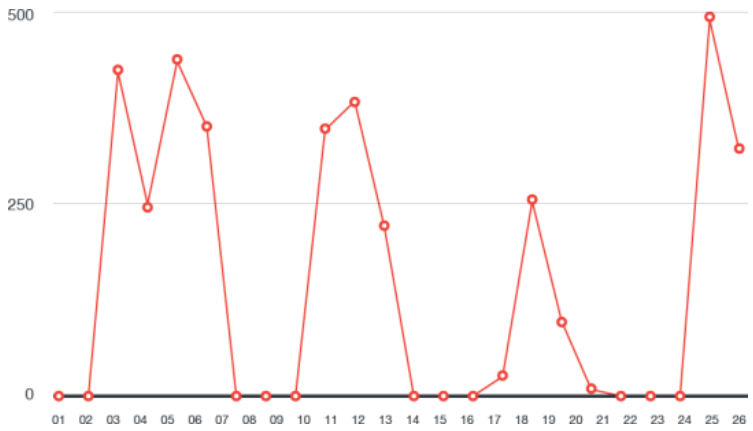

Figure 1. Timeline and number of Bizarro Sundown victims

We observed the ShadowGate campaign closing their redirections and removing the malicious redirection script from the compromised server during weekends and resuming their malicious activities on workdays. As for distribution, more than half of the victims were located in only two countries: Taiwan and South Korea. Germany, Italy, and China rounded out the top five countries.

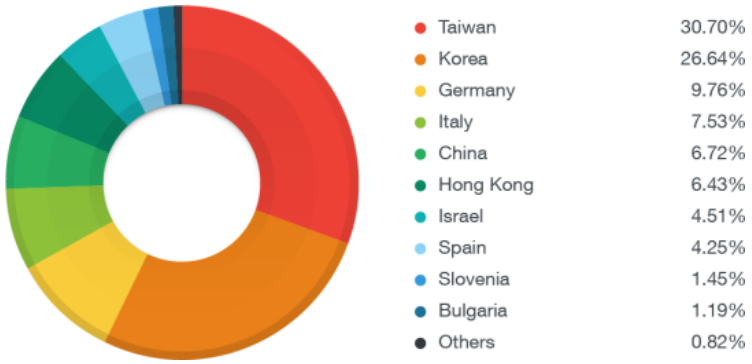

Figure 2. Distribution of Bizarro Sundown attacks, per country basis

Description of the Attacks

Bizarro Sundown targeted a memory corruption vulnerability in Internet Explorer (CVE-2016-0189, fixed in May 2016) and two security flaws in Flash: a type confusion vulnerability (CVE-2015-7645) and an out-of-bound read bug (CVE-2016-4117). The first of these was fixed a year ago (October 2015), with the second patched earlier this year (May 2016). Bizarro Sundown's second version leveraged only the two Flash exploits.

Bizarro Sundown attacks shared a similar URL format as Sundown. However, it obfuscates its landing pages differently, without using a query string. Bizarro Sundown also added anti-crawling functionality. An increasingly common feature found in exploit kits today, anti-crawling functions are designed to defeat automated crawlers used by researchers and analysts. It was used to deliver a Locky variant which appended the *.odin* extension for encrypted files.

#	Result	Protocol	Host	URL	Body	Content-Type	Comments
63	200	HTTP	bne.fdfxf.com	/index.php?5kv_Y3qejuBCWXs=siy8Y23y0KEFHS6P16cfqFmEjZJkqxds9QCvyApnJVikk...	54,767	text/html; charset=UTF-8	Sundown Exploit Kit
67	404	HTTP	bne.fdfxf.com	/undefined	142	text/html	Sundown Exploit Kit
68	200	HTTP	bne.fdfxf.com	/45786437956439785/153.swf	22,693	application/x-shockwave-flash	Sundown Exploit Kit
69	200	HTTP	bne.fdfxf.com	/58036758967895465498645928 6/489567945678456874356487356743256.swf	33,591	application/x-shockwave-flash	Sundown Exploit Kit
70	404	HTTP	bne.fdfxf.com	/undefined	142	text/html	Sundown Exploit Kit
75	200	HTTP	t.7865687.com	/z.php?id=153	397,305	application/octet-stream	Sundown Exploit Kit

#	Result	Protocol	Host	URL	Body	Content-Type	Comments
2	200	HTTP	jewelry.earwhig.net	/microcomputers/features.js	176	text/javascript	ShadowGate
3	200	HTTP	aided.theteragroup.com	/index.php	20,846	text/html; charset=utf-8	Bizarro Sundown EK
4	200	HTTP	aided.theteragroup.com	/sadwqwd.swf	19,447	application/x-shockwave-flash	Bizarro Sundown EK
5	200	HTTP	references.vietnamesebaby.com	/k.php?ins=22	407,884	text/html; charset=utf-8	Bizarro Sundown EK

Figure 3. Traffic of Sundown (above) and Bizarro Sundown (below) exploit kits (click to enlarge)

Two weeks later, we saw a new version of Bizarro Sundown that included changes to its redirection chain; its URLs are now more similar to typical advertising traffic. This version was given the name GreenFlash Sundown. It can now be integrated more directly into ShadowGate's new redirection method, which used to rely on scripts to route potential victims to malicious servers. It utilizes a malicious Flash (.SWF) file for this purpose.

This file determines the version of Flash Player installed, which is relayed to the exploit kit via a query string. Bizarro Sundown uses that information to deliver the appropriate Flash exploit. This can be seen as a way to streamline redirections by removing intermediaries (landing pages) from the infection chain. During this time, we've seen ShadowGate delivering another Locky variant (detected by Trend Micro as RANSOM_LOCKY.DLDSAPZ) that appends a *.thor* extension to encrypted files.

#	Result	Protocol	Host	URL	Body	Content-Type	Comments
1	200	HTTP	[redacted]	/	15,254	text/html	
15	200	HTTP	[redacted]	[redacted]/www/delivery/ajs.php?zoneid=1&target=_blank&cb...	986	text/javascript; charset=utf-8	Compromised OpenX Server
17	200	HTTP	[redacted]	[redacted]/www/images/1x1.js	1,243	application/x-javascript	Compromised OpenX Server
20	200	HTTP	[redacted]	[redacted]/www/images/1x1.swf	1,040	application/x-shockwave-flash	Compromised OpenX Server
36	200	HTTP	ads.phoenixhealthtechnology.com	/images/adv.swf	1,224	text/html; charset=utf-8	ShadowGate
44	200	HTTP	ads.dudleywells.com	/checks.swf?advbannerid=21	19,442	text/html; charset=utf-8	Bizarro Sundown Exploit Kit (v2)
61	200	HTTP	ads.dudleywells.com	/k.php?id=3	407,879	text/html; charset=utf-8	Bizarro Sundown Exploit Kit (v2)

Figure 4. GreenFlash Sundown from a compromised ad server (click to enlarge)

Figure 5. Part of code that determines the version of Flash Player installed on the system (click to enlarge)

Mitigation

While a solid backup strategy is a good defense against ransomware, doubling down on sound patch management helps further secure the device's perimeter. Keeping the operating system and other installed software up-to-date mitigates the risks of exploits targeting vulnerabilities that have already been fixed by software vendors.

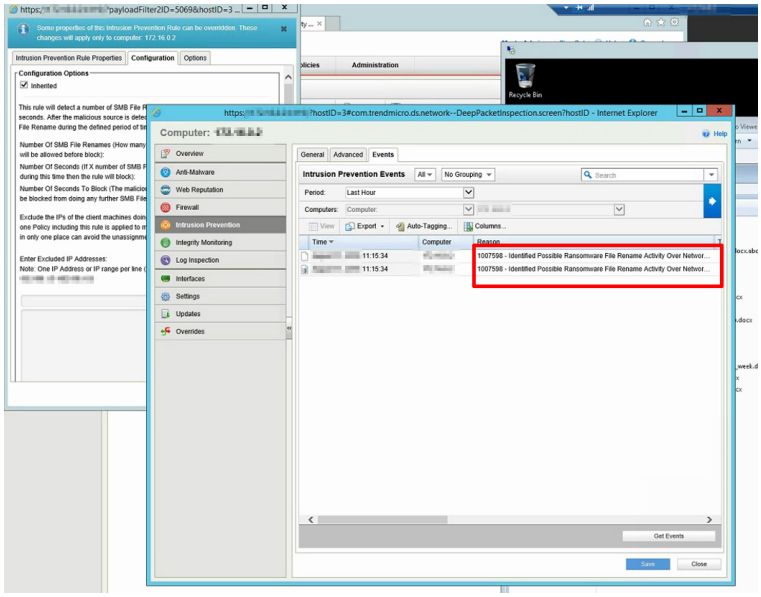

Figure 6. A snapshot of Trend Micro™ Deep Security™ providing virtual patching

Users and enterprises can also benefit from a multilayered approach to security—from gateway, endpoints, networks, and servers. Using a security solution that can proactively provide defense against attacks leveraging system and software vulnerabilities is also recommended.

Hat tip to @kafeine whom we collaborated with in this research/analysis

Some of the indicators of compromise (IoCs) include:

SHA1 detected as RANSOM_LOCKY.DLDSAPZ

- 867ed6573d37907af0279093105250a1cf8608a2

Related to ShadowGate:

- jewelry[.]earwhig[.]net
- ads[.]phoenixhealthtechnology[.]com

Related to Bizarro Sundown Exploit Kit:

- aided[.]theteragroup[.]com
- references[.]vietnamesebaby[.]com
- ads[.]dubleywells[.]com

Updated on November 5, 2016, 09:45 AM (UTC-7)

We clarified what was originally written in the third paragraph regarding how domains used by ShadowGate were taken down. We also listed SHA-1 which we detect as RANSOM_LOCKY.DLDSAPZ, and some of the IoCs related to ShadowGate and Bizarro Sundown.

Updated on November 8, 2016, 09:00 PM (UTC-7)

We have clarified the naming of the second attack, which is called GreenFlash Sundown.

Updated on December 14, 2016, 12:15 AM (UTC-7)

Further analysis has indicated that the vulnerability used was CVE-2015-7645 instead of CVE-2015-5119. We have updated the text accordingly.

Related Posts:

- **Updated Sundown Exploit Kit Uses Steganography**
- **Locky Ransomware Spreads via Flash and Windows Kernel Exploits**
- **After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity**
- **Massive Malvertising Campaign in US Leads to Angler Exploit Kit/BEDEP**

Tags: Bizarro Sundownexploit kitsLockyShadowGateSundown

Featured Stories

- Pawn Storm Ramps Up Spear-phishing Before Zero-Days Get Patched
- New Bizarro Sundown Exploit Kit Spreads Locky
- The Internet of Things Ecosystem is Broken. How Do We Fix It?
- CVE-2016-3298: Microsoft Puts the Lid on Another IE Zero-day Used in AdGholas Campaign
- FastPOS Updates in Time for the Retail Sale Season

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

Recent Spam Runs in Germany Show How Threats Intend to Stay in the Game

Mobile Ransomware: How to Protect Against It

Mobile Ransomware: Pocket-Sized Badness

HDDCryptor: Subtle Updates, Still a Credible Threat

Businesses as Ransomware's Goldmine: How Cerber Encrypts Database Files

Recent Posts

- Recent Spam Runs in Germany Show How Threats Intend to Stay in the Game
- Updated Sundown Exploit Kit Uses Steganography
- Alice: A Lightweight, Compact, No-Nonsense ATM Malware
- Fake Apps Take Advantage of Super Mario Run Release

- Mobile Ransomware: How to Protect Against It

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

One Bit To Rule A System: Analyzing CVE-2016-7255 Exploit In The Wild
Alice: A Lightweight, Compact, No-Nonsense ATM Malware
New Flavor of Dirty COW Attack Discovered, Patched
New SmsSecurity Variant Roots Phones, Abuses Accessibility Features and TeamViewer
CEO Fraud Email Scams Target Healthcare Institutions

Latest Tweets

- Learn how attackers can infiltrate their target network by using leaked info from #pagers. https://t.co/aNgK8sTkMh… twitter.com/i/web/status/8…
  about 3 hours ago
- First spotted in 2014, we take a closer look at an #ATMmalware family called Alice. Our analysis:… twitter.com/i/web/status/8…
  about 6 hours ago
- A look back at the most notable #cybersecurity moments of 2016: bit.ly/2hNVkfc
  

  about 9 hours ago

Stay Updated

Email Subscription

Your email here

Subscribe

- Home and Home Office
- |
- For Business
- |
- Security Intelligence
- |
- About Trend Micro

- Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣
- Latin America Region (LAR): Brasil, México
- North America Region (NABU): United States, Canada
- Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

- Privacy Statement
- Legal Policies