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

Updated Sundown Exploit Kit Uses Steganography

- Posted on:December 29, 2016 at 12:01 am
- Posted in:Exploits, Malware, Vulnerabilities
- Author:
  Brooks Li and Joseph C. Chen (Threats Analysts)

0

This year has seen a big shift in the exploit kit landscape, with many of the bigger players unexpectedly dropping out of action. The Nuclear exploit kit operations started dwindling in May, Angler disappeared around the same time Russia's Federal Security Service made nearly 50 arrests last June, and then in September Neutrino reportedly went private and shifted focus to select clientele only. Now, the most prominent exploit kits in

circulation are RIG and Sundown. Both gained prominence shortly after Neutrino dropped out of active circulation.

Sundown is something of an outlier from typical exploit kits. It tends to reuse old exploits and doesn't make an effort to disguise their activity. The URLs for Sundown requests for Flash files end in *.swf*, while Silverlight requests end in *.xap*. These are the normal extensions for these file types. Typically, other exploit kits make an effort to hide their exploits. In addition, Sundown doesn't have the anti-crawling feature used by other exploit kits.

Recent use of Sundown/RIG

Sundown and RIG were both in the spotlight last September when a malvertising campaign was found to be distributing the CryLocker ransomware through both exploit kits. Researchers first detected RIG pushing this ransomware as its payload on September 1, Sundown started doing so on September 5. CryLocker was unique in that it used Portable Network Graphic (PNG) files to package the information stolen from the infected system. The PNG file was then uploaded into an Imgur album, where ransomware operators could access it easily but also evade detection.

The developers of this particular malware gave their files a valid PNG header, but no image. The file only had the system information as ASCII strings. This makes it distinct from steganography, which hides secret messages, files, or information in an image.

Steganography Techniques used by Exploit Kits

Steganography is an advanced technique used to hide malicious code into an image to prevent signature based detection. It's quite popular and has been used in several malvertising and exploit kit attacks. Earlier this year, the massive GooNky malvertising campaign used multiple techniques to hide their malvertising traffic, including moving part of malicious code into images to prevent detection. However, here the attackers didn't really "hide" the data in the picture itself – they merely appended their malicious code at the end of the file.

In a more advanced case, Trend Micro researchers worked with colleagues across the security community to dive into the steganography tactics used in the AdGholas malvertising campaign and its associated Astrum exploit kit. The campaign encoded a script into an image's alpha channel, which defines the transparency of the pixels. The minor modification allows the malware designer to mimic a legitimate ad, with only a slight difference in color. This makes it more difficult for these malicious ads to be spotted and analyzed.

On December 27, 2016, we noticed that Sundown was updated to use similar techniques. The PNG files weren't just used to store harvested information; the malware designers now used steganography to hide their exploit code.

The newly updated exploit kit was used by multiple malvertising campaigns to distribute malware. The most affected countries were Japan, Canada, and France, though Japanese users accounted for more than 30% of the total targets.

Figure 1. Distribution of the Sundown exploit kit targets from December 21 to 27

As we noted earlier, previous Sundown versions directly connected victims to the Flash exploit file on their landing page. In this updated version, the exploit kit's malvertisement creates a hidden iframe that automatically connects to the Sundown landing page. The page will retrieve and download a white PNG image. It then decodes the data in this PNG file to obtain additional malicious code:

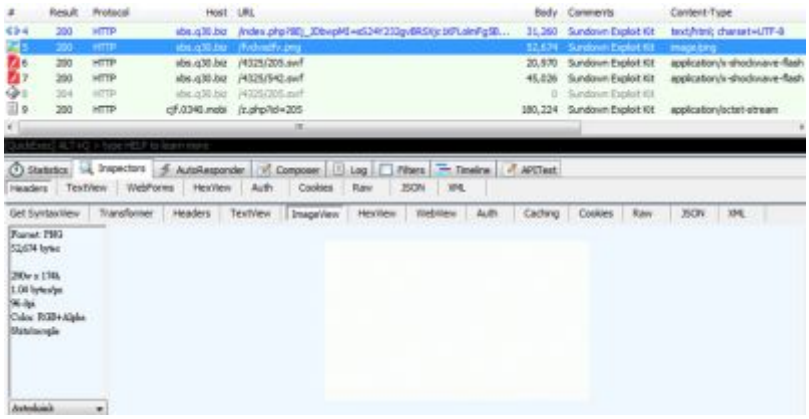


Figure 2. Steganography used in Sundown exploit kit infection chain (Click to enlarge)

Upon further analysis of the exploit code inside the PNG image, we found that it included the exploit code targeting CVE-2015-2419, a vulnerability in the JScript handling of Internet Explorer. A Flash exploit for CVE-2016-4117 is also retrieved by the exploit code. The landing page itself includes an exploit targeting another Internet Explorer (IE) vulnerability, CVE-2016-0189. All of these exploits have been patched and have been used by other exploit kits this the past year.

```
retObj = getBodyLength(rng, imageData, newData, deletedbytes);
newData = retObj.newData;
len = retObj["len"];

for (var i = 0; i < len; i++) {
    var randnum = Math.floor(rng() * newData.length);
    var redIndex = randnum - (randnum % 4);

    if (newData[redIndex] == -1) {
        i--;
        continue;
    }
    byte = ((imageData[redIndex] & 7) << 5 | (imageData[redIndex + 1] & 3) << 3 | (imageData[redIndex + 2] & 7));
    body += String.fromCharCode(byte);
    newData[redIndex] = -1;
    deletedbytes++;
}
document.write(body);
```

Figure 3. JavaScript Code inside landing page to decode the PNG file

The malware dropped by Sundown here is the Chthonic banking Trojan (detected by Trend Micro as TSPY_CHTHONIC.A). Chthonic is a variant of the Zeus malware that was used in a PayPal scam last July.

The Sundown exploit kit exploits vulnerabilities in Adobe Flash and JavaScript, among others. Trend Micro protects users against this threat. The existing Sandbox with Script Analyzer engine, which is part of Trend Micro™ Deep Discovery, can be used to detect this threat by its behavior without any engine or pattern updates. The Browser Exploit Prevention feature on endpoint products such as Trend Micro™ Security, Smart Protection Suites, and Worry-Free Business Security blocks the exploit once the user accesses the URL it is hosted in. Browser Exploit Prevention protects against exploits that target browsers or related plugins.

Indicators of Compromise

The following domains were used by the Sundown Exploit kit with the matching IP addresses:

- xbs.q30.biz (188.165.163.228)
- cjf.0340.mobi (93.190.143.211)

The Chthonic sample has the following SHA1 hash:

- c2cd9ea5ad1061fc33adf9df68eeed6a1883c5f9

The sample also used the following C&C server:

- pationare.bit

Related Posts:

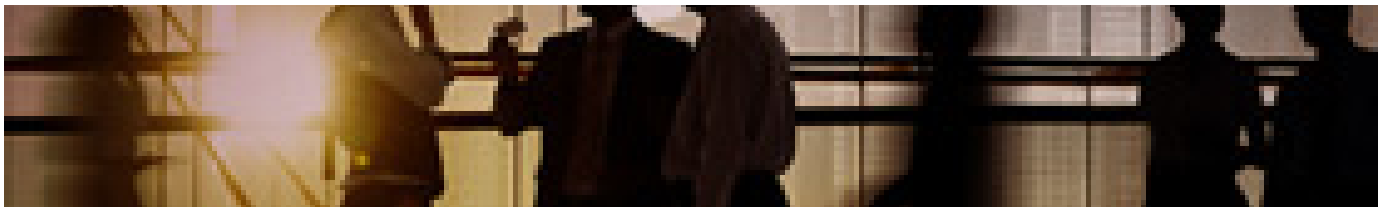
- **New Bizarro Sundown Exploit Kit Spreads Locky**
- **Exploit Kits in 2015: Flash Bugs, Compromised Sites, Malvertising Dominate**
- **After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity**
- **Exploit Kits in 2015: Scale and Distribution**

Tags: exploit kitsteganographySundown

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

Alice: A Lightweight, Compact, No-Nonsense ATM Malware
One Bit To Rule A System: Analyzing CVE-2016-7255 Exploit In The Wild
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

- Gear up for 2017 and find out the #cybersecurity challenges that you may face. Read our #securitypredictions:… twitter.com/i/web/status/8…
  about 4 hours ago

- Before getting a smart gadget for your kid, we suggest taking this quiz first: bit.ly/2gXKIg7 #IoT

about 10 hours ago

- 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 1 day ago

Stay Updated

Email Subscription

Your email here

Subscribe

- 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