Angler and Nuclear Exploit Kits Integrate Pawn Storm Flash Exploit

- Posted on:November 3, 2015 at 8:49 am
- Posted in:Vulnerabilities
- Author:
  Brooks Li and Joseph C. Chen (Threats Analysts)

1

When it comes to exploit kits, it’s all about the timing. Exploit kits often integrate new or zero-day exploits in the hopes of getting a larger number of victims with systems that may not be as up-to-date with their patches. We found two vulnerabilities that were now being targeted by exploit kits, with one being the recent Pawn Storm Flash zero-day.

Starting on October 28, we found that these two vulnerabilities were being targeted by the Angler and Nuclear exploit kits. (The second vulnerability was a Flash vulnerability that worked on versions up to 18.0.0.232; we are currently working with Adobe to confirm the CVE number for this exploit.)

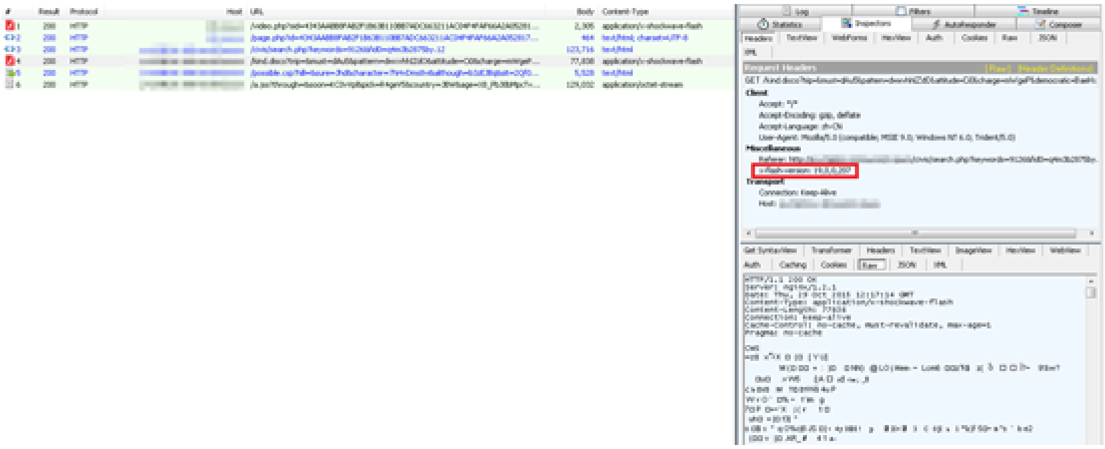


Figure 1. Angler EK .saz snapshot for CVE-2015-7645 (click to enlarge)

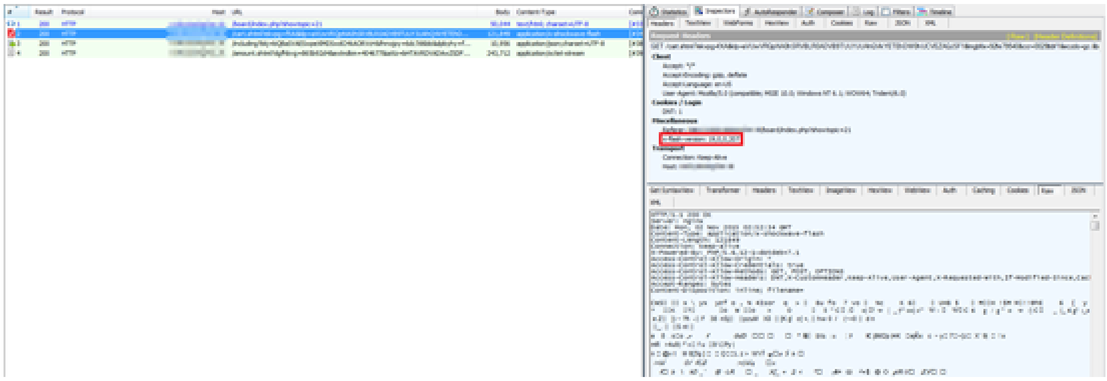


Figure 2. Nuclear EK .saz snapshot for CVE-2015-7645 (click to enlarge)

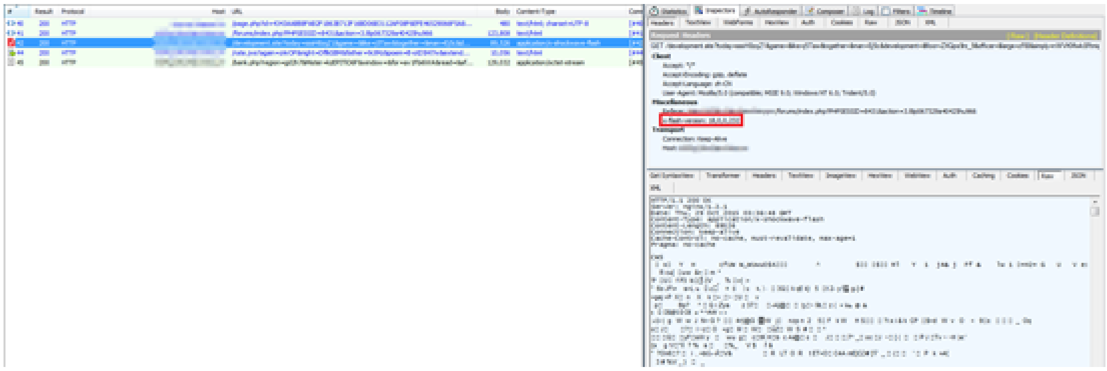


Figure 3. Angler EK .saz snapshot for the second exploit (click to enlarge)

Diffie-Hellman Protocol Misuse

Our latest research confirms that the two exploit kits abusing the Diffie-Hellman key exchange, with some minor differences from the previous usage. This is being done to hide their network traffic and to get around certain security products.

The changes are an attempt to make analysis of their key exchange by researchers more difficult. The Angler EK has made the following changes to its usage of the Diffie-Hellman protocol. They add some obfuscation to what had previously been a relatively clear and obvious process.

1. It will no longer send *g* and *p* from the client to server. Instead, it sends an *ssid* which identified the *g* and *p* pair.
2. The random key *K* is 128-byte, rather than 16-byte. The use of a 128-byte key makes it harder to decrypt the raw data.

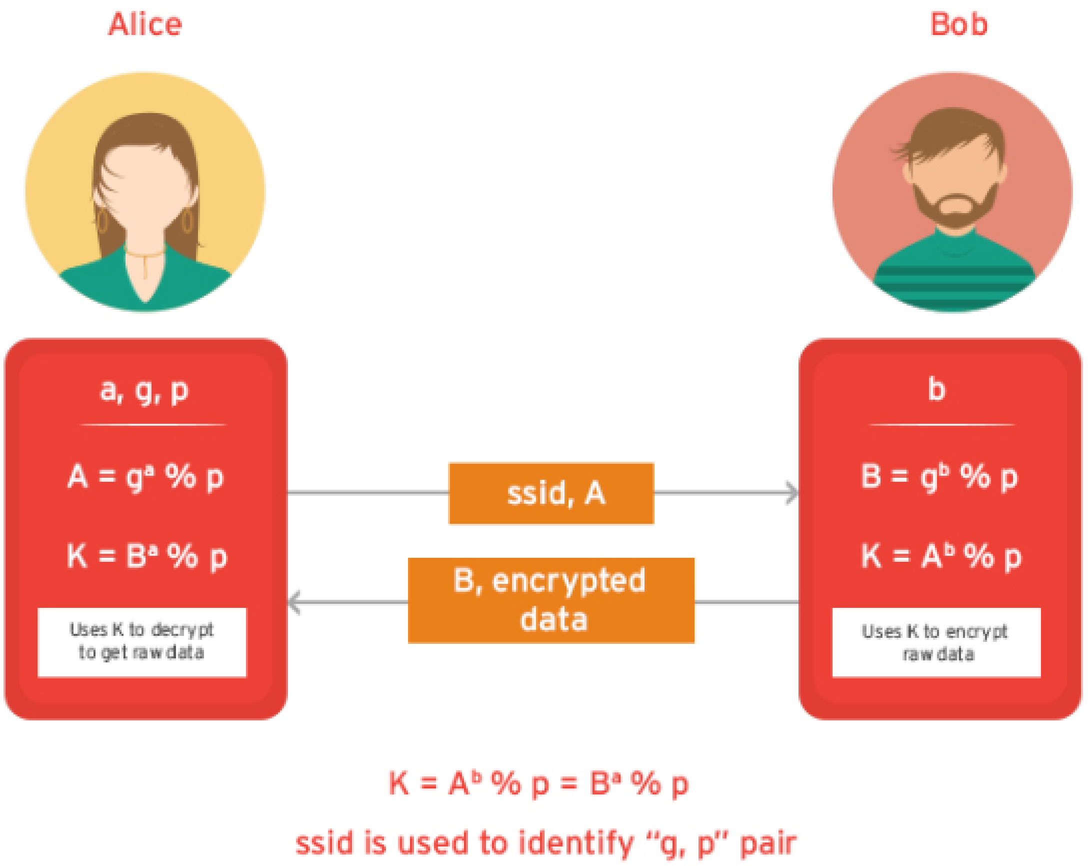
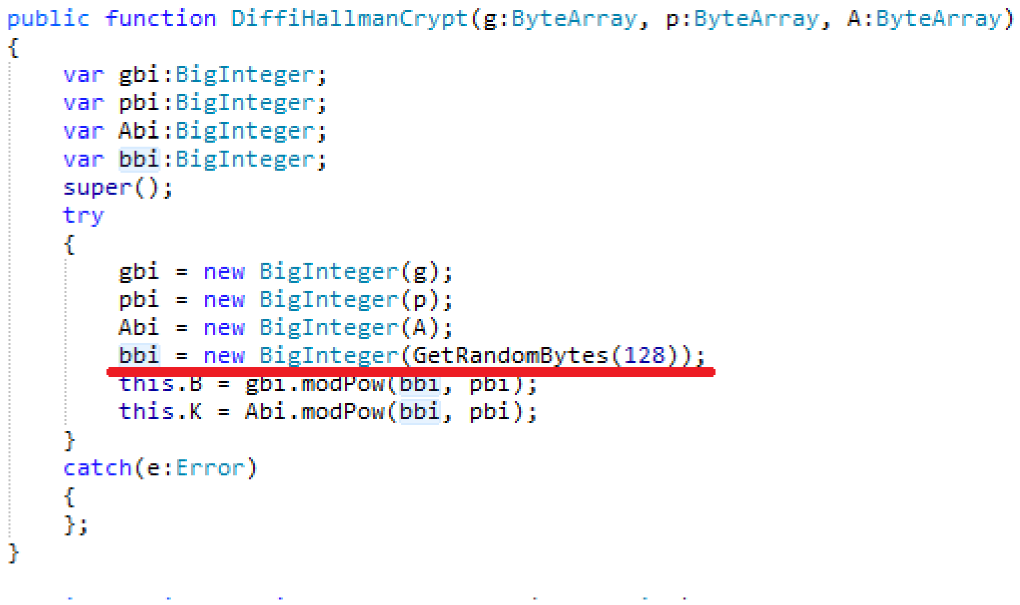

Alice
Bob
a, g, p
$A = g^a \% p$
$K = B^a \% p$
Uses K to decrypt to get raw data
ssid, A
B, encrypted data
b
$B = g^b \% p$
$K = A^b \% p$
Uses K to encrypt raw data
$K = A^b \% p = B^a \% p$
ssid is used to identify "g, p" pair

Figure 4. Diffie-Hellman protocol, using SSID to identify g, p pair

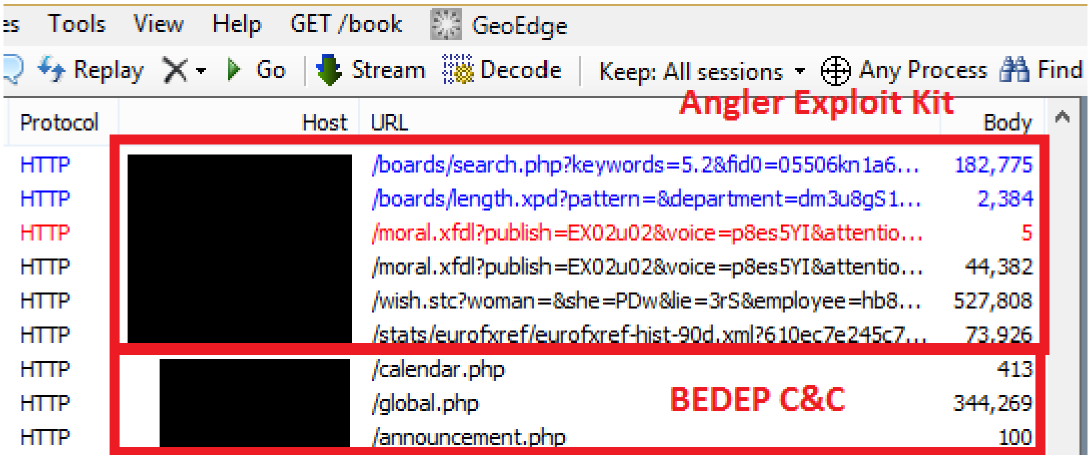


```
public function DiffiHallmanCrypt(g:ByteArray, p:ByteArray, A:ByteArray)
{
    var gbi:BigInteger;
    var pbi:BigInteger;
    var Abi:BigInteger;
    var bbi:BigInteger;
    super();
    try
    {
        gbi = new BigInteger(g);
        pbi = new BigInteger(p);
        Abi = new BigInteger(A);
        bbi = new BigInteger(GetRandomBytes(128));
        this.B = gbi.modPow(bbi, pbi);
        this.K = Abi.modPow(bbi, pbi);
    }
    catch(e:Error)
    {
    };
}
```

Figure 5. Code snippet showing 128-byte key

Multiple Payloads

Multiple payloads were downloaded onto user systems by these exploit kits. We saw instances wherein the final payload were BEDEP and CryptoLocker—at the same time. In other cases, backdoor ROVNIX malware, TeslaCrypt/CryptoWall ransomware, and KASIDET infostealers were downloaded onto user machines.



Angler Exploit Kit

Protocol	Host	URL	Body
HTTP	[redacted]	/boards/search.php?keywords=5.2&fid0=05506kn1a6...	182,775
HTTP	[redacted]	/boards/length.xpd?pattern=&department=dm3u8gS1...	2,384
HTTP	[redacted]	/moral.xfdl?publish=EX02u02&voice=p8es5YI&attentio...	5
HTTP	[redacted]	/moral.xfdl?publish=EX02u02&voice=p8es5YI&attentio...	44,382
HTTP	[redacted]	/wish.stc?woman=&she=PDw&lie=3rS&employee=hb8...	527,808
HTTP	[redacted]	/stats/eurofxref/eurofxref-hist-90d.xml?610ec7e245c7...	73,926
HTTP	[redacted]	/calendar.php	413
HTTP	[redacted]	/global.php	344,269
HTTP	[redacted]	/announcement.php	100

BEDEP C&C

Figure 6. BEDEP C&C server activity

Feedback from the Smart Protection Network indicates that activity for the Angler exploit kit was higher in the earlier weeks of October; perhaps the addition of these vulnerabilities is an attempt to raise the traffic levels of the exploit back to the earlier levels. Users in Japan, the United States, and Australia were the most affected.

Countermeasures

Trend Micro is already able to protect 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.

Trend Micro Deep Security and Vulnerability Protection, on the other hand, protect user systems from threats that may leverage the Pawn Storm Flash vulnerability with the DPI rule **1007119 – Identified Malicious Adobe Flash SWF File**.

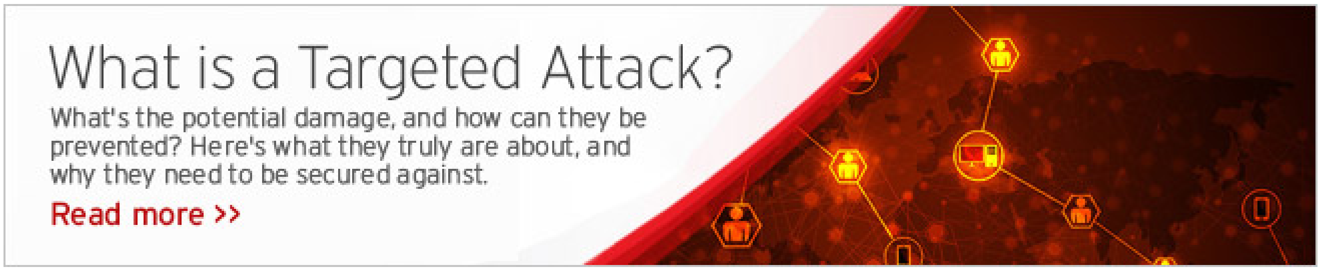
The SHA1 of the Flash exploits and payloads are:

- 0e05229784d993f1778bfc42510c1cd2d90f3938
- 4cf3361c750135eaa64946292ea356f4a75b9b1c
- 56a96c79b027baa70fc5f388412c6c36e4aa3544
- 600fd58cdd0d162dd97be1659c5c0c4b9819e2e3
- 69143d6bd45f99729123531583c54740d6be190d
- af6c40b12e5cd917bb02440d8f3db85c649b8ba9
- c332856b0b85b06235c440c4b1d6a48afdf9775b
- f6b6287240323f914bd0c7ddf768d850d8002592

Updated on November 4, 2015, 11:21 A.M. PST (UTC-8) to include relevant Trend Micro Deep Security and Vulnerability Protection DPI rule.

Related Posts:

- **Latest Flash Exploit Used in Pawn Storm Circumvents Mitigation Techniques**
- **Latest Flash Exploit in Angler EK Might Not Really Be CVE-2015-0359**
- **Freshly Patched Flash Exploit Added to Nuclear Exploit Kit**
- **Hacking Team Flash Zero-Day Integrated Into Exploit Kits**


What is a Targeted Attack?
What's the potential damage, and how can they be prevented? Here's what they truly are about, and why they need to be secured against.
Read more >>

Tags: adobe flashAngler Exploit KitExploitexploit kitFlashnuclear exploit kitPawn Stormvulnerability

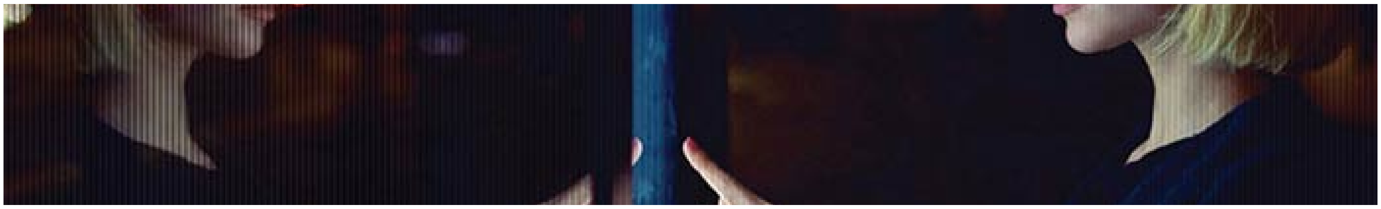
Featured Stories

- 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

- DRIDEX: Down, But Not Out
- Moplus SDK Issues Extend to Non-Baidu Apps
- Angler and Nuclear Exploit Kits Integrate Pawn Storm Flash Exploit
- Setting the Record Straight on Moplus SDK and the Wormhole Vulnerability
- 2016 Predictions: The Fine Line Between Business and Personal

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

New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministries
Setting the Record Straight on Moplus SDK and the Wormhole Vulnerability
Latest Flash Exploit Used in Pawn Storm Circumvents Mitigation Techniques
New Headaches: How The Pawn Storm Zero-Day Evaded Java's Click-to-Play Protection
Pawn Storm Targets MH17 Investigation Team

Latest Tweets

- What can you expect from 2016? Evolved ransomware, stronger cybercrime legislation, and more: bit.ly/1ict7gc about 16 mins ago

- New post: Moplus SDK Issues Extend to Non-Baidu Apps bit.ly/1Ota7J0 @TrendMicro
  about 9 hours ago
- Users avert #Malvertising through ad-blocking tools; advertisers will seek new online advertising methods: bit.ly/1RVzrpk
  about 2 days 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

- Copyright © 2015 Trend Micro Incorporated. All rights reserved.