



Exploit Kits in 2015: Flash Bugs, Compromised Sites, Malvertising Dominate

- Posted on:March 10, 2016 at 4:00 am
- Posted in:Exploits, Malware, Vulnerabilities
- Author:
  Brooks Li and Joseph C. Chen (Threats Analysts)

0

Threats never stand still, and exploits kits were no exception. 2015 saw multiple changes to this part of the threat landscape: freshly-discovered exploits were added, and compromised websites and malvertising were used to deploy and spread threats using exploit kits.

Exploit kits were a key part of the threat landscape in 2015. In this series of posts, we will examine developments in exploit kits in 2015, starting with new exploits added as well as the new techniques that have been used as part and parcel of attacks using exploit kits. In a future post, we will look at feedback from our customers to determine the scale of the problems as well as to show which countries/regions are most affected.

New Exploits: Flash dominates

Exploits kits need to continuously add new vulnerabilities to target to ensure they remain potent even as users upgrade to newer versions of software. It's no surprise, then, that 17 new vulnerabilities were targeted by various exploit kits in 2015. Of these, 14 were patched before any exploits were widely used in the wild. The remaining three became zero-days that affected users before a patch was available. Some of these vulnerabilities were first used in targeted attacks like Pawn Storm or leaked online (the Hacking Team vulnerabilities), while others were "discovered" from careful analysis of the patches.

What is remarkable about this total is how dominant just one application was – Adobe Flash Player. Thirteen of the vulnerabilities were from this application alone. It highlights the importance of Flash vulnerabilities in the exploit kit ecosystem – without the presence of Flash, exploit kits would be far less powerful.

CVE Number	Vulnerable Application	Date Identified	First Exploit Kit to Integrate	Patch Release Date
CVE-2015-8651	Adobe Flash	2016-01-26	Angler	2015-12-28
CVE-2015-8446	Adobe Flash	2015-12-15	Angler	2015-12-08
CVE-2015-7645	Adobe Flash	2015-10-29	Angler	2015-10-16
CVE-2015-5560	Adobe Flash	2015-08-28	Angler	2015-08-11
CVE-2015-2419	Microsoft Internet Explorer	2015-08-10	Angler	2015-07-22
CVE-2015-1671	Microsoft Silverlight	2015-07-21	Angler	2015-05-12
CVE-2015-5122	Adobe Flash	2015-07-11	Angler	2015-07-14
CVE-2015-5119	Adobe Flash	2015-07-07	Angler	2015-07-08
CVE-2015-3113	Adobe Flash	2015-06-27	Magnitude	2015-06-23
CVE-2015-3104	Adobe Flash	2015-06-17	Angler	2015-06-09
CVE-2015-3105	Adobe Flash	2015-06-16	Magnitude	2015-06-09
CVE-2015-3090	Adobe Flash	2015-05-26	Angler	2015-05-12
CVE-2015-0359	Adobe Flash	2015-04-18	Angler	2015-04-14
CVE-2015-0336	Adobe Flash	2015-03-19	Nuclear	2015-03-12
CVE-2015-0313	Adobe Flash	2015-02-02	HanJuan	2015-02-04
CVE-2015-0311	Adobe Flash	2015-01-20	Angler	2015-01-27
CVE-2015-0310	Adobe Flash	2015-01-15	Angler	2015-01-22

Table 1. Exploits added to exploit kits in 2015 (newest to oldest by date of identification)

As we'll note later on, the Angler exploit kit has been the most successful exploit kit of 2015. Angler adds new exploits on a regular basis, and as the above table noted it is frequently the first exploit kit to target a vulnerability. The table below lists the various vulnerabilities that were newly targeted by exploit kits in 2015.

Exploit Kit	Application	Vulnerability
Angler	Flash	CVE-2015-8446, CVE-2015-7645, CVE-2015-5560, CVE-2015-5122, CVE-2015-5119, CVE-2015-3113, CVE-2015-3104, CVE-2015-3090, CVE-2015-0359, CVE-2015-0336, CVE-2015-0313, CVE-2015-0311, CVE-2015-0310
	Internet Explorer	CVE-2015-2419
	Silverlight	CVE-2015-1671
Magnitude	Flash	CVE-2015-7645, CVE-2015-5122, CVE-2015-5119, CVE-2015-3113, CVE-2015-3105, CVE-2015-3090, CVE-2015-0359, CVE-2015-0336, CVE-2015-0311
	Internet Explorer	CVE-2015-2419
	Silverlight	CVE-2015-1671
Nuclear	Flash	CVE-2015-7645, CVE-2015-5560, CVE-2015-5122, CVE-2015-5119, CVE-2015-3113, CVE-2015-3104, CVE-2015-3090, CVE-2015-0359, CVE-2015-0336, CVE-2015-0313, CVE-2015-0311
	Internet Explorer	CVE-2015-2419
Neutrino	Flash	CVE-2015-7645, CVE-2015-5122, CVE-2015-5119, CVE-2015-3113, CVE-2015-3090, CVE-2015-0359, CVE-2015-0336, CVE-2015-0313, CVE-2015-0311
	Internet Explorer	CVE-2015-2419
Rig	Flash	CVE-2015-5122, CVE-2015-5119, CVE-2015-3113, CVE-2015-3090, CVE-2015-0359, CVE-2015-0311
	Internet Explorer	CVE-2015-2419
Sundown	Flash	CVE-2015-0313, CVE-2015-0311
Hanjuan	Flash	CVE-2015-3113

Table 2. Exploits added to exploit kits in 2015 (by exploit kit)

Evasion Techniques

A standard part of analyzing and detecting exploit kit attacks is to analyze any network traffic that is generated. To combat this, in 2015 attackers started using encryption to protect their network traffic.

They did so by using the Diffie-Hellman key exchange algorithm to exchange encryption keys between the victim and the exploit kit servers. This protects the exploit file from network security products, since for starters they would be unable to scan and detect any transferred malicious files. Similarly, products that rely on traffic

capture to detect exploit-related activity would also become less effective, as traffic replay would no longer be effective.

In addition to hampering detection, these steps would also make life more difficult for researchers trying to analyze exploit kit activities.

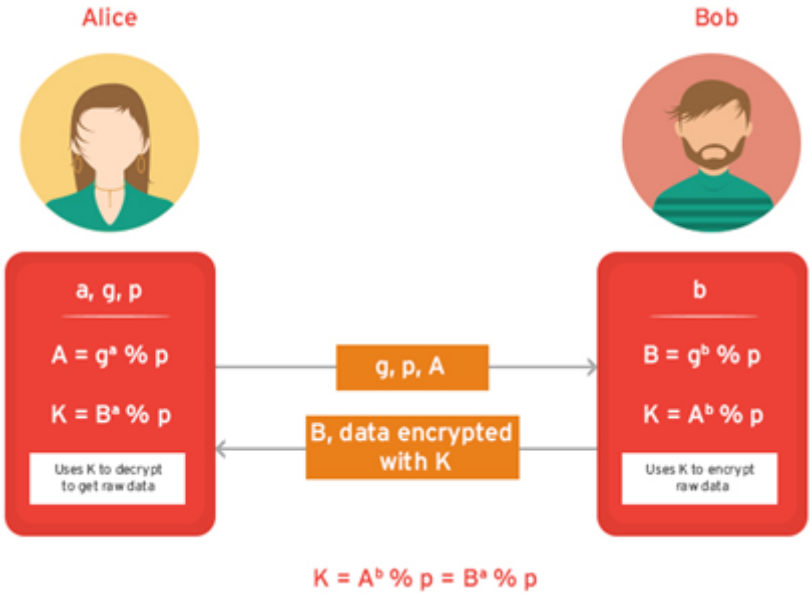


Figure 1. How the Diffie-Hellman protocol can be used to exchange data

Compromised CMS Sites and Malvertising

In 2015, there were two primary methods used to direct users to exploit kits: compromised sites and malvertising. Let's discus the former method first.

Compromised sites victimize users by redirecting visitors to visit a separate site that contains the exploit kit code. In many cases, these sites are easily compromised because of the content management system (CMS) software used for these servers.

In November 2015, we reported on the *ElTest* campaign which delivered ransomware to visitors of compromised websites using the Angler exploit kit. The campaign was able to take over more than 1,500 websites to distribute ransomware. The *ElTest* campaign usually added a SWF object to pages on the compromised website which loads another Flash file to inject a hidden iframe which leads to exploit kits. All of this is happening essentially unknown to the user.

ElTest was far from the only campaign that targeted websites in order to compromise them. However, all these campaigns shared similar characteristics: they targeted sites that run well-known CMSes like WordPress, Joomla, and Drupal. The affected sites were running unpatched and vulnerable versions of either these systems or widely used third-party add-ons, highlighting how important it is to keep these up to date. This combination of factors allowed attackers to target large numbers of websites and compromise them with a relatively low amount of effort expended, putting large numbers of users at risk.

Figure 2. Inserted SWF Object (Click to enlarge)

Alternately, advertising may be used to lead visitors to malicious sites – without them knowing any better. The vast majority of websites rely on advertising to help pay the bills, but these ads are rarely directly managed by the site owners. Instead, these are managed by ad networks. If these ad networks fail to insure that all ad buyers are legitimate, attackers can "buy" ad traffic and lead them to exploit kits. Site owners can find these attacks quite difficult to detect and remove, as it all takes place via the ad network, which they do not directly control.

Figure 3. Invisible iframe Hiding a Malvertisement

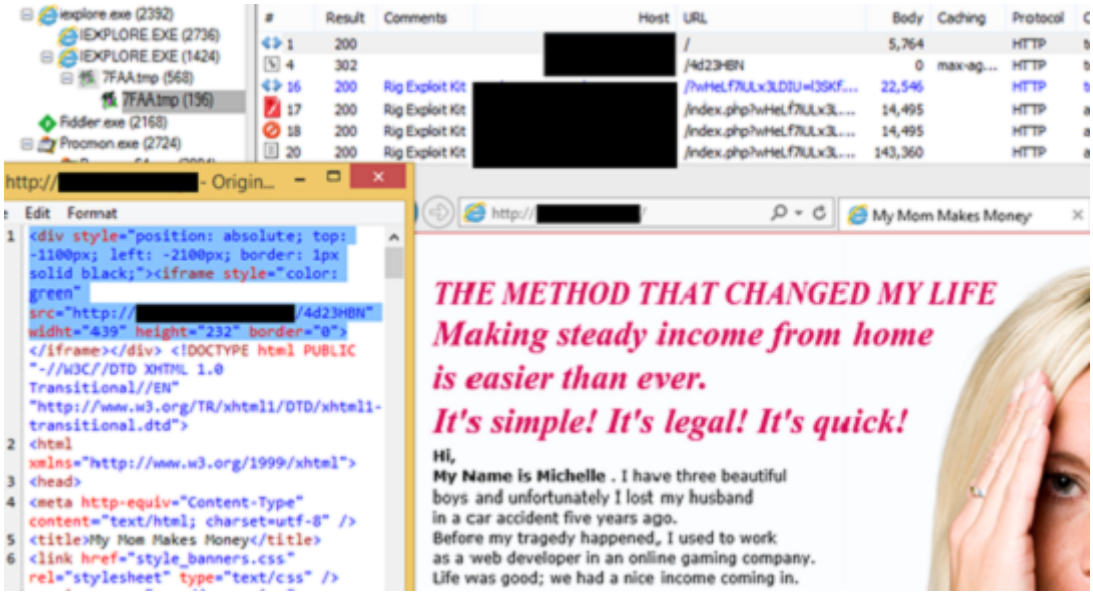


Figure 4. Pop-up advertisement leading to exploit kits

2015 saw many malvertisers use either banner/embedded ads or pop-up ads to send people to exploit kit pages. They would create a fake ad (or copy the picture from a legitimate one) and add scripts which would redirect the users to exploit kit pages in the background, without the user having to click anything or seeing anything unusual. As a result, an attacker can deliver their attacks to large numbers of users more quickly. Our data indicates that around 88% of exploit kit attacks in December 2015 were tied to malvertising.

	From Malvertising	**From Other Sources**
Angler Exploit Kit	89.32%	10.68%
Magnitude Exploit Kit	100%	0%
Neutrino Exploit Kit	39.80%	60.20%
Rig Exploit Kit	85.93%	14.07%
Nuclear Exploit Kit	33.81%	66.19%

Sundown Exploit Kit	100%	0%
Total	88.07%	11.93%

Table 4. Distribution of exploit kit traffic by source (December 2015)

Summary

Exploits kits have proved to be enormously powerful for years, and 2015 was no different. With such an effective tool in place there was no reason to expect radical changes; instead we saw more evolutionary changes in how they worked.

New vulnerabilities in software (particularly Adobe Flash) were rapidly integrated into exploit kits. Encryption is now being used to protect the network traffic of exploit kits, making detection and analysis more difficult. Both compromised CMSes and malvertisements are being used to victimize users with increasing frequency.

By themselves none of these are especially revolutionary. Taken together, however, they continue to make attacks using exploit kits more effective and attractive to cybercriminals. How big is this problem? That is something we will examine in the second blog post in this series.

Updated on March 16, 2016, 10:40 AM (UTC-7)

Updated to correct an information related to Sundown Exploit Kit. It was previously mentioned that a vulnerability in Internet Explorer (CVE-2015-2444) was incorporated in this Exploit Kit, but apparently it was not fully weaponized. We have updated the tables above to remove the said CVE.

Related Posts:

- **Angler and Nuclear Exploit Kits Integrate Pawn Storm Flash Exploit**
- **Hacking Team Flash Zero-Day Integrated Into Exploit Kits**
- **Latest Flash Exploit in Angler EK Might Not Really Be CVE-2015-0359**
- **Exploit Kits in 2015: Scale and Distribution**

Tags: Adobeadobe flashexploit kitInternet ExplorerVulnerabilities

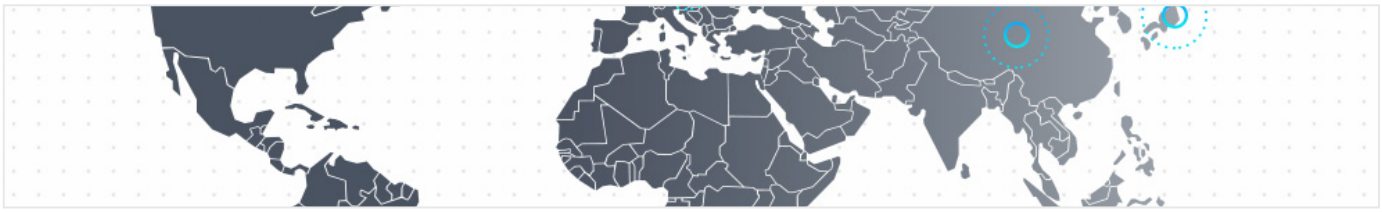
Featured Stories

- How Bad is Badlock (CVE-2016-0128/CVE-2016-2118)?
- ATM Malware on the Rise
- Mobile Devices Used to Execute DNS Malware Against Home Routers
- Indian Military Personnel Targeted by "Operation C-Major" Information Theft Campaign
- Massive Malvertising Campaign in US Leads to Angler Exploit Kit/BEDEP

Recent Posts

- US and European companies Top Targets of CEO Fraud
- April 2016 Patch Tuesday Releases 13 Security Patches; Addresses the Badlock Vulnerability
- How Bad is Badlock (CVE-2016-0128/CVE-2016-2118)?
- ATM Malware on the Rise
- Mobile Devices Used to Execute DNS Malware Against Home Routers

Cybercrime Across the Globe: What Makes Each Market Unique?

- 

  This interactive map shows how diverse the cybercriminal underground economy is, with different markets that are as unique as the country or region that it caters to.
  Read more

Business Email Compromise

- A sophisticated scam has been targeting businesses that work with foreign partners, costing US victims $750M since 2013.
  How do BEC scams work?

Popular Posts

Data Protection Mishap Leaves 55M Philippine Voters at Risk
PETYA Crypto-ransomware Overwrites MBR to Lock Users Out of Their Computers
Massive Malvertising Campaign in US Leads to Angler Exploit Kit/BEDEP
Android Vulnerabilities Allow For Easy Root Access
CERBER: Crypto-ransomware that Speaks, Sold in Russian Underground

Latest Tweets

- Are enterprises prepared for crypto #ransomware? bit.ly/1PYjYkR #infosec #cybersecurity
  about 3 hours ago

- New post: US and European companies Top Targets of CEO Fraud bit.ly/263mlPg @TrendMicro
  about 7 hours ago
- @TrendLabs Brazil is the right answer! For more details, check out this link! bit.ly/1qtuzja

  about 8 hours ago

Stay Updated

Email Subscription

Your email here

Subscribe