TrendLabs

SECURITY INTELLIGENCE BLOG

Threat News and Information Direct from the Experts

TREND MICRO

Bad Sites | Botnets | CTO Insights | Exploits | Internet of Everything | Mac | Malware | Mobile | Social | Spam | Targeted Attacks | Vulnerabilities

blog.trendmicro.com Sites > TrendLabs Security Intelligence Blog > Exploits > Exploit Kits and Malvertising: A Troublesome Combination

Mar16

Exploit Kits and Malvertising: A Troublesome Combination

12:00 am (UTC-7) | by Brooks Li and Joseph C. Chen (Threats Analysts)

Share Tweet

In the past few weeks we've noticed a problematic pattern developing: the increasing use of exploit kits in malvertising. In particular, zero-day exploits (usually seen first in targeted attacks) are now being deployed in malicious ads right away, instead of first being used in targeted attacks against enterprises or other large organizations.

This is a worrying trend, as it means that more users could be affected by these threats before a patch becomes available. Two of the recent Adobe Flash zero-days (CVE-2015-0311 and CVE-2015-0313) were delivered to end users via malvertisements, putting large numbers of users at risk.

We recently released a paper titled *The Evolution of Exploit Kits* which discusses the threat from exploit kits. This paper continues our previous discussion and outlines the existing threat from these today, which are a key tool in the arsenal of attackers today. We also partially delve into the history of exploit kits, including the notorious Blackhole exploit kit, which collapsed with the arrest of its author in late 2013.

Some patterns in the attacks from 2014 are expected to continue into 2015, such as:

- Increasing targeting of Flash vulnerabilities for exploitation. Previously, Java and Acrobat/Reader vulnerabilities were some of the most frequently targeted by exploit kits.
- We saw fewer exploit kit "brands" in use in 2014. This was in contrast to previous years, where the number of exploit kit "brands" was growing. However, the kits that are currently being actively developed are becoming more sophisticated, with increasing use of evasion techniques.

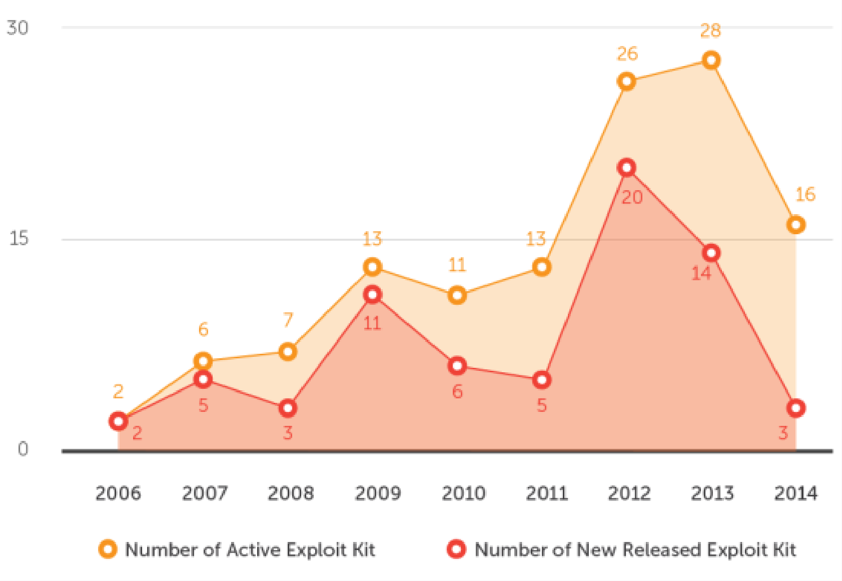

Figure 1. Number of exploit kits in use

What can users and enterprises do to protect themselves against these threats? The most important defense against an exploit kit is to keep installed versions of software as up-to-date. While zero-days are seeing more usage in exploit kits, older vulnerabilities that have already been patched are still widely used. By keeping their software updated, end users can mitigate much of the risk associated with these risks.

Search our blog:

Go

Targeted Attacks

- How Targeted Attacks Changed in 2014
- Kjw0rm VBS Malware Tied To Attacks on French TV Station TV5Monde
- Securing The IT Supply Chain

Bookmark the Threat Intelligence Resources site to stay updated on valuable information you can use in your APT defense strategy

Recent Posts

- Behind Tax Fraud: A Profile of 3 IRS Scammers
- April 2015 Patch Tuesday Issues Updates to Microsoft Office
- How Targeted Attacks Changed in 2014

Calendar

April 2015

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

« Mar

Email Subscription

Email Subscription

Your email here

Subscribe

About us

Security products can also help mitigate the risks. Products with smart sandboxes can be used to help find and detect malicious behavior, including zero-day exploits. In addition, products that use web and file reputation detection can also block the redirection chain and detect payloads.

Share this article

Get the latest on malware protection from TrendLabs

This entry was posted on Monday, March 16th, 2015 at 12:00 am and is filed under Exploits, Vulnerabilities . You can leave a response, or trackback from your own site.

CTO Insights: Vulnerabilities for Sale

Bypassing ASLR with CVE-2015-0071: An Out-of-Bounds Read Vulnerability

Other Trend Micro blogs

- CTO Insights
- CounterMeasures Blog
- Cloud Security Blog
- Consumerization Blog
- Fearless Web
- Internet Safety for Kids & Families
- Simply Security News
- Trend Micro Blog [German]
- TrendLabs Security Blog [Japan]
- Cloud Security APAC

Do you have a product-related question? Visit our eSupport website.