- Trend Micro
- About TrendLabs Security Intelligence Blog

TrendLabs SECURITY INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Search:

Go to…

- Home
- Categories

Home » Exploits » Tracking the Decline of Top Exploit Kits

Tracking the Decline of Top Exploit Kits

- Posted on:February 14, 2017 at 5:09 am
- Posted in:Exploits, Vulnerabilities
- Author:
  Giannina Escueta (Technical Communications)

0

The latter half of 2016 saw a major shift in the exploit kit landscape, with many established kits suddenly dropping operations or switching business models. As we discussed in our 2016 Security Roundup, Angler, which has dominated the market since 2015, suddenly went silent. We tracked 3.4 million separate Angler attacks on our clients in the first quarter of 2016, while the rate of attacks suddenly fell to a flat zero in the latter half of the year.

There was a significant change on the overall rate of attacks. Our data shows that exploit kit attacks in 2016 were only a third of what they were in 2015—from almost 27 million detected down to 8.8 million. We can trace the events that led to the conclusion of Angler activity, as well as what triggered the general drop in most exploit kit activity.

Major Factors Impacting Exploit Kits

Based on previous events, law enforcement seems to be most effective in disrupting exploit kit operations. In late 2013, the arrest of BlackHole author "Paunch" by Russian authorities took out the most damaging kit of the past year. After the arrest, BlackHole suddenly ceased operations and a vacuum was left in the market. This triggered a shift that made Angler the prime exploit kit in 2015, with 57.25% of all recorded exploit kit attacks. In 2016, history seemed to repeat itself. Fifty people in Russia were arrested and the event is widely credited for the plunge in Angler operations. The recent arrests also probably caused the end of Nuclear operations, although as noted before, it had been losing traction since 2015.

Aside from the arrests, the current dip in exploit kit attacks can also be attributed to the lack of zero-day vulnerabilities. Compared to previous years, 2016 saw less zero-days, particularly in perennial exploit kit favorites like Adobe Flash, Internet Explorer, and Java. Currently, most kits rely on outdated exploits, which translates to lower success rates. Also, kits that used to quickly incorporate exploits for new vulnerabilities have slowed down.

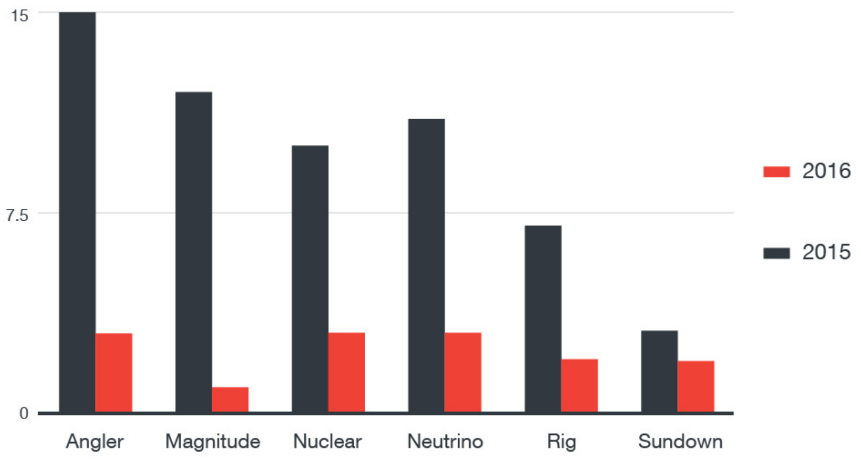

Figure 1. Rate of new vulnerabilities incorporated by exploit kits by year

Enterprises and users are also becoming more aware of and proactive about security, updating software and relying on professionals to defend systems against known exploits. These combined factors mean exploit kits are significantly less successful.

Updated Tools and Payloads Mean Exploit Kits Still a Relevant Threat

Although there is a lack of potent zero-days and slower integration of new vulnerabilities, exploit kits still remain a threat. Older kits in circulation can cause damage to unprotected users, particularly those that don't with no defenses in place and do not update their software. Some exploit kits zero-in on older systems; one example is Magnitude which still targets outdated versions of Flash players.

Developers behind these kits have proven adaptable in the past and are expected to evolve their arsenal and continue adopting effective obfuscation techniques. Past examples of this include the adoption of antivirus detection, which allowed some kits to detect security software and also shut down if certain products are installed. There are also kits that misuse legitimate applications to hide their activity—in the past the Angler kit used Pack200, which compresses files. Magnitude and the FlashPack exploit kit used a commercially available Flash-centric tool called DoSWF to obscure files.

Exploit kit operators are also constantly taking on new infection techniques, trying to keep pace with new security technology and savvier targets. In 2016 we saw an uptick in the use of images to hide malicious code. In July, we saw the AdGholas malvertising campaign, which is associated with the Astrum exploit kit, start encoding malicious script into an image's alpha channel. The slight variance in color was the only thing that separated a legitimate ad from one infected with the malware.

In December, we also identified that the Sundown kit was updated to use steganography. The authors hid the exploit code in a white PNG image. The kit's malvertisement connects victims to the Sundown landing page, which retrieves the image with the exploit code. Though the vulnerabilities used in this version have all been patched, outdated systems might still be susceptible.

The payloads dropped by exploit kits are also regularly updated. Ransomware is a common payload, and was first adopted into exploit kits in 2013. The tandem proved to be very popular with cybercriminals and more operators jumped on the trend, much to the detriment of their targets. Victims now have to deal with the ransomware infection along with whatever other payload the kit is dropping. CryptoWall, Tesla, and CryptoLocker were the choice options from 2013 to 2015, until exploit kits included a variety of other ransomware in 2016.

The Future of Exploit Kits

If the trend continues and no new exploits for popular browsers appear, we can expect cybercriminals to turn away from exploit kits and return to more effective means of dropping their payloads—social engineering tactics like phishing or spam mail. Recently, spam seems to be the preferred method for delivering ransomware.

Though there is a lull in activity, exploit kits still pose a risk and are expected to evolve as they have been doing for the past few years. And since law enforcement in certain countries, particularly Russia, seem to be successful at shutting down exploit kit operators and developers, criminals will start to avoid these countries. Distributors will shift their attention to areas that don't have the knowledge of more targeted nations. Countries with less experience dealing with exploit kits are likely to be more vulnerable.

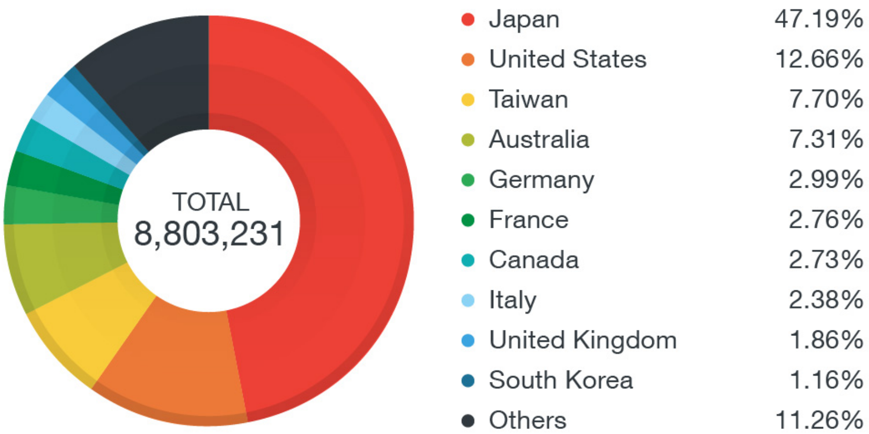

Figure 2. Countries most affected by exploit kit attacks in 2016

We can expect the business models to continuing changing as well. We may see more customized exploit kits for private use—the Neutrino kit is an example of this technique. Managing customers privately, focusing on select targets, and keeping a low profile helps avoid detection. This model also helps kits avoid being tracked by security products.

New exploit kits are likely to pop up to fill the vacuum left behind by Angler, Nuclear, and Neutrino, despite the availability of exploits, law enforcement, and other factors that impact the landscape. And it is safe to assume that popular payloads—ransomware, banking Trojans, information stealers and botnets—ransomware, banking Trojans, information stealers and botnets—will still be distributed through exploit kits. Developers will most likely find new evasion techniques to prevent detection. It is also likely that they will try and make exploit kit traffic more similar to normal traffic—using techniques like steganography or masking it as ad traffic.

Exploit kits are a constant and evolving threat, and developers continue to adopt new strategies. To address this, a cross-generational security solution that can detect and counteract future variants is necessary; as well as solutions with high fidelity machine learning which can help detect and block exploits in real-time.

Trend Micro leverages XGen™ security across all solutions—it has advanced techniques such as behavioral analysis, machine learning and sandbox analysis to quickly and accurately handle harder-to-detect, unknown threats. And all of these capabilities are fueled by the Trend Micro Smart Protection Network, which uses threat intelligence to detect and manage zero-hour threats. Products with Web Reputation Services protect clients at a network level. The existing Sandbox with Script Analyzer engine, which is part of Trend Micro™ Deep Discovery, can be used to detect threats by their behavior without any engine or pattern updates. Our endpoint products such as Trend Micro™ Security, Smart Protection Suites, and Worry-Free Business Security uses the Browser Exploit Prevention feature to prevent exploits from running on affected systems, preempting any possible threats from taking root.

With additional insights from Joseph C. Chen

Related Posts:

- **Updated Sundown Exploit Kit Uses Steganography**

Featured Stories

- IIS 6.0 Vulnerability Leads to Code Execution
- Winnti Abuses GitHub for C&C Communications

- MajikPOS Combines PoS Malware and RATs to Pull Off its Malicious Tricks
- New Linux Malware Exploits CGI Vulnerability
- CVE-2017-5638: Apache Struts 2 Vulnerability Leads to Remote Code Execution

2016 Annual Security Roundup

- 2016 was an unprecedented year for cybersecurity, particularly for enterprises. The Trend Micro™ Smart Protection Network™ blocked over 81 billion threats in 2016, a 56% increase from the threats blocked in 2015.
  Read our 2016 Annual Security Roundup

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

Cerber Starts Evading Machine Learning

TorrentLocker Changes Attack Method, Targets Leading European Countries

CERBER Changes Course, Triple Checks for Security Software

Unix: A Game Changer in the Ransomware Landscape?

Brute Force RDP Attacks Plant CRYSIS Ransomware

Recent Posts

- April Patch Tuesday: Microsoft Patches Office Vulnerability Used in Zero-Day Attacks
- How Mobile Phones Turn Into A Corporate Threat
- Smart Whitelisting Using Locality Sensitive Hashing
- IIS 6.0 Vulnerability Leads to Code Execution
- Cerber Starts Evading Machine Learning

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

CVE-2017-5638: Apache Struts 2 Vulnerability Leads to Remote Code Execution
IIS 6.0 Vulnerability Leads to Code Execution
Winnti Abuses GitHub for C&C Communications
Cerber Starts Evading Machine Learning
MajikPOS Combines PoS Malware and RATs to Pull Off its Malicious Tricks

Latest Tweets

- How do you keep your child’s smart device safe from potential attacks? Tips: bit.ly/2nD2lWb #IoT

  about 5 hours ago
- We predict that #BusinessProcessCompromise will gain traction this year. What you need to know about the threat:… twitter.com/i/web/status/8…
  about 8 hours ago
- Smart buildings need smarter security. Learn how to protect your systems from network attacks:… twitter.com/i/web/status/8…
  about 11 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