# Exploit Kits in 2015: Scale and Distribution

- Posted on:March 15, 2016 at 5:43 pm
- Posted in:Exploits, Vulnerabilities
- Author:
  Brooks Li and Joseph C. Chen (Threats Analysts)

0

In the first part of this series of blog posts, we discussed what new developments and changes in the exploit kit landscape were seen in 2015. In this post, we look at the scale of the exploit kit problem – how many users were affected, which exploit kits are popular, and where are the users coming from?

The data was taken from analysis of exploit kit URLs that were blocked by Trend Micro products over the entirety of 2015. This information represents a sizable sample of the overall threat landscape. This allows us to observe any long-term trends in the overall landscape and protect our users accordingly.

In 2015, we detected and blocked approximately 14 million visits to exploit kit-related URLs aimed at users from all over the world. Figure 1 shows the quarterly progression of the number of these blocked visits. The biggest increase took place from Q1 of 2015 to Q2. By Q4, the number we saw per quarter had doubled from the year before. This is a significant increase in the level of exploit kit activity by any measure.

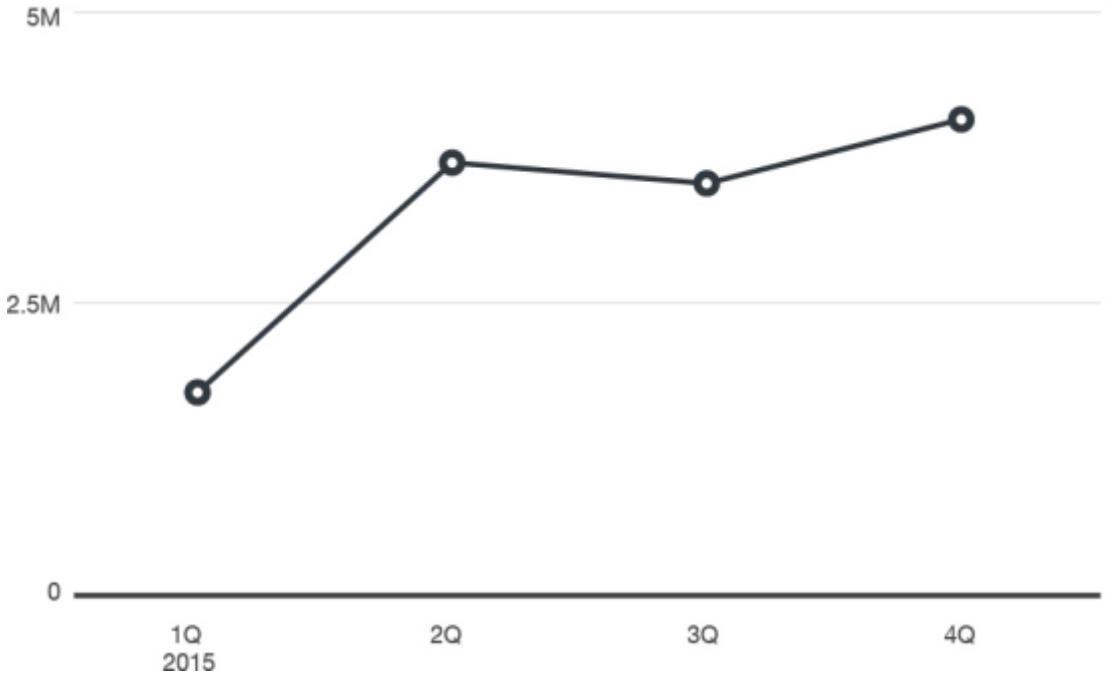



*Figure 1. Number of Detected Exploit Kit Attacks in 2015*

Was any single exploit kit responsible for this increase in activity? No. However, three exploit kits made up the bulk of exploit kit activity in 2015: Angler, Nuclear, and Magnitude. Angler, in particular, is well-known for its timely integration of newly discovered exploits to its arsenal. Together these three kits made up 86% of all exploit kit activity in the previous year, as the chart below shows:

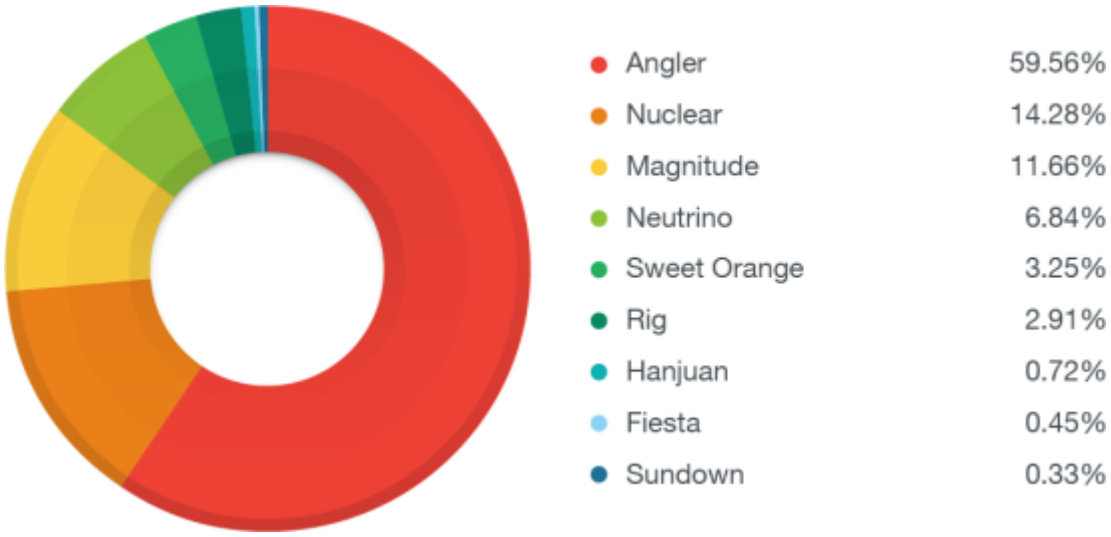



*Figure 2. Distribution of Detected Exploit Kit Attacks in 2015*

All three of the dominant exploit kits were previously active in 2014 and continued to be used throughout 2015. Other kits that saw consistent usage in both years were Neutrino and Rig. However, some exploit kits that were commonly used in 2014 died off as 2015 progressed: both Fiesta and Sweet Orange were in this category. A new exploit kit, Sundown, was introduced to the market in 2015.

Our data indicates that users in Japan and the United States were the most targeted by exploit kits in 2015, a continuation of the pattern from 2014. Users in Japan were targeted by multiple kits, with particular spikes occurring in March (Nuclear), April (Neutrino), and a sustained increase over the summer months (Rig). By the second half of the year, Japanese users were most frequently hit by the Angler exploit kit, largely due to ongoing malvertising campaigns.

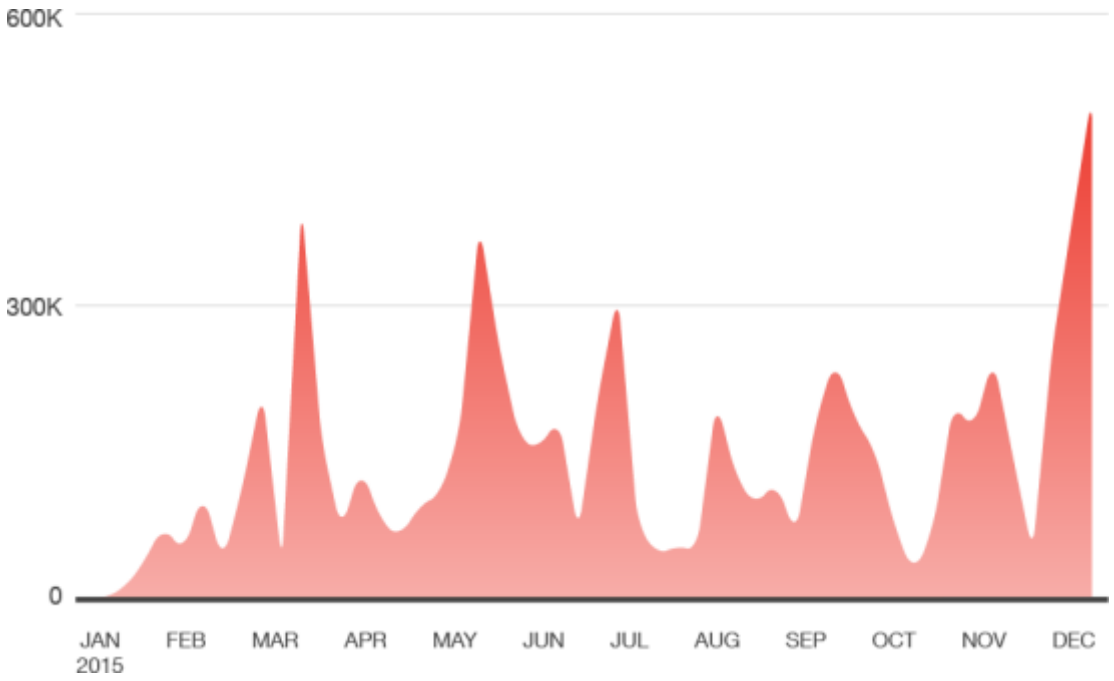



*Figure 3. Weekly Count of Exploit Kit traffic in Japan*

In the United States, there were also similar spikes over the 12-month period. Early in the year Hanjuan caused a spike due to its use of a zero-day exploit. In April and July, an increase in activity was tied to the Magnitude exploit kit. The increase in July may be tied to an Adobe Flash vulnerability that was added to Magnitude in June. Like Japan, by the second half of the year Angler exploit kit was the most prominent threat for users. Other countries that were prominent target of exploit kits were Australia, Canada, France, Germany, and the United Kingdom.

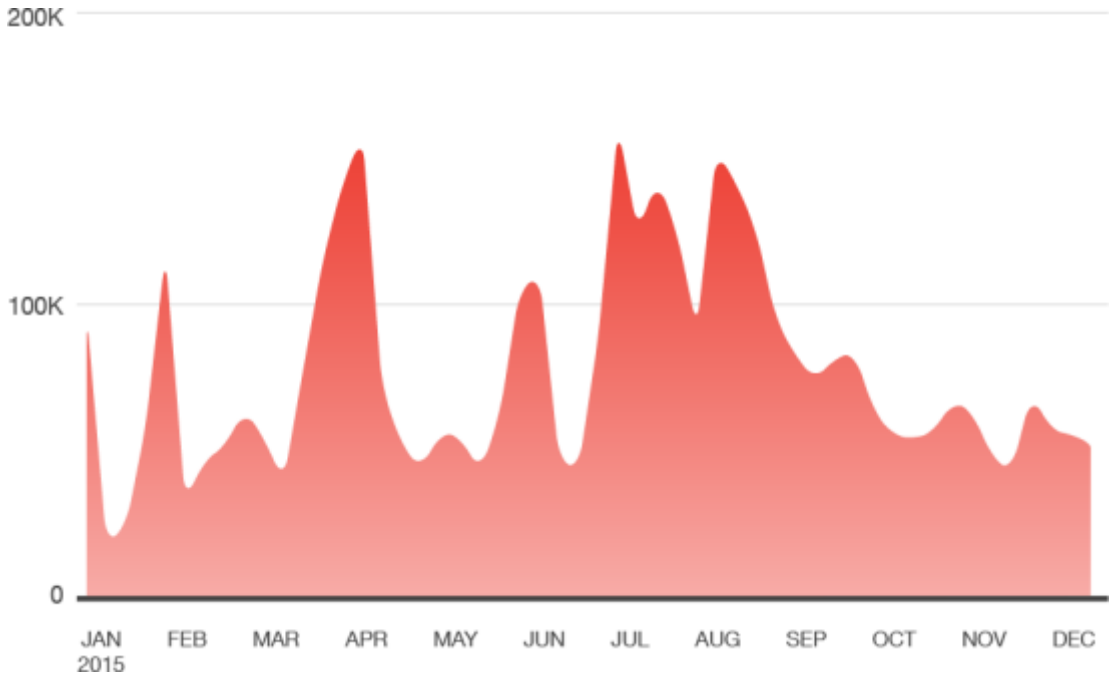



*Figure 4. Weekly Count of Exploit Kit traffic in the United States*

If we look at the distribution of where the targets of the top three exploit kits are located, the patterns are broadly similar to the global findings: the Angler and Nuclear exploit kits most affected users in Japan. Almost half of Magnitude exploit kit targets were in the United States.

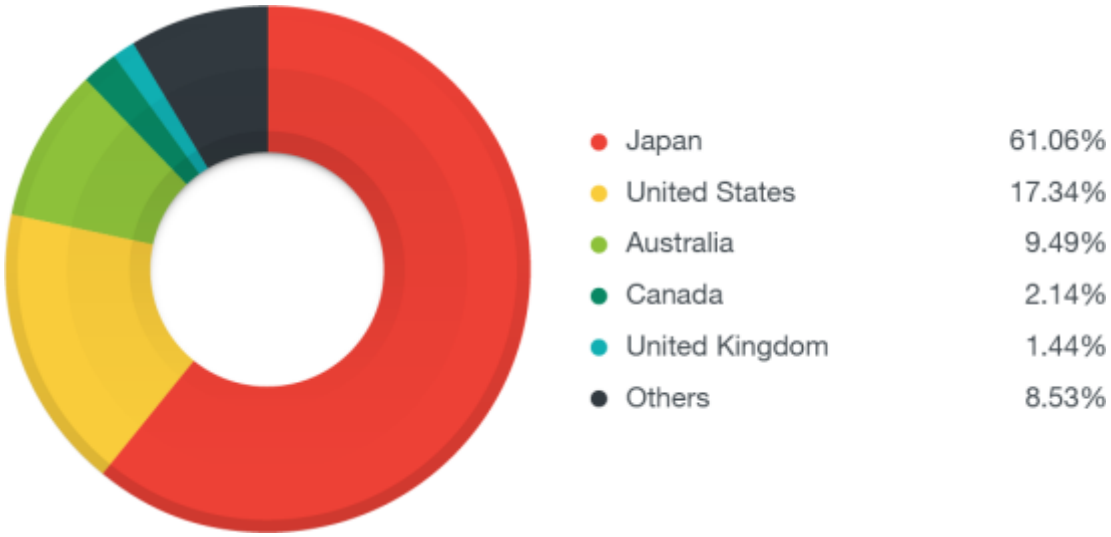



*Figure 5. Global distribution of Angler Exploit Kit traffic in 2015*

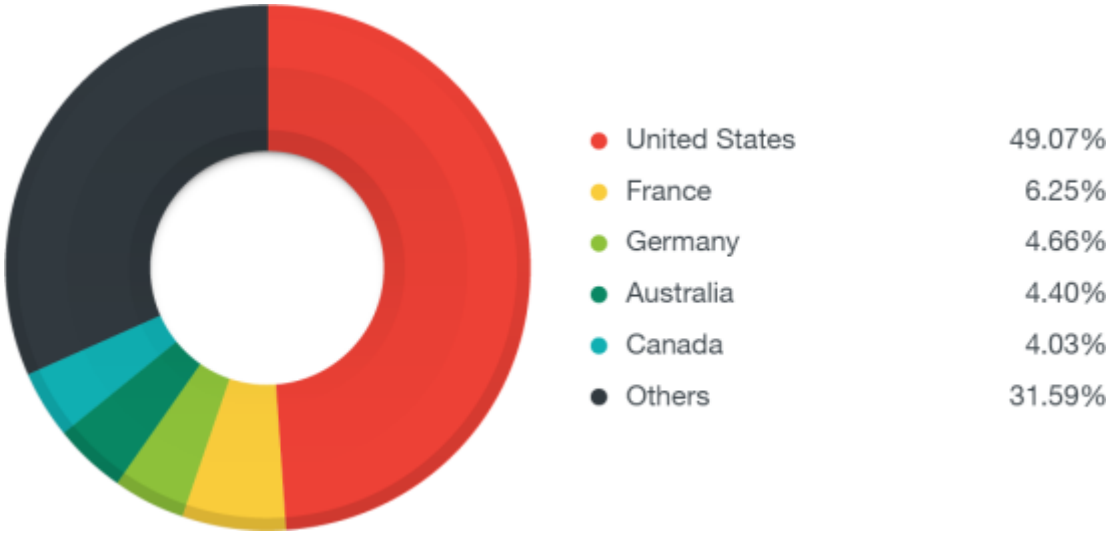



*Figure 6. Global distribution of Magnitude Exploit Kit traffic in 2015*

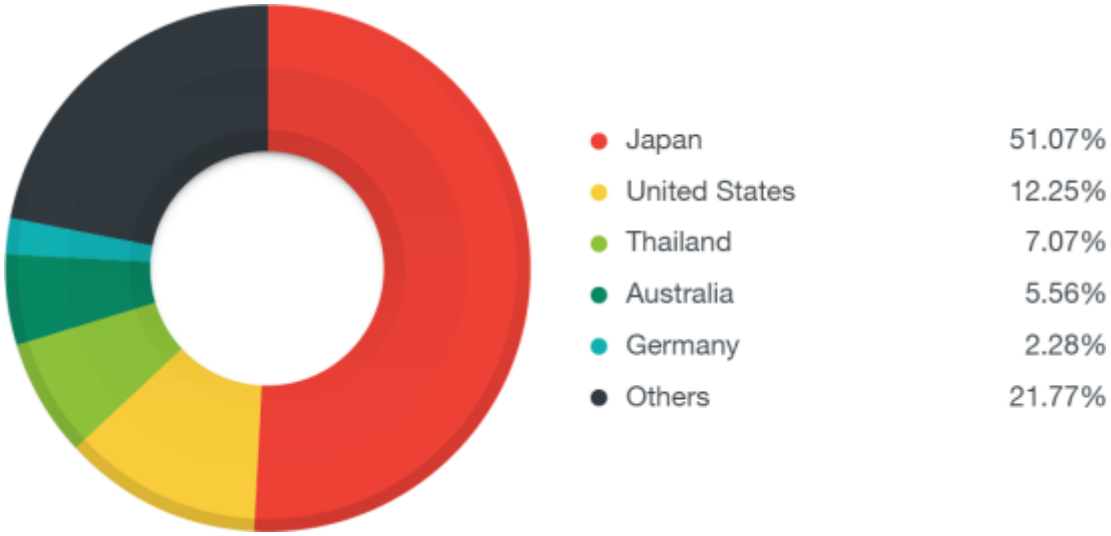



*Figure 7. Global distribution of Nuclear Exploit Kit traffic in 2015*

***Trend Micro Solutions***

Trend Micro products and solutions defend against exploit kits in a variety of ways. Trend Micro™ Deep Discovery uses the Sandbox with Script Analyzer to detect this threat by its 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.

***Summary***

2015 saw significant growth in the number of exploit kit attacks seen in the wild, thanks in part to the strategies and tactics that were employed throughout the year. The period of highest growth was the second quarter of the year.

As for who was affected, our data indicates that users in Japan and the United States were most affected. Other countries that were frequent victims were Australia, Canada, France, Germany, and the United Kingdom.

Exploit kits have been a significant threat for years, and so long as vulnerable applications continue to be in widespread use they will continue to be a threat. The best way to deal with exploit kits has not really changed either. We strongly urge users and system administrators to keep software up to date to minimize the potential risk window to any exploits in use.


## Related Posts:

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




Tags: Anglerexploit kitmagnitude


## Featured Stories

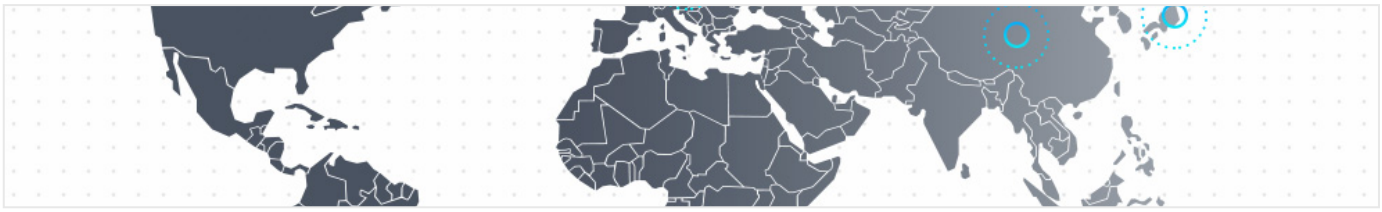
- Indian Military Personnel Targeted by "Operation C-Major" Information Theft Campaign
- Olympic Vision Business Email Compromise Campaign Targets Middle East and Asia Pacific Companies
- Massive Malvertising Campaign in US Leads to Angler Exploit Kit/BEDEP

- Android Vulnerabilities Allow For Easy Root Access
- The Aftermath: 2015 Breaches and Other Threat Trends

## Recent Posts

- Tax Day Extortion: PowerWare Crypto-ransomware Targets Tax Files
- Critical 'CVE-2015-1805' Vulnerability Allows Permanent Rooting of Most Android Phones
- PETYA Crypto-ransomware Overwrites MBR to Lock Users Out of Their Computers
- Indian Military Personnel Targeted by "Operation C-Major" Information Theft Campaign
- Online Banking Threats in 2015: The Curious Case of DRIDEX's Prevalence

## 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

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
Hacking Team Flash Zero-Day Integrated Into Exploit Kits
Cybercriminals Improve Android Malware Stealth Routines with OBAD

## Latest Tweets

Error: Rate limit exceeded

## 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