Tech Brief: An inside view of a zero-day campaign

Jerome Segura
Senior Security Researcher, Malwarebytes

Overview

Discovering a new vulnerability in a popular piece of software is the Holy Grail for cybercriminals. The period between this vulnerability being weaponized into an exploit and becoming public knowledge poses a huge security risk to consumers and businesses. During this time, a completely open window of attack exists because even fully-patched systems are affected. This is a zero-day.

This paper details one such exposure using Malwarebytes' unique view of zero-day threats as collected through its anti-exploit products. Because the anti-exploit products are deployed on a large user base that spans the globe, researchers were able to profile accurately a zero-day (CVE-2015-0313) that leverages Adobe Flash Player, and shine a light on the lifecycle, delivery mechanism, and criminal practices behind it.

Why we chose this zero-day

There have been three Flash Player zero-days so far in 2015, but the reasons we focused on this was because:

- Targeting was very specific, adding to its potency and showing a clear capability for organization.
- The Malwarebytes data shows a lengthy attack campaign—nearly two months between December 2014 and early February 2015.
- The potentially high volume of infections achieved by the poisoning of advertisements on high-volume sites.

Tech Brief: An inside view of a zero-day campaign

Jerome Segura
Senior Security Researcher, Malwarebytes

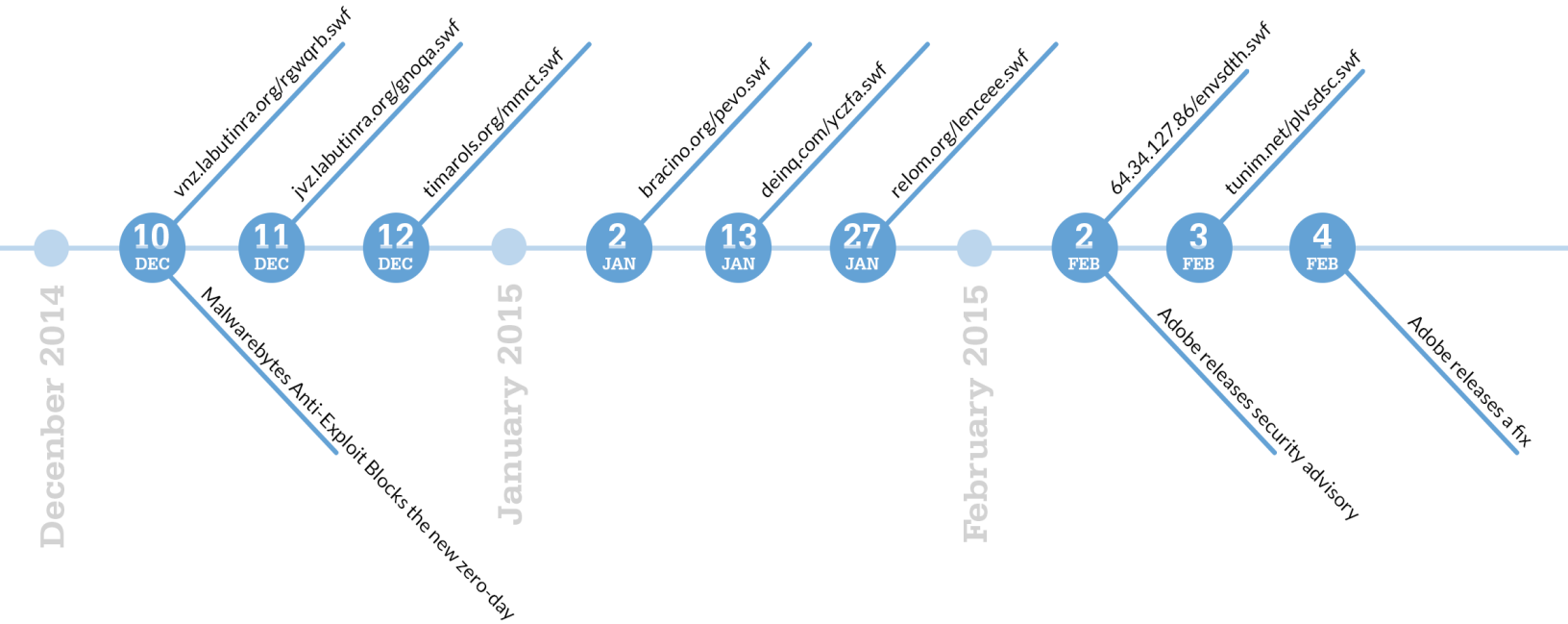
TOP-LINE FACTS

CVE-2015-0313: Adobe Flash vulnerability, fixed with version 16.0.0.305.
Delivery: Malvertising on a popular ad network using the HanJuan exploit kit. The exploit was hosted on a rotating series of domains.
Window of exposure: First seen 12/10/2014; made public 2/2/2015.
Payload: Crypto Ransomware/click fraud.

TIMELINE

This zero-day campaign is notable for its length, lasting approximately two months. Typically, such exploits have a relatively short shelf life due to discovery by the security or research community. This campaign remained below the radar for a longer than usual period of time, as follows:

First seen: Retrospective data analysis shows the first instance of the zero-day being blocked by Malwarebytes Anti-Exploit on December 10, 2014.
Dynamic domains: The campaign rotated the exploit landing page around numerous domains, each hosting it for approximately two days on average.
Campaign exposed: The final day of this particular campaign was February 3, 2015—one day after Adobe issued a security advisory that publicly alerted everyone to the zero-day. Adobe issued a fix (patch) one day later.
Take-up by others: The exploit, now not a true zero-day given its "known" status, is quickly integrated into other exploit kits.



See full timeline at http://mwb.to/TechBrief

Tech Brief: An inside view of a zero-day campaign

Jerome Segura
Senior Security Researcher, Malwarebytes

TARGETING

The actors used a highly targeted mass malvertising campaign to deliver the zero-day threat.

Scale: Delivered using a well-known advertising network that claims to have a reach of 500+ million uniques, and is "ranked No. 1 in the U.S." by Comscore by reaching 97% of Internet users.
Known targets: Geo-targeted at U.S. consumers, and aimed at residential IP addresses at particular times of day to ensure the highest possible return. Each visitor was pre-qualified by OS type, device, and other demographics to ensure only the most relevant were served the exploit.
Stealth: Each individual visitor was exposed to the exploit just once, and would not infect anyone using a VPN or web proxy, ensuring it remained hidden from security researchers and software.
Costs: Threat actors paid an average of $0.75 per each 1000 pre-qualified users exposed to the infected adverts. However, this dropped to as low as $0.06 per 1000 during less trafficked times of day and on lesser-known websites.

TRAFFIC GUARANTEED

To maximize the exposure window, the bad actors chose to advertise on an array of highly ranked websites to deliver the zero-day. Whilst stealth was important, the importance of volumes of infections was also notable:

Respected sites: Throughout the campaign, some of the most respected sites on the planet were delivering the threat, including Dailymotion and Huffington Post. People's innate "trust" for such sites enabled the group to infect visitors with minimal suspicion.
Traffic numbers: Similarweb.com shows the collective number of visits to the websites offering the zero-day to be over one billion in February 2015. It should be pointed out that this is an external data point that does not directly equate to a number of infections; rather, it gives an approximate idea of potential visitors exposed. The previously mentioned targeting features used, and natural cycling of advertisements on site, would filter overall visitor numbers down to live infection prospects.

Domain Name	Website rank by traffic (Alexa)	Site visits per month (Similarweb, Feb 2015)
dailymotion.com	82	360m
huffingtonpost.com	92	209.5m
sexuality.about.com	137	subdomain so exact number unknown
dictionary.reference.com	170	62.3m
gmx.com	231	8.4m
answers.com	334	69.7m
nydailynews.com	563	37.1m
tagged.com	800	44.9m
forums.androidcentral.com	908	17.2m
howtogeek.com	914	51.3m

Jerome Segura
Senior Security Researcher, Malwarebytes

CONCLUSIONS

This particular zero-day has all the hallmarks of a highly professional operation with significant resources. The precision with which it was targeted and its ability to avoid detection demonstrates significant forward thinking. This was a well planned and executed attack that leveraged the availability of cheap, yet highly effective, modern ad-serving technology to great effect.

Malvertising allows cyber criminals to target popular websites, which would normally be practically impossible to hack directly. Instead, crooks piggy back on ad networks that are already trusted and allowed. To use a metaphor, the bad guys are not attempting to go through a Maginot line, but, rather, are simply going around it.

The HanJuan exploit kit that was used to deliver this zero-day is notoriously quiet compared to its counterparts. Also, the URL patterns that it uses are rather standard looking and don't really allow it to be identified. Had this zero-day been in another exploit kit, such as Angler EK, there's no doubt but that it would have been spotted much sooner.

In addition, both the length with which the campaign was able to run and the volumes of traffic visiting the impacted sites point to a high volume of successful infections. It is impossible to say for sure without access to the exploit kit back-end, but the threat to Internet users from an unknown vulnerability such as this will amplify its success rate exponentially.

All in all, this zero-day underlines how the threat from exploits delivered through malvertising is one that should be taken much more seriously. Not just because of the growing technical proficiency of well-funded adversaries, but also because this is a trend that continues largely unregulated in the major markets wherein victims are specifically targeted. Malvertising is increasing in frequency and, when combined with a zero-day, can prove devastatingly effective. It is a problem, and one that the advertising industry should be working closely with security companies and regulators to address.

About Malwarebytes

Malwarebytes provides anti-malware and anti-exploit software designed to protect businesses and consumers against zero-day threats that consistently escape detection by traditional antivirus solutions. Malwarebytes Anti-Malware earned an "Outstanding" rating by CNET editors, is a PCMag.com Editor's Choice, and was the only security software to earn a perfect malware remediation score from AV-TEST.org. That's why more than 38,000 SMBs and Enterprise businesses worldwide trust Malwarebytes to protect their data. Founded in 2008, Malwarebytes is headquartered in California, operates offices in Europe, and employs a global team of researchers and experts.