Mozilla to Enforce Signing for Firefox Extensions Soon

Ryan Naraine on SAS 2015

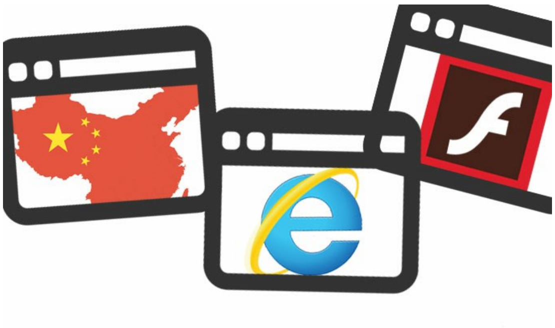
Chinese Hackers Compromised Forbes.com Using IE, Flash Zero Days

Author:
Chris Brook

February 11, 2015
/ 4:07 pm

2:30 minute read

Share this article:



A Chinese APT group has been linked to a watering hole attack on Forbes.com used to target defense and financial targets.

A Chinese APT group was able to chain together two zero day vulnerabilities, one against Adobe's Flash Player and one against Microsoft's Internet Explorer 9, to compromise a popular news site late last year.

The group's aim was to gain access to computers at several U.S. defense and financial firms by setting up a watering hole attack on the site that would go on to drop a malicious .DLL.

Researchers with Invincea and iSIGHT Partners worked in tandem to dig up information about the group, which was able to compromise a part of Forbes.com's website that appears to users before they're ported over to articles they've clicked on. That portion of the site, Forbes.com's Thought of the Day, is powered by a Flash widget.

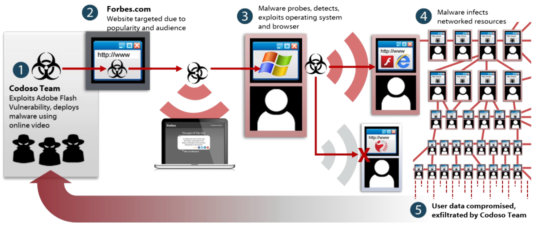
According to researchers with Invincea the group was able to use a zero day vulnerability to hijack that widget for a short period, from Nov. 28 to Dec. 1. Over the course of those four days, the group targeted visitors to the site who worked at a handful of unnamed U.S. defense and financial firms.

Researchers with iSIGHT discovered that in addition to the Flash flaw, the attackers also exploited an Internet Explorer vulnerability, a zero day that helped attackers bypass Address Space Layout Randomization (ASLR) in IE 9.

While the Adobe bug, a buffer overflow (CVE-2014-9163) was patched back on Dec. 9, the ASLR mitigation bypass (CVE-2015-0071) was one of many patched yesterday in Microsoft's monthly Patch Tuesday round of patches, an update that was especially heavy on Internet Explorer fixes.

In a technical writeup of the attack yesterday, Invincea explained how Forbes' site was able to redirect to an IP address, load the Flash exploit, and drop a DLL, hrn.dll, to be loaded into the machine's memory.

"Once in memory, the exploit gains administrative privileges and opens a command prompt," Invincea's executive summary reads, "Next the victim system was scanned to report on its current patch levels, network mapping, and complete IP configuration, including any VPN connections."


1
Codoso Team
Exploits Adobe Flash Vulnerability, deploys malware using online video
2
Forbes.com
Website targeted due to popularity and audience
http://www
3
Malware probes, detects, exploits operating system and browser
4
Malware infects networked resources
5
User data compromised, exfiltrated by Codoso Team

Both firms agreed to set their disclosures for yesterday to coincide with Microsoft's patching of the Internet Explorer bug.

While Chinese APT groups have been in the news lately – some reports have already pinned last week's Anthem breach on shadowy hackers from the PRC – several firms are already familiar with the APT group behind this campaign. FireEye, first published research on the group back in 2013, referring to the collective as the Sunshop Group. Researchers there caught the group carrying out a campaign that hit a series of victims – a science and technology journal, a website for evangelical students, etc. – by exploiting an IE zero day and several Java bugs in May of that year.

> Chinese APT group uses IE, Flash zero days to compromise Forbes.com, via @threatpost
>
> Tweet

Throughout its research, dating back to 2010, iSIGHT has taken to calling the group Codoso Team. This attack, like others its linked back to them, used similar malware (Derusbi) and called on a command and control (C+C) domain its been seen using in the past as well.

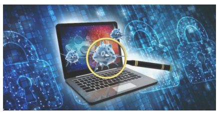
Regardless of what it goes by, the group has been seen targeting U.S. government entities, the military/defense sector, and financial services groups for at least five years running. FireEye found the same group was also responsible for hacking the Nobel Peace Prize Committee website in 2010. That attack also used a watering hole and made use of a browser (Firefox) zero day.

While neither iSIGHT or Invincea could give concrete numbers regarding the number of victims Codoso was able to compromise with this campaign, both were firm in their stance that the attacks were highly targeted in nature and only visitors who worked at the defense and financial firms were infected.

Share this article:

Government Malware

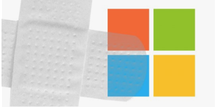
SUGGESTED ARTICLES



Coronavirus-Themed APT Attack Spreads Malware

The APT group was spotted sending spear-phishing emails that purport to detail information about coronavirus – but they actually infect victims with a custom RAT.

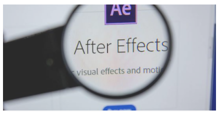
March 13, 2020



Microsoft Exchange Server Flaw Exploited in APT Attacks

A vulnerability is Microsoft Exchange servers is being actively exploited by multiple APT groups, researchers warn.

March 9, 2020



Critical Adobe Flaws Fixed in Out-of-Band Update

Two critical Adobe vulnerabilities have been fixed in Adobe After Effects and Adobe Media Encoder.

February 20, 2020

DISCUSSION