FireEye
SECURITY REIMAGINED

WHITE PAPER

ZERO-DAY DANGER:

A Survey of Zero-Day Attacks and What They Say About the Traditional Security Model

CONTENTS

Introduction

Zero-day vulnerabilities are software flaws that leave users **exposed to cyber attacks before a patch or workaround is available.**

Of all the hazards confronting enterprise IT systems, zero-day vulnerabilities are among the most harmful.

Zero-day vulnerabilities are software flaws that leave users exposed to cyber attacks before a patch or workaround is available. Sometimes, a zero-day vulnerability is unknown to anyone but a cyber attacker (or a supplier who sells zero-day discoveries on the black market). In other cases, the software vendor knows about the flaw but has not yet issued a fix.

Although all software probably has unknown vulnerabilities, these flaws become especially threatening "in the wild" when discovered by attackers and used to launch cyber assaults.

By definition, they are unknown and unpredictable, exposing systems of even the most diligent users and administrators. Even enterprises with big-ticket defenses in place are wide open to attack.

Patching your systems will not stop them. Updating malware definitions on anti-virus (AV) software will not stop them. In many cases, not even multi-layered "defense-in-depth" security schemes are enough to prevent a zero-day attack from hitting your IT assets.

"There is almost no defense against a zero-day attack," as one security report puts it. "While the vulnerability remains unknown, the software affected cannot be patched, and anti-virus products cannot detect the attack through signature-based scanning."[1]

This paper explains the dangers of zero-day attacks and why traditional defenses are powerless against them. It also outlines 18 zero-day attacks discovered by FireEye since late 2012, and how they were used in real-world attacks. Finally, the paper recommends 11 practical steps to reduce the risks of zero-day attacks.

[1] Leyla Bilge and Tudor Dumitras (ACM Conference on Computer and Communications Security). "Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World." October 2012.

Zero-Day Exploits Alarmingly Common

Zero-day threats are everywhere. On any given day over the last five years, cybercriminals had access to at least 85 vulnerabilities targeting widely used software from Microsoft, Apple, Oracle, and Adobe.[2] That estimate includes only vulnerabilities that were eventually reported. The true number of zero-day vulnerabilities available to cybercriminals could be much higher.

Vulnerabilities discovered by cybercriminals remain unknown to the public—including vendors of the software—for an average of 310 days.[3]

Not surprisingly, zero-day exploits are heavily used in targeted attacks. These secret weapons give attackers a crucial advantage over their targets, even those that have invested millions of dollars into conventional security products.

Thanks to an abundance of zero-day vulnerabilities and increasingly mature global black market for exploits, these weapons are proliferating. Governments remain the top buyers of zero-day exploits, according to a Reuters article.[4] But anyone with enough money—as little as$5,000 in some cases[5]—can purchase one.

In mid-2015, a marketplace calling itself TheRealDeal Market emerged from the shadows of the darknet. Unlike other, similar markets, the focus of TheRealDeal was exclusively dedicated to brokering hackers' premium zero-day attack methods—often for exclusive, one-time sales. TheRealDeal uses the anonymity software Tor and the digital currency bitcoin to hide the identities of its buyers and sellers.[6]

Vulnerabilities discovered by cybercriminals remain unknown to the public—including vendors of the software—for an average of

310 days

[2] Kelly Jackson Higgins (Security Dark Reading). "Hacking The Zero-Day Vulnerability Market." December 2013.
[3] Andy Greenberg (Forbes). "Hackers Exploit 'Zero-Day' Bugs For 10 Months On Average Before They're Exposed." October 2012.
[4] Joseph Menn (Reuters). "Special Report: U.S. cyberwar strategy stokes fear of blowback." May 2013.
[5] Andy Greenberg (Forbes). "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits." March 2012.
[6] Andy Greenberg (Wired). "New Dark-Web Market Is Selling Zero Day Exploits To Hackers." April 17, 2015.

Standard Defenses are Powerless Against Zero-Day Threats

Traditional security tools rely on malware binary signatures or the reputation of outside URLs and servers. By definition, these defenses identify only known, confirmed threats. An attacker can easily hijack a legitimate website to bypass a blacklist.

Code morphing and obfuscation techniques generate new malware variants faster than traditional security firms can generate new signatures. And spam filters will not stop low-volume, targeted spear-phishing attacks.

At the same time, operating system-level protections such as Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) are becoming less effective. Several zero-day exploits discovered by FireEye in recent years used ASLR-bypassing methods that have all but neutered this once-effective safeguard.[7]

It's no wonder that the typical zero-day attack lasts an average of eight months—and can last close to three years in some cases.[8] That gives attacks ample time to steal organizations' most valuable assets and leave before anyone knows what happened.

The typical zero-day attack lasts an average of eight months. **That gives attacks ample time to steal organizations' most valuable assets.**

[7] Xiaobo Chen (FireEye). "ASLR Bypass Apocalypse in Recent Zero-Day Exploits." October 2013.
[8] Leyla Bilge and Tudor Dumitras (ACM Conference on Computer and Communications Security). "Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World." October 2012.

FireEye Zero-Day Discoveries

Since just before New Year's Day 2013 through mid-2015, FireEye has discovered and reported 18 zero-day vulnerabilities. That's by far the most of any cyber security company. In fact, it's more than all the other top-10 vendors (as ranked by security-related revenue) combined. This gap underscores the difficulty in detecting zero-day attacks, especially by conventional cyber defenses.

Many security researchers identify software flaws—some as a byproduct of detecting attacks and others as a core focus. Nearly all of them responsibly, and privately, send information about the flaws to the software publisher to fix.[9] Some of these flaws are critical holes,such as those exploited in globally popular software like Internet Explorer. Others are never-exploited flaws in obscure software.

FireEye has found many zero-day exploits "in the wild." These are the zero-day flaws being used in active attacks. In 2013, FireEye discovered 11 of these zero-day exploits. We discovered five more in 2014 and two in the first half of 2015.

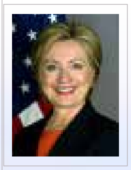
Zero-day exploits used by advanced persistent threat (APT) attackers represent some of the most critical cyber threats. Even if APT attackers do not target an organization, other criminal exploit authors often reverse the zero-day exploit and create their own version before patches can be released.

Here are the FireEye-reported zero-day vulnerabilities since late 2012, which are explained in the corresponding sections:

- CVE-2012-4792
- CVE-2013-0422
- CVE-2013-0634
- CVE-2013-0640 / CVE-2013-0641
- CVE-2013-1493
- CVE-2013-1347
- CVE-2013-3893
- CVE-2013-5065
- CVE-2013 -3918 / CVE-2014-0266
- CVE-2014-0502
- CVE-2014-0322
- CVE-2014-1776
- CVE-2014-4113 / CVE-2014-4148
- CVE-2014-0502
- CVE-2015-3043
- CVE-2015-3113

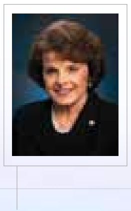
[9] Zheng Bu (FireEye). "Zero-Day Attacks Are Not the Same as Zero-Day Vulnerabilities." April 24, 2014.

JANUARY 2013



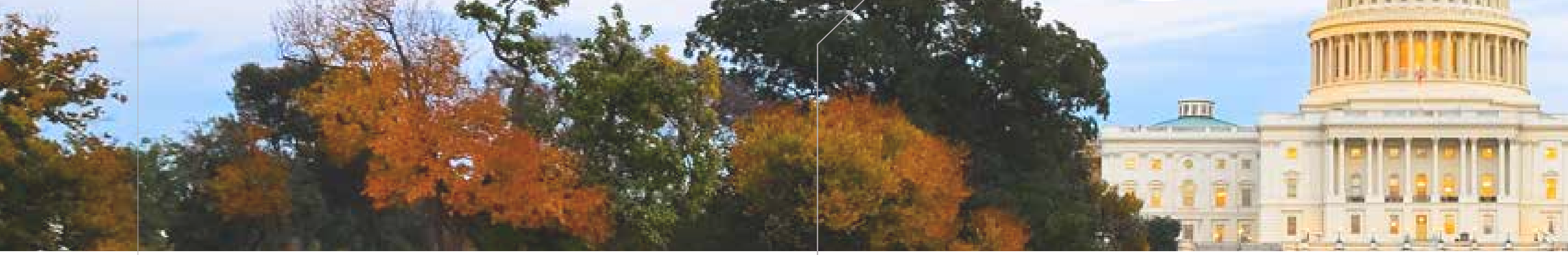
Former Secretary of State **HILLARY CLINTON**

Secretary of State **JOHN KERRY**



Former Senate Intelligence Committee Chairman Sen **DIANNE FEINSTEIN**

TOBFY SCREENSHOT



CVE-2012-4792

Discovered close to New Year's Day,[10] this vulnerability allows attackers to execute code on machines of Internet Explorer (IE) users who visit malicious websites. The exploit takes advantage of a "use-after-free" flaw. This hole appears when faulty code tries to improperly access memory that has been "freed up" for another purpose. The problem can allow attackers to remotely execute malicious code on a targeted system.

In this case, the malicious code was JavaScript hidden in the website of Council on Foreign Relations (CFR), a well-known foreign-policy group. The intended targets are unknown, but CFR members include Secretary of State Sen. John Kerry, former Senate Intelligence Committee Chairman Sen. Dianne Feinstein, and former Secretary of State Hillary Clinton.[11]

CVE-2013-0422

CVE-2013-0422, which was exploited as early as January 2, 2013,[12] is a Java 7 vulnerability that allows attacks to bypass Java security checks and executes code on a target machine. Though the exploit was designed for Windows, the vulnerability probably left other operating systems that run Java open to attack.

Attacks exploiting this flaw download ransomware known as Tobfy, which locks users out of their computer. It displays a full-screen message, purportedly from the FBI, accusing the user of a crime. If the victims pay a "fine" via wire transfer, the message promises, they can unlock their computer.

Tobfy also disables Windows Safe Mode. And it terminates processes such as taskmgr.exe, msconfig.exe, regedit.exe, and cmd.exe to deter users from trying to find or disable the malware.

Because of a coding mistake, the malware cannot communicate with the attacker—including letting the attacker know that the user has paid the ransom and should remove itself from the system. So even if targets paid up, they still could not access their PC.

[10] Darien Kindlund (FireEye). "CFR Watering Hole Attack Details." December 2012.
[11] Bill Gertz (The Washington Free Beacon). "Chinese Hackers Suspected in Cyber Attack on Council on Foreign Relations." December 2012.
[12] Yichong Lin (FireEye). "Happy New Year from New Java Zero-Day." January 2013.

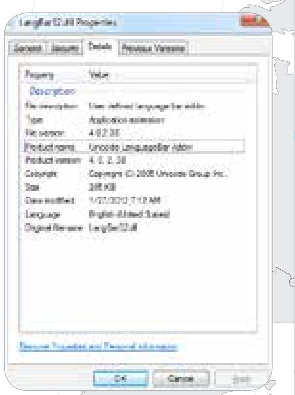
FEBRUARY 2013

LADY BOYLE

a character in the video game "Dishonored" is the likely namesake for a Flash exploit used in February 2013.

Photo credit: Arkane Studios. Used under Creative Commons Attribution-ShareAlike 3.0 Unported license

LANGBAR DIALOGUE BOX

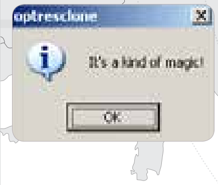


LangBar32.dll Properties

Property	Value
Description	
File description	User defined language bar addin
Type	Application extension
File version	4.0.2.38
Product name	Unicode LanguageBar Addin
Product version	4.0.2.38
Copyright	Copyright (C) 2008 Unicode Group Inc.
Size	395 KB
Date modified	1/17/2013 7:12 AM
Language	English (United States)
Original filename	LangBar32.dll

WEAPONIZED PDF

KIND OF MAGIC DIALOGUE BOX



optresclone

It's a kind of magic!

CVE-2013-0634

Identified on February 7, 2013,[13] this Adobe Flash vulnerability allows attackers to run malicious ActionScript code on Windows, Macs, Linux, and even Android mobile devices.[14]

The exploit was used in a cyber espionage campaign dubbed "LadyBoyle." Attacks exploiting this vulnerability sent Microsoft Word documents to target Windows users. The Word files contain a macro to load an embedded SWF Flash object.

The SWF file, in turn, contains an ActionScript with the name "LadyBoyle" that contains the exploit code. The exploit supports only a limited version of Flash, and it checks for the presence of ActiveX component, a Windows-only feature.

Once it has reached its target, the SWF file exploits the Flash Player flaw to run the payload DLL and embedded executables. The payload itself was from a known malware family that had been used in previous campaigns. One of the dropped executable files is digitally signed with an invalid certificate from MGAME Corporation, a Korean gaming company. The executable renames itself to try to pass itself off as the Google update process.

From there, the malware creates a startup entry (so it can restart after a reboot) and checks for anti-virus (AV) software. Oddly—and perhaps sloppily—the malware payload was not encrypted or obfuscated.

CVE-2013-0640 / CVE-2013-0641

Attackers exploited this pair of PDF vulnerabilities to install a remote administration tool (RAT) with a flexible, extensible architecture. Attackers can add new features easily with plug-in dynamic-link libraries (DLLs). The malware shellcode bypassed ASLR and DEP security features, upping the ante in the security arms race.

The JavaScript embedded in the crafted PDF is well hidden using string-manipulation techniques. The JavaScript checks the version of Adobe Reader running on the target system and creates shellcode tailored to it.

Attackers dropped three DLLs onto the target system that work in harmony to steal information. The main component (LangBar) inserts itself into Windows processes and helps manage other DLLs used in the attack. The second DLL (lbarhlp) performs most of the data-stealing functions. And the third DLL (lbarext) packages and encrypts the stolen data.

The malware, dubbed "666," was used in a spear-phishing email campaign against Japanese targets. The emails contained a weaponized PDF attachment purporting to be a security report.

[13] Thoufique Haq and J. Gomez (FireEye). "LadyBoyle Comes to Town with a New Exploit." February 2013.
[14] National Vulnerability Database. "Vulnerability Summary for CVE-2013-1493." March 2013.

MARCH 2013

SOUTH KOREAN MILITARY

and strategy think tanks were among the targets of the Sunshop campaign.

CVE-2013-1493

This Java Runtime Environment vulnerability allows attackers to compromise the integrity of the HotSpot virtual machine. It bypasses Java's Security Manager to manipulate heap memory and execute malicious code.[15]

Attacks exploiting the flaw downloaded the McRAT Trojan to give attackers control over the targeted systems. The exploit was unusual because it allowed attackers to read and write memory directly within the Java Virtual Machine process. It also reflected the trend of targeted attacks bypassing ASLR. Until then, ASLR had been one of the best safeguards for operating systems.

The zero-day exploit was one of three (along with Internet Explorer zero-day vulnerability CVE-2013-1347 and Java exploit CVE-2013-2423) used in the Sunshop campaign over the summer.[16] Sunshop compromised several strategic websites including:

- Multiple Korean military and strategy think tanks
- A Uyghur news and discussion forum
- A science and technology policy journal
- A website for evangelical students

MAY 2013

THE U.S. DEPARTMENT

of labor employees were the target of a watering hole attack that exploited an IE vulnerability.

CVE-2013-1347

Like CVE-2013-1493, this IE vulnerability was used in the Sunshop campaign.[17] It uses an ASLR-bypass technique to exploit a use-after-free vulnerability in IE versions 6 through 8 running on Windows XP.

In addition to Sunshop-related attacks, the exploit was used in a watering hole attack against visitors to the U.S. Department of Labor website, typically federal employees.[18] JavaScript embedded into the site redirected visitors to a site hosting the Poison Ivy RAT, which gives attackers control of target systems.

SEPTEMBER 2013

"DEPUTY DOG"

targeted organizations in Japan.

CVE-2013-3893

This IE vulnerability allows attackers to execute code on machines of users who visit maliciously crafted websites. It anchored a malware campaign dubbed "Deputy Dog."

The campaign began as early as August and targeted organizations in Japan. At least three other APT campaigns—dubbed Web2Crew, Taidoor, and th3bug—used the same exploit.

[15] Ned Moran (FireEye). "Ready for Summer: The Sunshop Campaign." May 2013.
[16] Ibid.
[17] Ibid.
[18] Lin (FireEye). "IE Zero-Day is Used in DoL Watering Hole Attack." May 2013.

NOVEMBER 2013

U.N. GENERAL ASSEMBLY BUILDING

PHOTO CREDIT: BASIL D SOUFI

CVE-2013-3918 / CVE-2014-0266

These ActiveX vulnerabilities affected nearly every version of Windows from XP Service Pack 2 onward. It allows attackers to execute malicious code on machines of IE users who visited maliciously crafted websites.

Attackers used this flaw in an "exceptionally accomplished and elusive" watering hole attack dubbed "Operation Ephemeral Hydra." It targeted a website known to draw visitors that are likely interested in national and international security policy.[19] The attack used the same infrastructure as the Deputy Dog campaign (see CVE-2013-3893). And the Trojan used in both attacks included a text string that also appeared in the infamous Operation Aurora attacks of 2009.

In a twist likely to make detection, forensics, and remediation tougher, the attackers loaded the payload in this attack directly into computer memory without writing anything to disk. So when an infected computer reboots, nearly all traces of the attack disappear. [20]

WINDOWS XP ACCOUNTS

CVE-2013-5065

Identified on November 27, 2013, this Windows XP and Windows Server 2003 vulnerability escalated local-user privileges. This change allowed a standard user account to execute code in the kernel.[23] Although the flaw does not allow attackers to execute code remotely, remote attackers can use it with other vulnerabilities to that end.

Attackers exploited CVE-2013-5065 along with CVE-2013-3346, an Adobe Reader flaw patched in May 2013. The targeted attacks used a weaponized PDF to drop the malware payload into a temporary directory in Windows and execute it.

[19] Ned Moran, et al (FireEye). "Operation Ephemeral Hydra: IE Zero-Day Linked to DeputyDog Uses Diskless Method." November 2013.
[20] Ms. Smith (NetworkWorld). "IE zero-day attack delivers malware into memory then poofs on reboot." November 2013.

FEBRUARY 2014

THE VETERANS OF FOREIGN WARS

website was targeted in Operation Snowman in February 2014.

AMERICAN RESEARCH CENTER IN EGYPT CONSERVATORS

clean the wall of "Theban Tomb 110" near the Nile River in Luxor, Egypt. The group's website was one of several compromised in Operation Greedy Wonk.

PHOTO CREDIT: JULIE FOSSLER, USAID

CVE-2014-0322

We saw watering-hole exploits accelerate in 2014 and 2015. CVE-2014-0322, which we identified on February 11, 2014, is a prime example.

The attack targeted American military personnel amid a paralyzing snowstorm at the U.S. Capitol in the days leading up to the 2014 Presidents' Day holiday weekend (We named the attack, naturally, "Operation Snowman.") We believe the attackers behind the campaign are connected with two earlier campaigns: Operation Deputy Dog and Operation Ephemeral Hydra.

The attack targeted IE 10 users visiting U.S. Veterans of Foreign Wars' (VFW) website (vfw.org).[21] The site, which draws past and current members of the U.S. military, was hijacked to deliver malicious drive-by downloads.

The exploit downloaded an XOR-encoded payload from a remote server, decoded it, and executed it. Given that the VFW website draws both retired and active service members, the attackers may have been trying to steal military intelligence.[22]

CVE-2014-0502

On February 13, 2014, FireEye identified a zero-day exploit that affects the latest version of the Flash player (12.0.0.4 and 11.7.700.261).[23] Visitors to at least three nonprofit institutions—two of which focus on matters of national security and public policy—were redirected to an exploit server hosting the zero-day exploit. We called this attack "Operation Greedy Wonk."

Greedy Wonk may be related to a May 2012 campaign uncovered by the Shadowserver Foundation.[24] Both attacks targeted the same kind of websites and used similar techniques, attack infrastructures, and malware configuration properties.

The group behind Greedy Wonk appeared to have ample resources, such as access to zero-day exploits. And it seemed determined to infect visitors to foreign and public policy websites. The attackers likely sought to infect users to lay the groundwork for future data theft, including information related to defense and public policy matters.

[21] Yichong Lin (FireEye). "New IE Zero-Day Found in Watering Hole Attack." February 13, 2014.
[22] Ibid.
[23] Dan Caselden, Jen Weedon, Ziaobo Chen, Mike Scott, Ned Moran (FireEye). "Operation GreedyWonk: Multiple Economic and Foreign Policy Sites Compromised, Serving Up Flash Zero-Day Exploit." February 20, 2014.
[24] Steven Adair and Ned Moran (The Shadowserver Foundation). "Cyber Espionage & Strategic Web Compromises—Trusted Websites Serving Dangerous Results." May 15, 2012.

APRIL 2014

OPERATION CLANDESTINE FOX

exploited a vulnerability in most versions of IE that bypassed ASLR and DEP protections.

OCTOBER 2014

CVE-2014-4148

exploited the Microsoft Windows TrueType Font (TTF) processing subsystem.

Helvetica Neue 25 Ultra Light
Helvetica Neue 35 Thin
Helvetica Neue 45 Light
Helvetica Neue 55 Roman
Helvetica Neue 65 Medium
Helvetica Neue 75 Bold
Helvetica Neue 85 Heavy
Helvetica Neue 95 Black

APRIL 2015

"OPERATION RUSSIAN DOLL"

attacked a government entity that is a known target of the Russian group that we track as APT28.

PHOTO CREDIT: 0X010C [CC BY-SA 4.0, VIA WIKIMEDIA COMMONS

CVE-2014-1776

On April 26, 2014, FireEye identified a zero-day vulnerability that affected IE versions 6 through 11, though the attacks exploiting it targeted users running version 9 and up. The attacks bypassed standard cyber defenses—including ASLR and DEP— allowing malicious code to access the memory of compromised machines at will.[25]

Attackers used the exploit in a campaign that we dubbed "Operation Clandestine Fox." It was a significant zero-day threat—the vulnerable versions collectively account for more than a quarter (26.25%) of the total browser market. The exploit dropped its payload using a new use-after-free vulnerability along with an older Flash exploit technique.[26]

CVE-2014-4148

We identified these two zero-day vulnerabilities on October 14, 2014. Both zero-days exploit the Windows kernel and were and used in two small but highly targeted attacks.[27]

CVE-2014-4148 exploited the Microsoft Windows TrueType Font (TTF) processing subsystem, It used a Microsoft Office document to embed and deliver a malicious TTF to an international organization.

CVE-2014-4113

CVE-2014-4113 rendered Microsoft Windows 7, Vista, XP, Windows 2000, Windows Server 2003 R2, and Windows Server 2008 R2 vulnerable to a local elevation-of-privilege (EoP) attack. The exploit can't be used on its own. An attacker would first need to gain access to a remote system running any of these Windows versions before executing code within the Windows kernel.

We found that attackers have likely used variants of these exploits for a while. We have no evidence of these exploits being used by the same actors. Instead, we have observed each exploit being used separately in unrelated attacks.

CVE-2015-3043

On April 13, 2015, FireEye detected a limited APT campaign exploiting zero-day vulnerabilities in Adobe Flash (CVE-2015-3043) and Windows (CVE-2015-1701).[28]

Attackers exploited the vulnerabilities together to attack a government entity that is a known target of the Russian group that we track as APT28.

Using HTML and JavaScript in a website controlled by the attackers, the attack first exploited the Flash vulnerability to download shellcode. This shellcode, in turn, exploited CVE-2015-1701 to gain control of the user's system. We dubbed this highly targeted attack "Operation Russian Doll."

We first detected a pattern of attacks using the FireEye Dynamic Threat Intelligence Cloud (DTI). By correlating the technical indicators and command-and-control infrastructure, we concluded that APT28 is probably behind the attack.

[25] Xiaobo Chen, Mike Scott, Dan Caselden (FireEye). "New Zero-Day Exploit targeting Internet Explorer Versions 9 through 11 Identified in Targeted Attacks." April 26, 2014.

[26] Xiaobo Chen (FireEye). "ASLR Bypass Apocalypse in Recent Zero-Day Exploits." October 15, 2014.

[27] Dan Caselden (FireEye). "Two Limited, Targeted Attacks; Two New Zero-Days." October 14, 2014.

[28] FireEye Labs. "Operation Russian Doll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack." April 18, 2015.

JUNE 2015

AEROSPACE AND DEFENSE FIRMS were among the targets of a spear-phishing campaign by the China-based threat group that FireEye tracks as APT3.

CVE-2015-3113

In June 2015, the FireEye as a Service team uncovered a phishing campaign exploiting an Adobe Flash Player zero-day vulnerability (CVE-2015-3113). The attackers' emails included links to compromised web servers that, depending on the system accessing the servers, served either benign content or a malicious Adobe Flash Player file that exploits CVE-2015-3113. (By the end of June 2015, Adobe had already released a patch for CVE-2015-3113 with an out-of-band security bulletin.)

The China-based threat group that FireEye tracks as APT3—also known as UPS—is responsible for this exploit. This group is one of the more sophisticated threat groups that FireEye Threat Intelligence tracks. It has a long history of introducing new browser-based zero-day exploits. What's more, APT3's command-and-control (CnC) infrastructure is difficult to track because its campaigns have few telltale overlaps.

In the first weeks of June 2015, APT3 actors launched a large-scale phishing campaign exploiting CVE-2015-3113 against organizations in the following industries:

- Aerospace and defense
- Construction and engineering
- High tech
- Telecommunications
- Transportation

FireEye dubbed this campaign Clandestine Wolf, after the 2014 zero-day attack by the same threat group that responsible for Clandestine Fox.

CONCLUSION

The zero-day vulnerabilities discovered from 2013 to present day reflect several trends that should prompt organizations to reassess their security posture:

- Operating system-level safeguards are becoming less effective against zero-day attacks. ASLR and DEP were big steps forward, but attackers are finding ways around them.
- Watering hole attacks are growing more common. By compromising trusted websites that cater to well-defined audiences, attackers can target precise industry or government segments. And rather than having to find ways into targeted systems, attackers can wait for the targets to come to them.
- Attacks are growing more sophisticated. Random crimeware and clumsy, high-volume attacks still occur. But laser-focused attacks against high-value targets are mushrooming. And these attacks are becoming much more adept at bypassing organizations' defenses.

Defending your IT assets against zero-day threats requires a fundamentally new approach to cyber security. Yesterday's signature-based defenses are not built for today's tidal wave of exploits.

Reputation-based defenses cannot detect brand-new attacks or those that commandeer trusted websites and servers to do their dirty work. And file-based sandboxes, which are easily fooled by the newest generation of malware, often miss zero-day attacks.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. FireEye has over 3,100 customers across 67 countries, including over 200 of the Fortune 500.

Expecting the Unexpected: **11 Steps to Reduce Your Risk**

Today's security professionals must equip themselves for not only known threats, but the new reality of unknown threats. To paraphrase the ancient Greek philosopher Heraclitus: expect the unexpected.[29]

To that end, FireEye recommends the following:

1. Segment your networks. Limit access between network segments with different risk profiles. This step includes limiting access from the Internet to the DMZ, the DMZ to the internal network, and so on. Prevent systems in one functional unit from accessing systems in another when they don't need to. Do not allow systems in the finance unit, for instance, to access systems in the engineering group. This move can block an attacker's access to an unpatched vulnerability.

2. Limit network privileges. Users and applications should access only the information and resources that are required to function. This step can shrink your "attack surface," because some attacks require elevated privileges to work. It also reduces the risk posed by a successful attack—compromising one system won't automatically grant attackers control of other systems.

3. Use application white listing. By allowing user to install only preapproved software, you can prevent unauthorized files from executing. This includes some executable exploits and malware payloads.

4. Have an incident response (IR) plan in place. By definition, you cannot predict a zero-day attack. This uncertainty makes a robust, resilient IR plan even more crucial.

5. Know your environment. Security teams cannot hope to reduce the risk of an application with an unpatched flaw unless they know the software is present and understand the network well enough to mitigate it.

6. Keep your systems patched. Your security team should apply the latest patches and audit the environment for missing patches. No, this step will not in itself protect your systems from zero-day attacks. But many organizations remain vulnerable to already-fixed zero-day flaws simply because they haven't fully patch their systems.

7. Use operating systems and applications that support DEP and ASLR. More zero-day attacks are bypassing DEP and ASLR protections. So this step is not a cure-all. But when the OS and applications support DEP and ASLR, exploiting flaws becomes much tougher. When possible, use the newest operating system releases, which usually incorporate new techniques to reduce threats.

8. Foster more collaboration in the security industry. Zero-day attacks move fast. The good guys need to move faster. To identify and counter zero-day exploits more quickly, the security industry must collaborate more often and more seamlessly. By sharing intelligence and quickly sounding the alarm, the community can contain the damage—and make everyone safer.

9. Deploy a security platform that identifies both known and unknown threats. Security experts widely agree that signature-based defenses are toothless against today's fast-moving, ever-evolving threats.[30] Signature-based defenses work only for threats that have been discovered and documented. Likewise, reputation-based defenses, by design, stop only known threats. Even file-based sandbox technology, touted as a fresh approach to security, cannot provide the deep insight required to block zero-day attacks. Zero-day attacks call for the right mix of technology, intelligence, and expertise to quickly detect attacks and respond to them before they cause lasting harm.

10. Get advanced threat intelligence. Enhance the value of your technology by subscribing to technical intelligence to put alerts on context and keep you abreast of emerging threats to your geography or industry.

11. Have advanced security expertise on tap for the worst attacks. Industry experts with experience resolving serious incidents can help bolster your security team. And they can be invaluable when resolving well-hidden and complex threats.

[29] Heraclitus (Edited by Charles H. Kahn). "The Art and Thought of Heraclitus: An Edition of the Fragments." 1979

[30] Gartner. "Best Practices for Mitigating Advanced Persistent Threats." January 2012.

To learn more about how FireEye can help your organization detect and respond to zero-day attacks, visit **www.fireeye.com**

FireEye