Indiana Department of Transportation

Security Awareness

Volume 2, Issue 7

July 2015

Microsoft Releases Emergency Patch Update for all versions of Windows

In the wake of a critical Remote Code Execution vulnerability in all supported versions of its operating system platform, Microsoft has just issued an emergency fix.

Yes, it's time to patch your Windows operating system against an alarming security hole that could allow remote attackers to run malicious code on your computer, thereby taking "***complete control of the affected system.***"

The critical flaw (***CVE-2015-2426***), which affects all the supported versions of Windows operating system, resides in the way Windows Adobe Type Manager Library handles specially crafted Microsoft's OpenType fonts.

Once exploited, the vulnerability could allow hackers to execute remotely malicious code on victims' computer if they open a specially crafted document or visit an untrusted web page that contains embedded OpenType fonts.

"*An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights*," Microsoft said in an **advisory** published Monday, releasing an *Out-of-Band Patch* to resolve the issue.

Microsoft's operating system including Windows Vista, Windows 7, 8, 8.1 and Windows RT are all affected by the critical vulnerability, along with those running Windows Server 2008 and later. Not just this, the flaw also affects Windows 10 Insider Preview.

So far, there are no such indications that the flaw is being actively exploited by the hackers in the wild. But, the chances of exploitation of the vulnerability are now high; so users are advised to update their systems using Windows Update as soon as possible.

Security researchers Mateusz Jurczyk of Google Project Zero, and Genwei Jiang of FireEye were credited by Microsoft for finding the flaw.

Inside this issue:

To Report SPAM

Open a new message

1. Address message to postmaster@iot.in.gov
2. Type "SPAM" on the subject line of the message
3. Drag and drop the SPAM email as an attachment in the new "SPAM" message.
4. Send message
5. Delete SPAM message from your mailbox

Once the SPAM postmaster has received your message you will receive an email acknowledging its receipt.

Please Note:

Do not respond to the SPAM, this will alert the spammers that they have a valid email address and can potentially increase SPAM received.

NATIONAL CYBER SECURITY MONTH
AWARENESS QUIZ

S E C U R I T Y O U R A N D I P O U I R T
N N O A E W E O T I O E T H G A I L S U O
O C P A S S W O R D W S N O I T A L O I V
I R U H M E R E T A M T R A C C E B D N U
T Y L A I P O B Y T E E A L O H A L F V L
A P S M R S M I T A A N I S E K R A N E N
L T D S C L H A C K E R N P L E A C E S E
U I C A S I C I O T T E S A E V W K L T R
G O M N L J A N N O E T W R S I A O E I A
E N A D A Y E E D G S N S T R N R R C G B
R N L A I T R M R D R I P R O T E C T A I
L A W R S T B I E D P N A S H O N R R A L
A O A N C D O T A A P T M N N N E E O T I
T L R S R E C O R D R R A O A S S M N T T
S O E W I E P O D A T A N C J B S I I S Y
N L A P F W R P H T E N T N O E N O C C Y
E L L N F E T H I O C E E I R M I W U R T
V A I D E N T I T Y T H E F T I P S O A E
E W V E T O E T E C D I L O L L I U D M K
R E E A R W C C C I A P A R A K K R T E M
R R E D A C T M H L T A E X P L O I T E A
E I R I C A I R C O A A T A L S O V E R R
T F N R K N C O M P L I A N C E R R A I E
N S E E K E R W O R K L A S O P S I D L T
I I N F O R M A T I O N N E A R S V S E S

AWARENESS
BREACH
BSI
BYTE
COMPLIANCE
COMPUTER
DATA
DISPOSAL
ELECTROINIC
ENCRYPTION
EXPLOIT
FIREWALL
HACKER
HIPAA
HITECH
IDENTITY THEFT
INFECTED
INFORMATION
INTERNET
ISO
MALWARE
PASSWORD
PATCH
PHI
PHISHING
POLICY
PROTECT
PROTECT DATA
RECORD
REDACT
REGULATIONS
SCAM
SECURITY
SPAM
TROJAN HORSE
VIOLATIONS
VIRUS
VULNERABILITY
WALKABOUT
WORM

Identity Theft

If you've recently done one of these 3 things, you're at a higher risk for having your identity stolen.

In the past year, have you bought a house, sold a house, gotten married, gotten divorced, had a child, become pregnant, lost your job, or gotten a new one?

If so, you have a higher risk of identity theft.

All of these major life events have one thing in common, according to Paige Hanson, educational programs manager at **Lifelock**, the identity-theft-protection company: You're sharing more personal information than you normally would.

Take buying or selling a house, for instance. "Your paperwork passes through the hands of multiple agents and representatives," Hanson explains.

Those documents might include your Social Security number, date of birth, passport number, or copies of your driver's license — all information that can be used to steal your identity.

Homebuyers are nearly three times as likely to be a victim of identity theft as the average person, according to statistics collected by Lifelock, and sellers are almost four times as likely.

You may not be able to avoid giving away that kind of personal information in a real-estate transaction, Hanson says, but it's always worth asking if providing your Social Security number, for instance, is really necessary.

"A lot of people think that just because they've been asked for information, they have to provide it," she says. "Before automatically giving it away, ask why. A lot of times, they won't have an answer. And maybe you'll be encouraging them to change their security standards."

Lifelock's research has found that just about any major life change comes with the danger of identity theft:

- Your risk of getting your identity stolen is 3.5 times higher if you've been married in the past year.
- Having a child or becoming pregnant increases the risk of identity theft by 2.7 times.
- Either losing or starting a new job raises your risk of identity theft by 50%.

People who have gotten divorced or become separated in the past 12 months are 3.5 times more likely to experience identity theft.

Often, it's not a data breach that puts your personal information out in the open — it's what you've posted yourself. Engaged couples often include details like where they live or where they're going on honeymoon on their wedding websites, and new parents share their children's full names and birth dates on Facebook.

There's also the risk of unintentionally exposing your personal data when you use public Wi-Fi networks to apply for jobs, shop online, or check dating websites.

So whether it's a form at the doctor's office that asks for your Social Security number or a website that wants to know your birth date, stop and think before you give that information away. "People need to take active ownership in protecting themselves," Hanson says.

Malicious Gaming App Infects More than 1 Million Android Users

It's not at all surprising that the *Google Play Store* is surrounded by a number of malicious applications that may gain users' attention to fall victim for one, but this time it might be even worse than you thought.

Threat researchers from security firm ESET have **discovered** a ***malicious Facebook-Credentials-Stealing Trojan*** masquerading as an Android game that has been downloaded by ***more than a Million*** Android users.

Malicious Android Apps downloaded 50,000-1,000,000 times

The Android game, dubbed "**Cowboy Adventure**," and another malicious game, dubbed "**Jump Chess**" – downloaded up to 50,000 times, have since been removed from Google Play Store.

However, before taking them off from the app store, the creepy game apps may have compromised an ***unknown number of victims' Facebook credentials***.

Both the games were created by the same software developer, Tinker Studio and both were used to gather social media credentials from unsuspecting users.

How Cowboy Adventure victimizes Android users?
Once installed, Cowboy Adventure produced a ***fake Facebook login window*** that prompted users to enter their Facebook usernames along with their passwords. A practice known as **OAuth** in which a 3rd party asks your Facebook login.

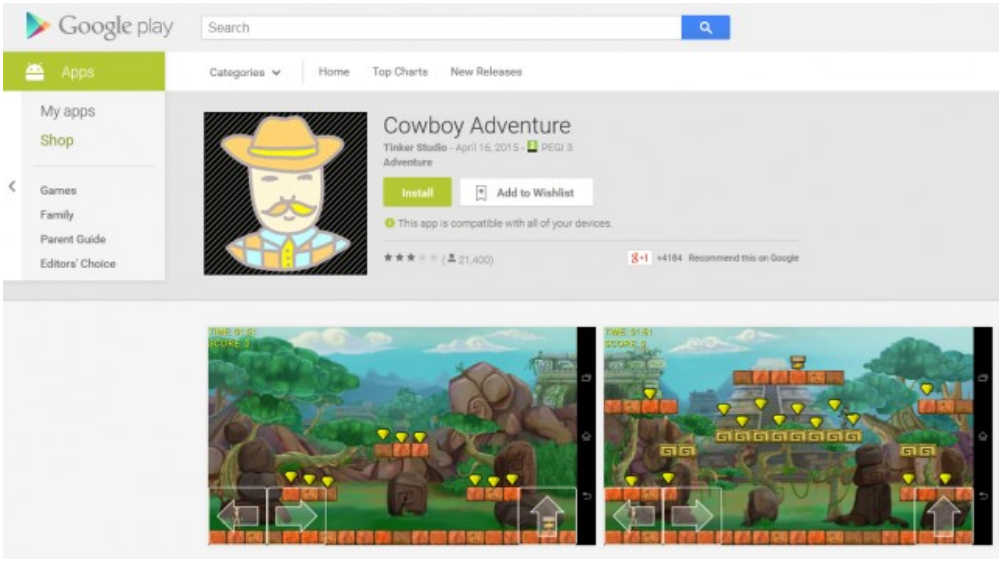
However, if users provide their credentials to Cowboy Adventure app, the malicious code within the game app allegedly sent their credentials to the attacker's server.

Therefore, If you have downloaded Cowboy Adventure or Jump Chess, ***you should immediately change*** not alone your Facebook password, but any service that uses the same combination of username and password as your Facebook account.

ESET senior security researcher ***Robert Lipovsky*** believes that the app malicious behavior is not just a careless mistake of the game developer, but the developer is actually a criminal minded.

Take Away
A few basic tips that you should always keep in your mind are:

Always download apps from official sources, such as Google Play Store or Apple's App Store.
Read reviews from other users before downloading an app (Many users complained about "Cowboy Adventure" that the game locked them out of Facebook accounts).
Always use two-factor authentication on services that makes it harder for hackers to access your accounts with just your password.
Always keep a malware scanning software from trusted vendors like Avast, AVG, ESET, Kaspersky and Bitdefender, on your smartphone.



17-Year-Old Lizard Squad Member Found Guilty Of 50,700 Hacking Charges

An alleged member of Lizard Squad, who claimed responsibility for knocking Sony's **PlayStation Network** and Microsoft's **Xbox Live** offline late last year has been ***convicted of 50,700 counts of cyber crime.***

The infamous computer hacker gang **Lizard Squad** launched massive Distributed Denial-of-Service (DDoS) attacks against the largest online gaming networks -- **PlayStation Network and Xbox Live** -- on Dec. 25, 2014. Then offered to sell its own Lizard-branded DDoS-for-hire tool called Lizard Stresser.

Julius "zeekill" Kivimaki, a 17-year-old was given a two-year suspended prison sentence and was "ordered to fight against cybercrime," according to Finnish newspaper **Kaleva**.

Facing more than 50,000 Counts of Computer Crime

Finnish authorities arrested Kivimaki in late 2014.

Under the alias "**Ryan**," the teen participated in an interview with U.K. television station Sky News, openly claiming that he is a member of Lizard Squad and that the cyber attacks on Xbox Live and PlayStation Network were conducted to ***raise awareness of the inadequate security at Microsoft and Sony.***

The DDoS attacks on gaming networks were ultimately stopped by **MegaUpload founder Kim Dotcom**, who offered the group 3,000 vouchers for his content hosting service, amounted to $300,000 in bribe.

Julius Kivimaki Harassed an American for 3 Years

While talking to the **Daily Dot**, a victim of Kivimaki's repeated harassment Blair Strater, a 20-year-old American, said he was "absolutely disgusted by the ruling" because he felt the sentence was too light.

According to Strater, Kivimaki called in false threats to American law enforcement, which results in ***SWAT teams arriving at his residence***. For almost three years, Kivimaki harassed his family by stealing their identities and ruining their finances and personal lives.

Kivimaki's computer hacking charges include data breaches, telecommunication harassments, payment fraud, and other counts related to fraudulence and violations of company secrets.

Malware And Hacking Forum Seized, Dozens Arrested

The FBI and other law enforcement agencies have ***arrested more than 70 people*** suspected of carrying out cyber criminal activities associated with one of the most active underground web forums known as **Darkode**.

Darkode, also used by notorious **Lizard Squad**, was an online bazaar for cyber criminals looking to buy and sell hacking tools, botnet tools, zero-day exploits, ransomware programs, stolen credit cards, spam services and many illicit products and services.
Darkode had been in operation since 2007 before law enforcement authorities seized it this week as part of an investigation carried out in 20 different countries.
"We have dismantled a cyber-hornet's' nest...which was believed by many, including the hackers themselves, to be impenetrable," **said *U.S. Attorney David J. Hickton***.
The crackdown, which the FBI dubbed **Operation Shrouded Horizon**, was initiated two years ago by its counterparts in Europe, Brazil and law enforcement agencies in more than 20 countries.
So far at least 12 suspects have been arrested in the United States, and around 28 people are known to have been arrested on Tuesday in other countries including Germany, Denmark, the UK, India, Romania, Sweden, and Israel.
According to the Department of Justice, the operation conducted by the authorities was *"the largest coordinated international law enforcement effort ever directed at an online cyber-criminal forum."*

The Suspects Arrested
Some of the suspects arrested in the United States in association with Darkode include:

Morgan C. Culbertson, 20, from Pittsburgh, with online moniker "Android," allegedly designed and sold a malicious program called **Dendroid** that steals data from Google Android phones.

Eric L. Crocker, 39, from Binghamton, New York, reportedly made use of a **Facebook Spreader** to **infect Facebook users** with botnet malware and sold the botnet to spammers for spreading spam.

Naveed Ahmed, 27, of Tampa, Florida, has been charged with maintaining a spam botnet to victimize millions of cell phone users.

Phillip R. Fleitz, 31, of Indianapolis, has been charged with maintaining a spam botnet to victimize millions of mobile phone users.

Dewayne Watts, 28, of Hernando, Florida, has been charged with maintaining a spam botnet to send spam messages to millions of cell phone users.

Daniel Placek, 27 from Glendale, Wisconsin, has been charged with different conspiracy charges for creating the Darkode forum and enabling the crimes.

Rory Stephen Guidry of Opelousas, Louisiana has also been accused of selling botnet access on Darkode.

This is just the beginning, as the operation is ongoing which will result in more arrests from different countries. In June last year, the authorities took down the **GameOver Zeus** but the botnet again came into operation with more nasty features just after a month. You can read The Hacker News article **WHY BOTNET RE-EMERGE AFTER TAKEDOWNS?** This gives you a brief explanation about the re-emerging of botnets even after the shutdowns.

The **IRUA** is Posted at

http://iot.in.gov/security/irua/

The **Mobile Device** policy - http://www.in.gov/indot/div/pubs/mobile-device-policy.pdf

IOT's Information Security Framework page is located at the web address: http://www.in.gov/iot/2339.htm

Call 234-HELP

Scott T. Robison M.Ed.

INDOT Security Awareness Coordinator

Office: (317) 232-5179

Email: srobison@indot.in.gov

Indiana Department of Transportation