MCMC Network Security Centre

Advisory: July 2016 Edition

Table of Contents

Advisory 1: System Management Mode (SMM) BIOS Vulnerability

Systems Affected:

- Several Lenovo Products and other PC makers may also affected.

Risk

- High.

Overview

- A security researcher has identified a Unified Extensive Firmware Interface (UEFI) bug in Lenovo's Thinkpad System Management Mode (SMM) that allow attackers to bypass Windows' security protocols.
- Since this originated from independent BIOS vendors (IBVs), other PC hardware vendors might also be affected.

Description

- IBVs are software development firms that specialize in developing customized BIOS firmwares that is loaded into the PCs of original equipment manufacturers.
- The exploit, dubbed "ThinkPwn" targets a privilege escalation flaw in UEFI driver, allowing the attacker to remove the flash write protection and to execute rogeu code in the SMM.
- Attackers require physical access to targeted computers to exploit. However, it is possible for victims to be targeted through malware in the future.

Impact

- Attackers can install stealthy rootkit inside the UEFI leading to further exploitation.
- Attacker scan also disable Windows security features such as Secure Boot, Virtual Secure Mode and Credential Guard.

Recommendation

- Since this is a zero-day vulnerability, please review with your vendor if your hardware is affected.
- Set a BIOS setup password, this would assist in making sure Secure Boot cannot be disabled and boot to the UEFI shell cannot be re-enabled.
- Please run only trusted code from known sources.

Reference:

1. https://support.lenovo.com/my/en/solutions/LEN-8324
2. http://www.computerworld.com/article/3090950/security/firmware-exploit-can-defeat-new-windows-security-features-on-lenovo-thinkpads.html
3. https://github.com/Cr4sh/ThinkPwn

Advisory 2: Symantec and Norton Security Products Vulnerability

Systems Affected:

- All Symantec and Norton branded antivirus products.

Risk

- High.

Overview

- Multiple vulnerabilities have been found in Symantec and Norton branded antivirus products.
- Remote attacker exploiting these vulnerabilities could allow affected system being taken over.

Description

- Security software is usually the popular target by attackers for exploitation due to high level of privilege on machines.
- Some of the vulnerabilities doesn't require any physical interaction or changing default configuration by the user to be exploited.

Impact

- An attacker may be able to run arbitrary code at root privileged by taking advantages of this vulnerability remotely and unauthentically.

  CVE-2016-2207
  CVE-2016-2208
  CVE-2016-2209
  CVE-2016-2210
  CVE-2016-2211
  CVE-2016-3644
  CVE-2016-3645
  CVE-2016 -3646

Recommendation

- Please update Symantec or Norton antivirus products to the latest operating version.

Reference:

1. https://www.us-cert.gov/ncas/alerts/TA16-187A
2. https://googleprojectzero.blogspot.my/2016/06/how-to-compromise-enterprise-endpoint.html
3. https://www.wired.com/2016/06/symantecs-woes-expose-antivirus-software-security-gaps/

Advisory 3: Keysniffer Wireless Keyboard Vulnerability

Systems Affected:

- Wireless Keyboards from Anker, EagleTec, GE, HP, Insignia, Kensington, Radio Shack, Toshiba and possibly other vendors too.

Risk

- High.

Overview

- Researchers from security from Bastille Networks have discovered new vulnerability called Keysniffer that allow an attacker to monitor and secretly record your keystroke.
- The vulnerability also would likely open the opportunity for the attacker to use keystroke injection as well, injecting malicious command into the victim's computer.

Description

- The vulnerability occurs on the wireless keyboards that operates on 2.4GHz ISM band and are not encrypted when transmitting data.
- As the keystrokes is transmitted in clear text, an attacker can exploit by intercepting the transmission as long as they are at range of 250 yards
- The wireless keyboard vulnerable cannot be patched, as they do not support firmware updates.

Impact

- An attacker may be able to install malware, exfiltrate data or any other malicious act that a hacker could perform with physical access to the victim's computer.
- An attacker may be able to eavesdrop and record your personal and private date such as credit card numbers, password, etc.

Recommendation

- Users of vulnerable keyboards should switch to Bluetooth or wired keyboards.

Reference:

1. http://www.keysniffer.net/
2. http://siliconangle.com/blog/2016/07/26/not-good-many-wireless-keyboards-found-to-lack-encryption-vulnerable-to-attack/
3. http://www.techworm.net/2016/07/millions-wireless-keyboards-can-hacked-radio-hack-keystrokes-can-stolen.html

Security News Headline

A Crash Course in Ransomware and How to Protect Yourself From It – Lifehacker

LastPass security flaws put passwords at risk; patch rolling out – Techtarget

Update your Apple devices now to fix a terrifying security bug – Quartz

20 Year Old Windows Printer Security Vulnerability Discovered – Ubergizmo

Overeager 'Pokemon Go' fans are an opportunity for cybercriminals, cybersecurity expert says – Cnbc

“HummingBad,” a new Android malware, has infected more than 10 million devices – Digital Trends

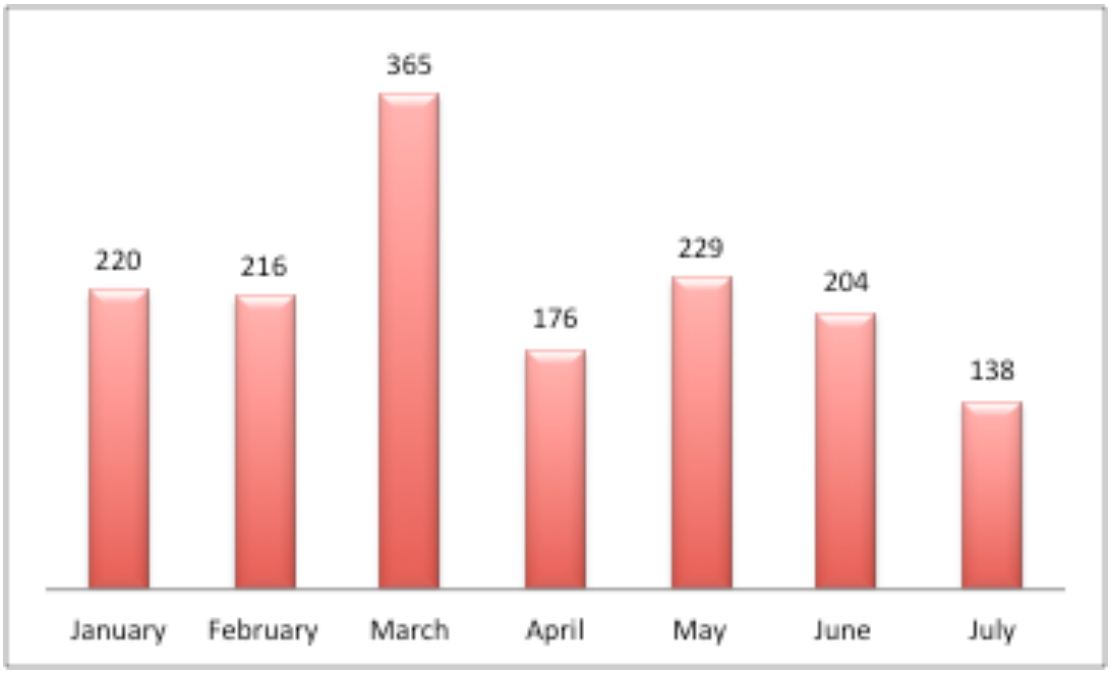
Feds Seize KickassTorrents Domains, Arrest Alleged Owner – Torrentfreak

BlackBerry Announces the DTEK50, $300 Phone All About Security – DroidLife

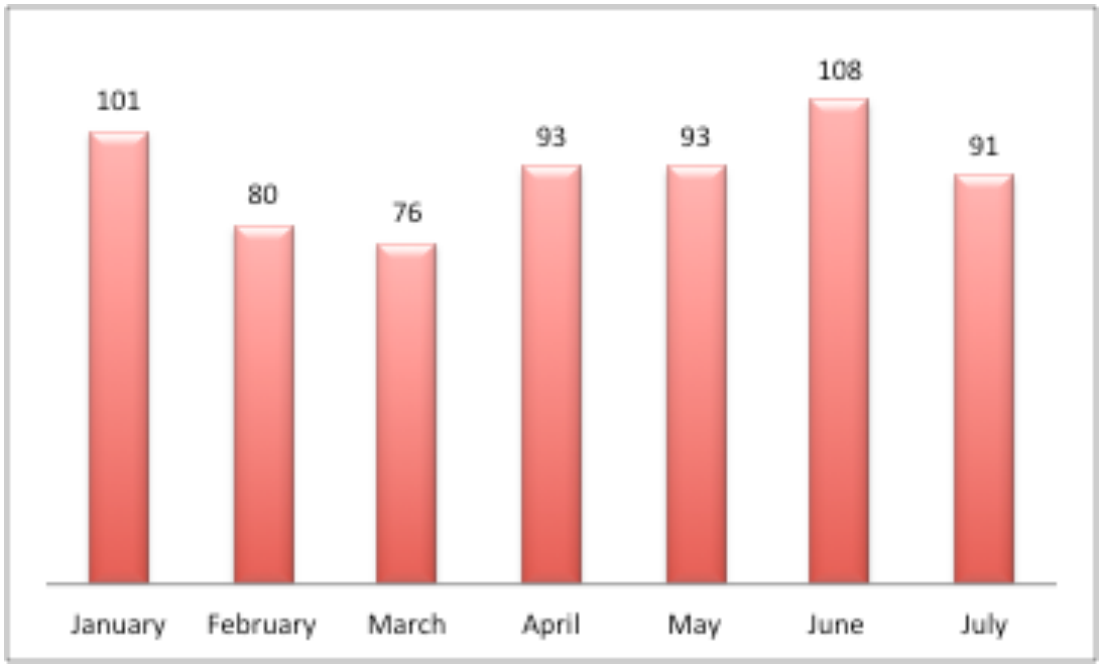
US believes Russian hackers are behind Democratic National Committee leak – Theguardian

Defacement .My and Phishing Statistic for 2016

Defacement .My:



Phishing:



Please note that defacement and phishing statistics are only based on incidents handled by MCMC NSC team. It is not a total indication of defacement and phishing occurring on that given month.

Contact Us:

MCMC Network Security Centre,
Network Surveillance Department,
Malaysian Communications and Multimedia Commission,
MCMC Tower 1,
Jalan Impact, Cyber 6,
63000, Cyberjaya,
Selangor Darul Ehsan
Tel: 03 8688 8303
Fax: 03 8688 1018
Email: nsc@cmc.gov.my
Incident Report: incident@nsc.org.my
Phishing Report: antiphishing@cmc.gov.my
Website: www.nsc.org.my