PwC Weekly Security Report

This is a weekly digest of security news and events from around the world. Excerpts from news items are presented and web links are provided for further information.

Threats and vulnerabilities

Critical security flaw found in Lenovo PCs

Malware

Facebook users hit by malware: 10,000 victims in two days

Ransomware

Satana ransomware encrypts MBR and user files

Top story

Your smartwatch is giving away your ATM PIN

pwc

Critical security flaw found in Lenovo PCs

LENOVO has issued an official response to a security researcher's claim that the company is shipping more bad software with its hardware.

The problem, according to a security researcher called Dymtro Oleksiuk, is that Lenovo is shipping a flaw that undermines Windows security protocols.

Oleksiuk has posted details of the Lenovo ThinkPad System Management Mode flaw on GitHub, and has published a blog about his work.

"The new 0day vulnerability in Lenovo firmware allows arbitrary SMM code execution on a wide range of Lenovo models and firmware versions including the most recent ones," he said.

"Exploitation of the vulnerability may lead to the flash write protection bypass, disabling of UEFI Secure Boot, Virtual Secure Mode and Credential Guard bypass in Windows 10 Enterprise and other evil things."

Lenovo has tackled this, in a way. The firm is getting used to discussing problems with its products having given a wide selection of devices a dose of Superfish. The company claimed that it tried to get in contact with Oleksiuk before he went public, but failed.

"Lenovo's Product Security Incident Response Team is fully aware of the uncoordinated disclosure by an independent researcher of a BIOS vulnerability located in the System Management Mode (SMM) code that impacts certain Lenovo PC devices," said Lenovo in a security alert.

"At this point, Lenovo knows that vulnerable SMM code was provided to Lenovo by at least one of our independent BIOS vendors (IBVs). These are software development firms that specialise in developing the customised BIOS firmware that is loaded into the PCs of original equipment manufacturers, including Lenovo."

The firm added that this is common and that it will be difficult to identify the source.

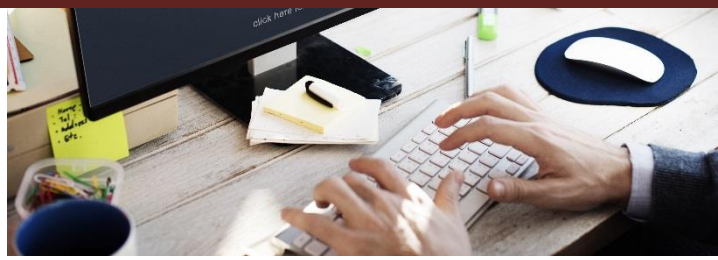
"Following industry standard practice, IBVs start with the common code base created by chip vendors, such as Intel or AMD, and add additional layers of code that are specifically designed to work with a particular computer. Lenovo currently works with the industry's three largest IBVs," the firm added.

Source:
http://www.theinquirer.net/inquirer/news/2463830/lenovo-pcs-flagged-for-onboard-security-flaws-again

Our perspective

As of now, Lenovo has not specified the models that have been affected by this flaw, but Oleksiuk has confirmed the vulnerability on several Lenovo laptops, from ThinkPad T450s to the older ThinkPad X220. We recommend that business users avoid using such laptops to minimise the risk.

Facebook users hit by malware: 10,000 victims in two days



A new malware was spotted by security researchers at Kaspersky Lab, targeting Facebook users. According to the researchers' new report, there have been 10,000 victims in two days.

The malware has two stages: firstly, an unsuspecting victim gets a message from a Facebook friend, saying they had mentioned them in a comment. But when the victim clicks to see the comment, they instead download a bunch of malware, including a Chrome add-on which can take over the victim's Facebook account, once they log back in.

After that, anything is possible, including privacy settings changes, data extraction, and so on. The victim's account is also used to keep spreading the message, as well as gather fraudulent likes and shares. The malware is protecting itself by trying to blacklist antivirus sites.

In two days, between 24th and 27th June, 10,000 people were infected. Brazil was hit hardest, with 37 per cent of cases. The country is followed by Poland, Peru, Colombia, Mexico, Ecuador, Greece, Portugal, Tunisia, Venezuela, Germany and Israel.

"Two aspects of this attack stand out. Firstly, the delivery of the malware was extremely efficient, reaching thousands of users in only 48 hours. Secondly, the response from consumers and the media was almost as fast. Their reaction raised awareness of the campaign and drove prompt action and investigation by the providers concerned," said Ido Naor, Senior Security Researcher, Global Research and Analysis Team, Kaspersky Lab."

Kaspersky Lab urges all Facebook users to stay safe, by keeping an antivirus software and think twice before opening any links or attachments, even if they are from a friend.

Source:

http://www.itproportal.com/2016/07/06/facebook-users-hit-by-malware-10000-victims-in-two-days/

Our perspective

Even though no such cases have been observed in India as of now, we recommend that Facebook users exercise caution and avoid opening any suspicious links while they are logged in.

Satana ransomware encrypts MBR and user files

Satana, a new ransomware family that emerged in the past week, has copied some of its functionality from Petya and Mischa, two connected crypto-lockers observed over the past several months.

What makes Satana stand out, beside its devilish name (Satana means devil in Italian and Romanian), is the fact that it comes with two modes, one to rewrite the infected computer's Master Boot Record (MBR) to take over it, and the other to encrypt user files. Apparently, the new malware family uses both modes at the same time, which allows it to completely undermine its victim's computer.

The Petya ransomware emerged in March, when it made a name for itself because it was able to encrypt entire drives. The malware was performing a two-step encryption, rewriting the computer's MBR to take over the reboot process and to ensure persistence on the infected machine, and encrypting the entire hard drive during the second stage, after reboot.

Petya was being distributed mainly within enterprise environments, via emails sent to the organization's human resources department. In May, Petya received an update and started dropping a second ransomware onto the infected machines in the event that it didn't manage to successfully perform the second step of the encryption process. Dubbed Mischa, this ransomware would use AES-encryption to lock user files, and would also target .exe files, something that most ransomware out there doesn't.

Unlike the Petya/Mischa bundle, the Satana ransomware both rewrites the MBR and encrypts user's files one by one, Malwarebytes Labs researchers explain. After execution, the new malware disappears from the infected computer, though it installs a copy of itself in the %TEMP% folder, under a random name.

When first executed, the malware triggers a User Account Control (UAC) notification that appears in a loop until the user allows it to make changes to the computer, then it writes its malicious code to the beginning of the disk and saves contact data for a particular client in the Windows Registry. According to researchers, the ransomware announces everything that it does, including the progress in encrypting files, and includes debug code in it, suggesting that it might be in the early stages of development.

Unlike Petya, which triggers a BSOD prompt to determine users reboot their machines, Satana patiently waits for the reboot. However, as soon as the system boots up, it displays a screen with the ransom note. During the first step of the attack, in low-level mode, only the MBR is encrypted (and stored in Sector 6), but not beyond repair: a backup can be used to recover the original MBR, it seems.

The ransomware encrypts users' files (on local disks and unmapped network shares) one by one, drops a ransom note in each folder, and deletes shadow backups to hinder data recovery attempts. All of the encrypted files are renamed with an email address taken out of a hardcoded pool and the original name. Malwarebytes Labs also explains that all files are encrypted with the same unique key using an encryption algorithm that is either a block cipher or custom XOR based.

According to researchers, the analyzed sample includes a hard-coded command and control (C&C) address and sends information about the client to it, along with the randomly generated key used in the encryption process. The issue with Satana is that it doesn't store the key locally, although it can perform the encryption process while offline, meaning that the key is permanently lost if communication to the C&C server is lost during encryption.

Malwarebytes Labs researchers explain that the sample they analyzed might have not been intended for public use, both because of issues with the code and because the Bitcoin wallet in the ransom note doesn't work. Moreover, they say that the malware's low-level attack code looks unfinished, but that its authors appear to be focusing on it, and that future malware variants might bring improvements.

Source:
http://www.securityweek.com/satana-ransomware-encrypts-mbr-and-user-files?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29

Our perspective

Email attachments should not be opened if they are received from a source that is not trusted. In such a situation, the user should forward the email to a sandbox or alert information security personnel.

Your smartwatch is giving away your ATM PIN

In the paper "Friend or Foe?: Your Wearable Devices Reveal Your Personal PIN" scientists from Binghamton University and the Stevens Institute of Technology combined data from embedded sensors in wearable technologies, such as smartwatches and fitness trackers, along with a computer algorithm to crack private PINs and passwords with 80-percent accuracy on the first try and more than 90-percent accuracy after three tries.

"Wearable devices can be exploited," said Yan Wang, assistant professor of computer science within the Thomas J. Watson School of Engineering and Applied Science at Binghamton University. "Attackers can reproduce the trajectories of the user's hand then recover secret key entries to ATM cash machines, electronic door locks and keypad-controlled enterprise servers."

Wang is a co-author of the study along with Chen Wang, Xiaonan Guo, Yingying Chen, and lead researcher Bo Liu from the Stevens Institute of Technology. The group is collaborating on this and other mobile device-related security and privacy projects.

"The threat is real, although the approach is sophisticated," Wang said. "There are two attacking scenarios that are achievable: internal and sniffing attacks."

"In an internal attack, attackers access embedded sensors in wrist-worn wearable devices through malware," Wang explained. "The malware waits until the victim accesses a key-based security system and sends sensor data back. Then the attacker can aggregate the sensor data to determine the victim's PIN."

"An attacker can also place a wireless sniffer close to a key-based security system to eavesdrop sensor data from wearable devices sent via Bluetooth to the victim's associated smartphones," Wang said.

Researchers conducted 5,000 key-entry tests on three key-based security systems, including an ATM, with 20 adults wearing a variety of technologies over 11 months.

The team was able to record millimeter-level information of fine-grained hand movements from accelerometers, gyroscopes and magnetometers inside the wearable technologies regardless of a hand's pose. Those measurements lead to distance and direction estimations between consecutive keystrokes, which the team's "Backward PIN-sequence Inference Algorithm" used to break codes with alarming accuracy without context clues about the keypad.

According to the research team, this is the first technique that reveals personal PINs by exploiting information from wearable devices without the need for contextual information.

Source: http://phys.org/news/2016-07-smartwatch-atm-pin.html

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,08,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

For any queries, please contact:

Sivarama Krishnan
sivarama.krishnan@in.pwc.com

Amol Bhat
amol.bhat@in.pwc.com

MB/July 2016-6850