ISECURION
YOUR SECURITY, OUR RESPONSIBILITY
VOLUME 4, AUGUST 2018

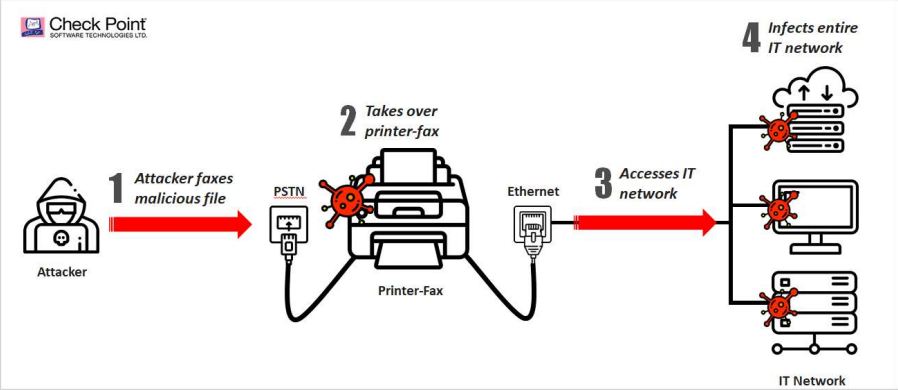
Infosec Newsletter

August, 2018

ISECURION TECHNOLOGY & CONSULTING PVT. LTD.
2nd Floor, #670, 6th Main Road, RBI Layout, Opp. Elita Promenade, J.P. Nagar 7th Phase, Bengaluru, Karnataka 560078

1. Sending a Fax Can Compromise your Network:-

Check Point researcher released two critical remote code execution (RCE) vulnerabilities discovered in the communication protocol used in millions of fax machines. The attacker only need the fax number which is easily available on the corporate website. The exploit has been dubbed as Faxploit, the attack involves two buffer overflow – CVE-2018-5925 and CVE-2018-5924, leading to remote code execution.



The researcher at Check Point used the popular HP OfficeJet Pro 6830 all-in-one printer and OfficeJet Pro 8720. If all are connected to the printer-fax machine, and, in turn, all of them are connected to one another, then an attacker need only to penetrate one access point (in this case the printer-fax) in order to enter the entire corporation's network.

To read more about this Click Here.

Video Poc: YouTube.

2. Man-in-the-Disk Attack

The new attack surface has been surfaced on the internet which is dubbed as "Man-in-the-Disk", which allows attacker to enter and manipulate the data stored on the external storage. Google has advised its developer to with few guidelines regarding the usage of the external storage for their apps:

- Perform input validation when handling data from external storage.
- Avoid the store of executable files in external storage.
- External storage files should be signed and cryptographically verified.

Checkpoint security researcher have tested few android application which are Google Translate, Yandex Translate and Google Voice Typing, which were found that the application failed to validate the integrity of data read from the external storage.

To read more about this Click Here.
Video Poc: YouTube.

3. Adobe Security Patches August 2018

- Adobe Acrobat and Reader (APSB18-29)[CVE-2018-12808, CVE-2018-12799]
- Adobe Experience Manager (APSB18-26)
- Adobe Flash Player (APSB18-25)
- Adobe Creative Cloud Desktop Application (APSB18-20)[CVE-2018-5003]

To read more about this Click Here.

4. macOS Zero-day by ex-NSA Hacker

Patrick Wardle, an ex-NSA hacker and now Chief Research Officer of Digita Security, discovered a critical zero-day vulnerability which allows a malicious application installed on the target macOS to virtually click on the object without any user interaction.

Well it's just a click, then how come it is dangerous. A single click can bypass security mechanism, authorize keychain access, allow to load 3rd party kernel extension or authorize outgoing network connection. Just tweaking a two lines can make your macOS hacked.

To Read More about this: Click Here.

5. Microsoft Tuesday Patch August 2018

This month's update covers vulnerabilities in:-

- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office and Microsoft Office Services and Web Apps
- ChakraCore
- Adobe Flash Player
- .NET Framework
- Microsoft Exchange Server
- Microsoft SQL Server
- Visual Studio

Software Patches Download List:-

- ADV180016
- ADV180018
- ADV180020
- CVE-2018-8273
- CVE-2018-8341
- CVE-2018-8348
- CVE-2018-8351
- CVE-2018-8360
- CVE-2018-8370
- CVE-2018-8378
- CVE-2018-8382
- CVE-2018-8394
- CVE-2018-8396
- CVE-2018-8398

Known Issues:-

- 4340731
- 4340733
- 4343897
- 4343900

6. PhishPoint Attack, a New Phishing Technique

To protect against potential threads, Office 365 scans the links in the email bodies to look for blacklisted domains, as the links in the email leads to actual SharePoint document, Microsoft did verify it as a threat.

How this works:

> The victim receives an email containing link to a SharePoint document. After the victim clicks on the link, a SharePoint file is opened which contains the hyperlink of a malicious URL. The link within the SharePoint redirects victim to a spoofed Office 365 login screen. When the victim attempts to login, their credentials are harvested by the hacker.

To Know More: Click Here

7. Cosmos Bank, 94 Crore Siphoned

Recently, hackers were able to withdraw a total of Rs 94 crore from a Pune based Cosmos Bank over a period of two days. Hackers were able to withdraw a total of Rs 78 crore from various ATMs in 28 countries which includes Hong Kong, Canada and few ATMs in India, another Rs 2.5 crore were taken out within India only. Hackers have cloned the cards and using a proxy switching system, hackers have self-approved the transactions and withdraw over Rs 80.5 crore in about 15000 transactions.

After the attack, cosmos bank have suspended its entire services, it has also appointed a professional forensic agency to investigate the attack. The proxy switch was operating on a payment gateway rather than core banking system.

To Know More: Click Here.

8. Cryptojacking, a crypto mining malware

Cryptojacking refers to crypto mining someone else computer with his or her consent. The hacker can either deliver the malware into someone's computer or mobile via website or infected software. He can inject JavaScript to drop a malware through a link and when the user opens the link his computer/mobile gets compromised. Now the hacker can use his/her computer or mobile to mine cryptocurrency. Cryptojacking attack uses leaked eternalblue NSA exploit. Quick Heal a Pune- based security company revealed that the cryptojacking malware has been increased from 2017 to 2018.
To identify the infection of such mining malware, the symptoms are the utilization of computational power, the system may frequently crashing, overheating or abnormal high fan speed.

To read more about this: Click Here

9. Bancor, cryptocurrency breach

Bancor, an Israeli based cryptocurrency reproted that $12.5 million tokens has bbeen stolen. The company stated that the cryptocurrency wallet on it's network has been already compromised to withdraw funds from a smart contract.

NPXS crypto of approx worth $1 million and BNT crypto currency of approx worth $10 million has been stolen. No user wallet has been compromised in the attack. Bancor was able to freeze $10 million BNT crypto tokens from its own network. The company has raised 3,96,720 etherium tokens, worth alomost $183 millions from its initial coin offering (ICO) last year.

Bancor was able to freeze token or invalidate the token with its built-in Bancor protocol that can be used to recover from an extreme security breach. It has also asked different crypto exchanges to freeze the stolen funds to make it more difficult to liquidate the tokens.

10. Indian Government may allow the use of crypto tokens for financial trnasacations

The government is planning to launch crypto tokens for financial transcations in the country, even the ban on cryptocurrency in effective. Crypto tokens operates in a closed system and does not impact the country monetary policy, one had to pay phiscal money to buy a token which can be stored as a code in any form, like paper, or mobile phone.

The government is also planning to use crypto tokens for the metro cards by replacing the smart card we use today. The toekns can also be used in a loyality program such as air miles where it is limited to buying next ticket and cannot be convereted into money.

11. Top list of mobile malware

1. **Lokibot** – Andorid banking trojan, data stealer, and locks the phone when admin privilege are removed.
2. **Triada** – Android modular backdoor malware, spoofing URL which are loaded in the browser.
3. **Guerilla** – Android ad-clicker, ability to communicate with command & contorl server, download additional plugins and perform ad-clicking wihtout the concent of the the user.

12. Top list of vulnerbilities

- **Mcirosoft IIS WebDAV SCStoragePathUrl Buffer Overflow (CVE-2017-7269)** – An attacker can send a crafted request over a network to Microsoft Windows Server 2003 R2 through IIS 6.0 could execute arbitrarty code execution or denial of service.
- **Apache Struts2 Content-Type Remote Code Execution (CVE-2017-5638)** – An attacker can exploit this vulnerbility by sending an invalid content-type as a part of the file upload request, which on success will give arbitray code execution.
- **Web servers PHPMyAdmin Misconfgiuration Code Injection** – A code injection vulnerbility reported on PHPMyAdmin misconfiguration which allows remote attacker to send a specially crafted HTTP request to the target.
- **Dasan GPON Router Authentication Bypass (CVE-2018-10561)** – An authentication bypass vulnerbility exits in GPON router which allows obtaining sensitive information and gain unauthorized access into the affected system.