WAN Msg.

To All FTRs/SHQs/Spl(Ops)/Bns/TCs/Academy
Fm FHQ SSB New Delhi

WT-8884

NO.3/SSB/MISC/BPR&D/2017/1960 Date: 26.04.2019

It is intimated that following Cyber Crime Related Inputs (Cyber Crime Information) have received form open source are as under:-

Sl. No.	Cyber Crime Information No.& Subject	Preventive measures/suggestions
1	26 Goggle just like Facebook collect a lot of personal data of users from what they have searched online and the websites they have visited to who your contact are and what you talk about.	• Use Google dashboard to see and manage the date in Google account. • Adjust privacy settings in Google's activity controls under Google account data & personalisation. • Use private browsing incognito mode to ensure that the pages user access won't show up in browsing history or search history. • Use a different browser and search engine to stop Google from tracking searches and website visits. • Turn off locations reporting in Google maps in android and pixel device settings.
2	27 Microsoft Internet Explorer and Edge browser allows a malicious website.	• Update the browser with latest security patches. • Use other web browsers that are not affected by this vulnerable.
3	28 Xiaomi's phones security application 'Guard Provider' allows man-in-the-middle attackers sitting on open Wi-Fi network to intercept device's.	• Do not use open Wi-Fi network e.g. at coffee shops, malls etc.
4	29 A iOS version of malware called 'Exodus' a spyware application targeting iPhone device has been identified.	• Do not click on suspicious links received from unknown sources. • Keep security software update in your device.
5	30 Hackers poses as seller & buyer on e-commerce website to dupe innocent people by compromising their mobile phone device through a malware link.	• Be cautious of deals which offer cheap rate, there could be traps. • Carry out due diligence to verify credentials of the buyer/seller before transacting on deals. • Do not click on suspicious links received from unknown sources.

Aforesaid informations have been shared by Threat Analytical Unit (TAU), Indian Cyber Crime Co-Ordination CIS Division, MHA. It is requested to go through the contents of the above mentioned information & share with all concerned officers/officials and submit feedback, if any.

This information is being shared for purpose of sensitization about cyber crime modus-operandi/trend, and no legal action can be initiated based on inputs without additional corroborative evidence.

Encld. Above Cyber Crime Informations

UP-2190
30/4/19

26/4/19
Dy. Commandant (Comn.)
FHQ SSB New Delhi

Copy to,

1. Server Room to upload on SSB official Website
2. All FHQ Branches (Through WAN)

Cyber Crime Information-26

To: All members

From: cyberdost@mha.gov.in

Subject: Cyber Crime Information-26

Respected Sir/Madam,

Google is a multinational organization and popular for search engine. Google's other enterprises include Internet analytics, cloud computing, advertising technologies, and Web app, browser and operating system development.

Google just like Facebook, collects a lot of personal data of users from what they have searched online and the websites they have visited to who your contacts are and what you talk about. The company is then able to take this information and make informed decisions regarding what you might be interested in, which they show you in the form of ads. Following are the example of Google services data collection.

Google app & activity & services	Data collected
Google Chrome	Browser history, websites visited
Google Search	Queries searched
Gmail	Contacts, emails sent, emails received, email content/conversations
Ads	Ads clicked on, topics interested in
Google Photos	People and places tagged
Google Fit	Fitness level and goals
Google Maps	Locations visited, places searched, methods of transportation, dates of tavel
Google Calendar	Upcoming plans and appointments
Google Hangouts	Contacts, conversations
YouTube	Videos watched, liked and uploaded
Google News	News sites visited, stories clicked on
Google Books	Books read and searched
Google Shopping	Products searched and clicked on
Waze	Directions and places searched, locations visited

Suggestions to maintain the privacy while using Google services -

- Use Google Dashboard to see and manage the data in Google Account
- Adjust privacy settings in Google's Activity Controls under Google Account > Data & Personalisation.

- Use private browsing Incognito Mode to ensure that the pages user access won't show up in browsing history or search history.
- Use a different browser and search engine to stop Google from tracking searches and website visits.
- Turn off location reporting in Google Maps in Android and Pixel device settings.

Regards

Threat Analytical Unit (TAU)
Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23093697

Cyber Crime Information-27

To: All members

From: cyberdost@mha.gov.in

Subject: Cyber Crime Information-27

Respected Sir/Madam,

Latest vulnerability has been discovered in Microsoft Internet Explorer and Edge Browser, which allows a malicious website to perform universal cross-site scripting (UXSS) attacks against any domain by bypass same-origin policy on victim's web browser.

Same Origin Policy (SOP) is a security feature implemented in modern browsers that restricts a web-page or a script loaded from one origin to interact with a resource from another origin, it prevent unrelated sites from interfering with each other.

To exploit these vulnerabilities, attackers need to convince a victim to open the malicious website through phishing/spear phishing, links etc. to steal victim's personal data.

Suggestions

- Update the browser with latest security patches.
- Use other web browsers that are not affected by this vulnerability.

Regards

Threat Analytical Unit (TAU)
Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23093697

Cyber Crime Information-28

To: All members

From: cyberdost@mha.gov.in

Subject: Cyber Crime Information-28

Respected Sir/Madam,

A man-in-the-middle vulnerability has been identified in Xiaomi's phones security application 'Guard Provider', which can modify pre-installed antivirus app into a malware.

The security app developed by Xiaomi, offers multiple third party programs in a single app and allow the user to choose antivirus programs such as Avast, AVL, and Tencent.

Guard Provider security application downloads antivirus signature updates through an unsecured HTTP connection, which allows man-in-the-middle attackers sitting on open Wi-Fi network (restaurants, malls, airport etc.) to intercept device's network connection and push malicious updates to gain access to the phone owner's pictures, videos, and other sensitive data, or inject other malware.

Suggestions

- Do not use open Wi-Fi network e.g. at Coffee Shops, Malls etc.

Regards

Threat Analytical Unit (TAU)
Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23093697

Cyber Crime Information-29

To: All members

From: cyberdost@mha.gov.in

Subject: Cyber Crime Information-29

Respected Sir/Madam,

An iOS version of malware called 'Exodus', a spyware application targeting iPhone devices has been identified.

Exodus is abusing the Apple Developer Enterprise program, which allows enterprises to distribute their own in-house apps directly to their employees without directing to iOS App Store. Attackers set up phishing traps to direct users toward the malicious apps. The sites were designed to look like information pages of mobile service providers.

Once Exodus is installed in the devices, it can steal the information from devices including contacts, audio recordings, photos, videos, GPS location, and device information further transmitted via HTTP to the attacker's controlled command and control server.

Suggestions

- Do not click on suspicious links received from unknown sources.
- Keep security software updated in your device.

Regards

Threat Analytical Unit (TAU)
Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23093697

Cyber Crime Information-30

To: All members

From: cyberdost@mha.gov.in

Subject: Cyber Crime Information-30

Respected Sir/Madam,

A new modus operandi has been identified, wherein hacker poses as seller & buyer on e-commerce website to dupe innocent people by compromising their mobile phone device through a malware link.

Many e-Commerce websites are providing an online platform to people where they can buy & sell products. In this process, interested buyer or seller exchange their mobile numbers to negotiate the deal.

Hackers have discovered a new pattern to distribute the malware on victim's mobile phone to gain the remote access. When suspect identifies the victim on e-commerce website who is ready to make the deal to buy or sell the product, the suspect sends a text message with encrypted link which contains malware to victim's mobile phone to confirm the bank account details. Once the victim click on the link, the mobile phone gets compromised and gives remote access to the hacker to operate the device. The hacker then access bank details and can carry out transactions.

Suggestions

- Be cautious of deals which offer cheap rate, there could be traps.
- Carry out due diligence to verify credentials of the buyer/seller before transacting on deals.
- Do not click on suspicious links received from unknown sources.

Regards

Threat Analytical Unit (TAU)
Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23093697