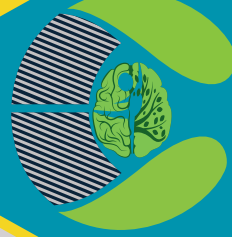
Volume - 2
Issue - 1
January
2020
e-ISSN
2582-5755

5



Juice Jacking - A type of Cyber Attack

– **Shivani Sanwal**
Computer Teacher, Tagore Model Senior Secondary School Nakodar, Jalandhar, India
shivanisanwal115@gmail.com

– **Kamaljit Singh**
Associate Professor, KRM DAV College, Nakodar, Jalandhar, India
kamaljit70@gmail.com

In this modern world, the mobile phone is an integral part of our daily life. In today's world, mobile phones are not used only for calling purpose but also for a host of other purposes that includes: photography, business transcations, video and audio recodings etc. Making easy payment within a fraction of seconds by simply using payment apps and the other online methods on the internet is what has been revolutionised by mobile phones. As these new methods of payments make transactions easy, it also gives birth to a number of problem with online frauds topping the list among others. As the technologies grow day by day the money related frauds are also witnessing a spike . In the article under reference , the new method of data theft, done by simply charging cable i.e the USB charging cable is being taken up. This type of the cyber attack is called the juice jacking method.

ARTICLE HISTORY
Paper Nomenclature:
Argument Based Credentials (ABC)
Paper Code: CYBNMV2N1JAN2020ABC3
Submission Online: 14-Jan-2020
Manuscript Acknowledged: 15-Jan-2020
Originality Check: 17-Jan-2020
Originality Test Ratio: 0% (Urkund)
Peer Reviewers Comment: 20-Jan-2020
Blind Reviewers Remarks: 21-Jan-2020
Author Revert: 28-Jan-2020
Camera-Ready-Copy: 29-Jan-2020
Editorial Board Citation: 30-Jan-2020
Published Online First: 31-Mar-2020

Keywords

- Jacking
- Laptop
- Mobile Phone
- Malware
- Data Theft

Introduction:

The smart phones are now everywhere. Nobody is left in the world who is not familiar with the smartphone , its use and the benefits it offers. In the smart phone era, the charging method of battery is also smart. USB cables are used for mobile charging. You might have the most costly and latest mobile phone but you cannot stop your data being stolen with so much ease. It only needs a charging station with power connectivity with cable. The data/ power cable that we used in the public charging station, gives unauthorized access to the attackers to steal our data. When the cyber attacks are done with these USB cables for stealing data , related to your personal life or any type of data theft , then it is called the juice jacking method. In this method the attacker simply steals all your mobile phone data, related to your personal stuff, contact details, bank details , passwords , browser cookies and all important data , which may affect you financially.

On the basis on internet news , I found a case related to juice jacking which is stated as under:

Mr. Mishra was at the airport when he found that his mobile battery had nearly drained out and was extremely low and needed to be recharged . So he plugged his mobile phone on public charging points . After a few hours , he has received an unauthorised debit SMS of Rs. 80000 in his account. On investigation, it was found that the said charging ports were neither monitored nor checked and the attacker simply temper the cord. The cord contains a chip that has spy malware that provides access to all the information stored in Mr Mishra mobile phone to the attacker device. The attacker then use these information for unauthorised money transaction .

Contact immediately your bank in case of unauthorised debit.

Working of juice jacking :

As we noticed that when we use the USB cable for laptop, or mobile phone charging it pops up some option while used to charging only or data transfer. It means it not only used for power charging purpose but also used for data transfer. In every regular USB cable has 4 to 5 pins, in which only one pin used for the charging and others are used for data transfer. The attacker used chip to interact with target mobile through USB cable. Which allows target USB data transfer pins to transfer all the data to the attacker device. The attacker use some type of malicious hardware that get installed on the public charging points. These are specially designed to install malicious code or apps on the target which helps attackers to gain the

access of target devices. As soon as they get the access we may lose the mobile data. Or we can say that we are hacked.

Pin	Name	Cable color	Description
1	V_{BUS}	Red	+5 V
2	D−	White	Data −
3	D+	Green	Data +
4	ID	N/A	Permits distinction of a host connection from device connection: • host: connected to the signal ground • device: not connected
5	GND	Black	Signal ground

USB Connection Table

Types of juice jacking :

Data theft:- In this type ,the attackers or cyber criminals steal all the data through USB cables. There are crawlers that can search your mobile phone for personally identifiable information (PII), account details, banking-related information, debit card details, credit card details and the other money transfer related apps i.e. user's name and passwords etc. within a fraction of seconds. There are lots of freeware apps and software available on the internet which clone target phones. It simply helps the attackers to get all the relevant information to perform smooth attack. On the internet or dark web various sources are available to provide the PII data which is sold on the dark web.

Malware installation.

The second way to install the malware on to the target device thought USB cable. On the internet or app store lots apps are available who help the attacker to install a malware onto the target mobile phones. These malware installed by the using the juice- jacking methods including the adware, spyware, ransom ware or Trojan. In fact ,android malware is mostly used now days. Spyware monitors the device for long time, whereas the ransom ware code freezes the device and encrypts all the data.

How to avoid being trapped:

Avoid public charging points or use power bank:- The very first method is to stop or avoid using the public charging point. Try use the private charging sources, if possible to carry a power bank or charge your mobile phones completely before leaving the home/ workplaces. Try to lessen the use of mobile phone while traveling . For a long distance travelling always use your own chargers or power bank.

Lock your mobile phones :- Make sure that you completely lock your mobile phone and don't give it to the unknown person for any reason. There are various locking methods available in the newly smartphones, i.e pin, pass code, draw patterns etc. But now days avoid using facelocks and finger lock because these locks are easily and fast accessible within fraction of seconds . So, make sure that phone securely locked and don't unlock at public charging point.

Switch off the mobile phone while charging:- Try to charge your mobile phone switched off conditions. In earlier mobile phones, there is a facility available in old mobile , but nowadays almost all mobile phones have these facilities inbuilt.

Used special cables:- In the market, there are lots of special cables which only meant for charging. So try to buy , carry and use these types of cables at the time using public charging points. These cables are only for charging and not meant for data transfer. It will help at some distant to become a juice jacking victim.

Use a USB Condom(Data blocker):- It is a normal device which is plugged between user cable and usb port to prevent the data transfer. In other words, this power adapter permits the user only to charging the device and halts the data transfer.

In the above picture t, a USB condoms (Data blocker device) is plugged on the usb cable.

Some factors of using USB condoms are :

- Charge mobile phone without worrying at public charging points.
- Turn a normal cable to charge only cable.
- Place it "always on" on our exiting USB cable.

Install an antivirus:- Make sure to Install an antivirus solution that stops any malware to download data theft. There are lots of paid anti- virus software available on the internet.

In the month of December 2019, the SBI bank issued a message on social media platform warning the public against the use of charging points.

Install an antivirus solution that stops any malware to download data theft .The best defence against any type of these attacks is to awareness and the safe use of mobile phones in public places .

Volume - 2
Issue - 1
January
2020
e-ISSN
2582-5755

References

- https://www.quora.com/Is-it-wise-to-charge-a-laptop-while-using-it?redirected_qid=2537830
- https://www.amazon.co.uk/Wireless-Charger-Mobile-Charging-Samsung/dp/B07WS2X7S6
- https://www.youtube.com/playlist?list=PLJ0VQ8a8YK1nCfB3NDf-_5trFLlR1s0lc
- https://zaroj.com/product/wireless-mobile-phone-charging-pad-dock/
- https://mobile.nation.co.ke/news/DusidD2-attack-suspect-lived-with-Jihadist-woman/1950946-4938638-format-xhtml-wkm2ia/index.html
- https://www.15minutenews.com/technology/2014/09/30/#!
- https://greedmedia.com/tag/mobile-phones/
- https://www.answers.com/Q/Does_Samsung_tab2_need_an_antivirus
- https://nationalcybersecurity.com/how-sim-swappers-can/
- https://forums.tomsguide.com/threads/antivirus-drives-direct-security-on-windows-10-am-i-able-to-use-on-windows-7.396241/?view=date
- https://security.stackexchange.com/questions/119988/out-of-band-verification-using-phone-a-fallacy/119998
- https://patents.google.com/patent/US20100151822A1/en
- https://es.scribd.com/document/236814966/PSP-gude-094
- https://www.mixcloud.com/blackhatbriefingslasvegas2006a/claudio-merloni-the-bluebag-a-mobile-covert-bluetooth-attack-and-infection-device/
- https://patents.google.com/patent/US9332119B1/en
- https://patents.google.com/patent/CN2660763Y/en
- https://www.quora.com/How-do-we-know-when-our-phone-is-hacked?redirected_qid=38440553
- https://www.collective-evolution.com/2018/03/20/why-multiple-countries-have-banned-wifi-cell-phones-around-schools-young-children-fetuses/?fbclid=IwAR1q1ethlHiPCUOOczGpmaTS4gbQqqg9L8uNF7hQ3ushIXs-cn-8eFsB95I
- https://es.scribd.com/document/92470380/Project-Report1
- https://www.researchgate.net/publication/332510509_Using_GPS-Enabled_Mobile_Computing_to_Augment_Qualitative_Interviewing_Two_Case_Studies
- https://www.crediteurope.ro/en/Data-security
- https://it.assam.gov.in/sites/default/files/swf_utility_folder/departments/it_dept_webcomindia_org_oid_2/portlet/level_1/files/CERT%20In%20Advisory%20notes%20for%20Cyber%20Security%20for%20Digital%20Payments.pdf
- https://medium.com/@remeshr/10-clear-signs-that-your-phone-was-hacked-35c3be4fa1f1
- https://www.phishprotection.com/content/cybersecurity-in-a-nutshell/
- https://www.protegent360.com/blog/
- https://docplayer.net/76390182-Introduction-to-cyber-security-fcs.html
- https://www.techslang.com/glossary/cybersecurity/
- https://www.1stadvantage.org/advice/security-center/information-cyber-security-corner/information-cyber-security-cyber-security-and-general-internet-terms
- https://www.snbt.com/assets/files/gUhfhTxX
- https://goldcoastpcrepairs.com.au/cyber-security

Ms. Shivani Sanwal is currently Computer Teacher in Tagore Model Senior Secondary School Nakodar distt Jalandhar Punjab.

shivanisanwal115@gmail.com

Dr. Kamaljit Singh is currently an Associate Professor in KRM DAV College, Nakodar, Jalandhar, India.

kamaljit70@gmail.com

Annexure I

Submission Date	Submission Id	Word Count	Character Count
17-Jan-2020	D63084224 (urkund)	1757	11153

Urkund Analysis Result

Analysed Document: vani new.docx (D63084224)
Submitted: 15/1/2020 9:46:00 AM
Submitted By: skesharwani@ignou.ac.in
Significance: 0 %

Sources included in the report:

Instances where selected sources appear: 0

Note:- The Cybernomics had used the Urkund plagiarism [http://www.urkund.com] tool to check the originality.

Reviewers Comment

Review 1: By way of you may have noticed, when you change your phone done the USB port of your computer or laptop, this also opens up the selection to change files spinal and forth amid the two systems.

Review 2: Except you have complete vicissitudes in your locations, the statistics transfer mode is incapacitated by default, except on devices consecutively older Android versions.

Review 3: In the first type of juice-jacking bout, cybercriminals could bargain any and all data from movable devices connected to charging positions through their USB ports. But there's no hoodie-wearing hacker sitting behind the panels of the kiosk.

Editorial Excerpt

The article has 0% plagiarism which is accepted as per the norms and standards of publication for the magazine. The authors have modified the article as per reviewers' comments and editorial boards suggestions. The comments related to this manuscript are noticeable related to the theme "**Juice Jacking**" both subject-wise and research- wise. Crimes and frauds of every kind these days are increasing with the evolution of information communication technologies. The new kind of data theft can be done by the USB charging cable known as Juice Jacking Method. After the editorial boards observations and blind reviewers remarks the article has been decided to categorise and publish under the "**Argument Based Credentials** (ABC)" category.

Acknowledgement

Author is highly indebted to Scholastic Seed Inc& editorial team of Cybernomics, For making the write-up in the shape of an article.

Disclaimer

All views expressed in this paper are my/our own. Some of the content is taken from open source websites & some are copyright free for the purpose of disseminating knowledge. Those some We/I had mentioned above in the references section and acknowledged/cited as when and where required. The author/s has cited their joint own work mostly, Tables/Data from other referenced sources in this particular paper with the narrative & endorsement has been presented within quotes and reference at the bottom of the article accordingly & appropriately. Finally some of the contents which are taken or overlapped from open source websites for the knowledge purpose. Those some of i/we had mentioned above in the references section.

Citation

Shivani Sanwal & Kamaljit Singh
"Juice Jacking - A type of Cyber attack"
Volume-2, Issue-1, Jan 2020.
(www.cybernomics.in)

Frequency: Monthly, Published: 2020
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.

Scholastic Seed Inc.
www.scholasticseed.in
https://orcid.org/0000-0002-7952-096X