Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

InfoSec Newsletter

MAY - JUNE 2019

E-WALLET SECURITY

InfoSec Concept 3 page

For Virus Alerts,Incident & Vulnerability Reporting
certin Handling Computer Security Incidents
www.cyberswachhtakendra.gov.in

सी डैक CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
Plot No. 6 & 7, Hardware Park, Sy No. 1/1,Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post)
Hyderabad - 501510 , Telangana(India)

ISEA oSec Newsletter

MAY - JUNE 2019

CREDITS

Honorary Professor. N Balakrishnan
(IISc, Bangalore)
Prof. Sukumar Nandi
(IIT, Guwahati)
Prof. V Kamakoti (IIT, Madras)
Prof. M S Gaur (SVNIT, Jaipur)

Design & Technical Team
Ch A S Murty
K Indra Veni
K Indra Keerthi
P S S Bharadwaj

Action Group Members
HoD (HRD), MeitY
Shri.Sitaram Chamarthy (TCS)
Prof. M S Gaur (MNIT, Jaipur)
Prof. Dr.Dhiren R Patel
(NIT Surat)
Representative of Chairman
(CBSE)
CEO, DSCI (NASSCOM)
Representative of Prasar Bharati,
Member of I & B
Shri U Rama Mohan Rao
(SP, Cyber Crimes, CID,
Hyderabad, Andhra Pradesh)
Shri S K Vyas, MeitY

Compiled by
G V Raghunathan
Ch A S Murty

From C-DAC
E Magesh, Director

Acknowledgement
HRD Division
Ministry of Electronics &
Information Technology

Supported by
For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

Message from

E Magesh

Director, C-DAC Hyderabad

Digital revolution has transformed every walk of our life ushering us into a new information age. Digitization has introduced us to new phase of cashless transactions making fiscal transactions seamless, transparent, safe and incredibly convenient. Right from shopping at big shopping malls to small scale vendors people are now using various available digital payment methods in India. e-wallets is one such digital payment method which gained immense popularity driven by ease of use, discounts and ubiquitous payment. According to the statistics projected by 'statista' the volume of mobile wallet transactions is projected to reach about 260 billion in 2022 from about 600 million transactions in 2016.

The risk of hacking will only grow as more and more people hop on to the digital platform. In view of rise in cyber frauds focusing on the prevailing digital payment methods, most of the e- wallets have incorporated strong security standards like encryption, biometric safeguards, and multifactor authentication etc. In spite of these measures e-wallets are potential target for hackers and possess the risk of security breach and fraud to the user. As responsible cyber user it is important to be aware of the different ways frauds can happen while using e-wallets.

The current newsletter educates its readers with the current cyber threats and vulnerabilities affecting e-wallets and the best practices that can be followed by the user to remain safe.

Connect us with /informationsecurityawareness

Follow us at /infosecawa

Subscribe us at /informationsecurityawareness

Follow us at /infosec_awareness

E-WALLET SECURITY

Mobile smart devices and mobile internet have changed the way we do things and how we connect with other people. With no doubt we can say that Smartphone has become a crucial part for our life. It has reached a state where it plays an important role in making our personal and professional lives easier. It also brought in remarkable changes in banking sector and also in the way we transact money online. When it comes to making payments in Cyberspace, there are many terms that are associated with it. The most commonly used ones are Virtual Payments, Virtual Currencies, e-wallets, Mobile Payments, etc. The boom in e-wallet transactions has been triggered by the rise tin E-commerce through mobiles, emergence of cheaper internet access and increasing mobile penetration.

More precisely we can say that an e-wallet refers to the method of transacting money online by making use of apps. It can be used in conjunction with mobile payment systems that allow customers to pay for purchases with their smart phones using QR codes, Unified payment Interface etc. An individual's bank accountcan be linked to these e- wallets to do the payments online.

What is an e-wallet?

e-wallet is a type of pre-paid account in which a user can store his/her money for any future online transaction. Instead of using your physical plastic card to make purchases, you can pay with your smartphone, tablet, or smartwatch. An e-wallet is protected with a password.

For setting up an e-wallet account, the user needs to install the software on his/her device, and enter the relevant information required. After shopping online, the e-wallet automatically fills in the user's information on the payment form. To activate the e-wallet, the user needs to enter his password.

With more and more people opting for e-wallets for making daily payments, e-wallet has become a major target for cyber criminals. There cannot be 100 percent security, it's all about managing the risk and minimising it to whatever extent possible. It is clear that the benefits of digital payments have made the e-commerce bloom in India but, at the same time, the risks associated has to be continuously monitored and managed.

Mobile payment Vs Mobile wallet

1. It is essential to keep in mind that there is a distinction between a Mobile Payment and a Mobile Wallet.
2. In mobile payment you are entering your credit card information at the final stage in the e-commerce transaction to complete the checkout process.Thus, no intermediary is involved.
3. Mobile wallets are specialized form of wallet to make the payment and it acts as an intermediary.

Difference between an E-Wallet and a Digital Wallet

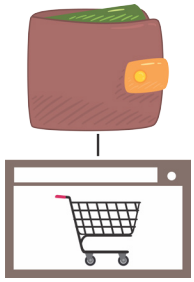
Digital wallet	E- Wallet
Cards details are saved in the wallets to transact cardless.	Money is preloaded in the wallets to transact cardless.
Money remains in user's bank account or credit card.	Money moves from user's account to either a merchant's current account or an escrow account
Example - Google Wallet, Apple's Passbook	Example - Paytm Wallet, Freecharge Wallet, Mobikwik.

Types of e-Wallets ?

In general, as per the Reserve Bank India, there are three kinds of e-wallets—closed, semi-closed and open

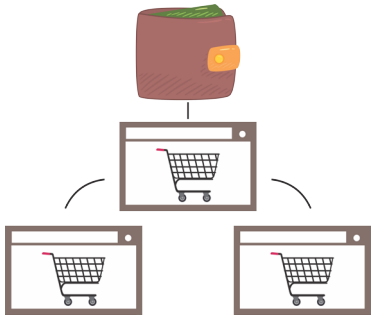
Closed wallet:

A closed wallet is one that a company issues to its consumers for in-house goods and services only. These do not carry the advantage of cash withdrawal or redemption. Several online shopping portals such as Flipkart, Jabong and MakeMyTrip offer such closed wallets. It is basically an account where money gets credited in case of a refund due to cancellation or return.



Semi-closed wallet:

In the payments space, companies such as MobiKwik, PayU and Paytm offer semi-closed wallets. As per the RBI, a semi-closed wallet can be used for goods and services, including financial services, at select merchant locations or establishments that have a contract with the issuing company to accept these payment instruments. Semi-closed wallets do not permit cash withdrawal or redemption by the holder as well.



Open wallet:

Such wallets can be used for purchase of goods and services, including financial services such as funds transfer at merchant locations or point-of-sale terminals that accept cards, and also cash withdrawals at automated teller machines or business correspondents. These kinds of wallets can only be issued by banks.

Where the money goes ?		
To the company's account	To excrow account	To bank account
What happens to the money ?		
Companies either earn interest on it or the money is taken as liability on the books of the company till the customer uses it to make a purchase	There is either no interest earned or 4-8% is earned based on the average balance calculation approved by the central bank	It earns interest, which is shared between the payment service provider and the bank depending on the agreement

How e –Wallets works ?

E-wallets have two primary components: software and information. The software component stores your personal information; provide security and encryption of data. The information component is a database of details provided by the user which includes names, shipping addresses, payment methods, amount to be paid and debit/credit card details.

To set up an e-wallet, you need to first choose an E-wallet and install the software on your device. To use this wallet, first you have to open your account in that wallet that you want to use and for this it is mandatory to have a mobile number. To activate the e-wallet, you will need a password. After registering to this service, money can be transferred to the wallet with the help of a debit or credit card and then at the time of purchase you can use money wallet with the help of a Smartphone.

How cyber criminals try to fraud an e wallet user ?

The E-wallet user is very much exposed to the technical side of the threat vectors, such as rogue mobile applications, Malware, and even Spyware being covertly installed on the Smartphone. However, the E-wallet user is also prone to Social Engineering attacks as well. For example, there is the risk of Phishing E-Mails to the enduser. However, the fraudster can make vishing calls, and convince the E-wallet user to share their private/ confidential data, also in giving out their financial information.

Using stolen Credit Cards

Cybercriminals are now relying on e-wallets to steal money from stolen Credit Cards. It is very easy to create an e-wallet account. All you need is a valid phone number. This allows scammers to create multiple e-wallet accounts using different SIM cards. They can then load money from the stolen cards into these accounts. Money can be loaded into e-wallets using debit and credit cards, or net banking passwords. These frauds are possible because the mobile wallet companies don't keep a check on who opens an e-wallet account. The stolen money is usually used to make purchases or do recharges online. The process of KYC is implemented by e-wallets as per RBI regulations to prevent such kind of frauds.

Impersonation

Frauds through impersonation have been prevalent in the banking industry. Impersonating basically involves stealing someone else's e-wallet information (including passwords) and making transactions by posing as them. The usual targets are less tech-savvy e-wallet users.

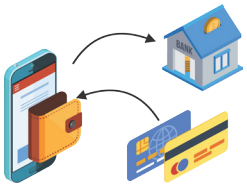
SIM swaps

With mobile phones becoming a convenient tool for banking, fraudsters have begun to use SIM-swap. Initial step taken by the fraudster is to get hold of your banking information. After obtaining your bank account details he registers your mobile phone number with the bank through phishing or malware. He approaches your mobile service provider with your fake identity proof and, claiming loss of handset or SIM damage, seeks a duplicate SIM card. Following verification, the original SIM is deactivated and a new one is issued to the fraudster. He then initiates financial transactions from your bank account, details of which he had earlier stolen, and receives payment confirmation requests on the duplicate SIM. Since the original SIM has been deactivated, you remain unaware about the fraudulent transactions he makes. The scammer can easily obtain one-time passwords and make transactions using the stolen e-wallet information of the user.

Malware attacks

Some e-wallet apps have not embedded proper security to prevent malware attacks. This makes it easy for tech-savvy fraudsters to inject malware into these applications and collect details of users from their phones.

Cashing out Credit Cards



A major ambiguity of e-wallets is that they allow users to cash out their credit cards easily. It means that an e-wallet account holder can transfer money from his credit card to his bank account without any fees or interest for using his account. All he has to do is load money from his credit card to the e-wallet and then transfer this amount to his bank account. Few Mobile wallet companies have addressed this issue by setting a limit on the amount that can be transferred to a bank account.

Public network

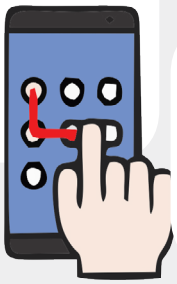
Using a public network can also be risky. Your sensitive data and the mobile device can easily be accessed if you use a public network. It is always better to avoid connecting your Smartphone to any public network.

Ransomware:

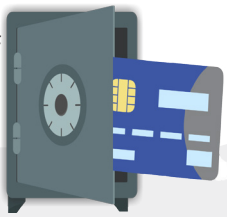
Ransomware has become a global cyber-threat. It blocks or encrypts one's files and then are asked for a ransom to decrypt those locked files. The biggest threat with Ransomware is that it's classified as a worm. Being a worm, the ransomware has the ability to spread to different systems running on the same LAN network or even spread through emails. This is the most trending security concern for e-wallets and online transactions. The scammers get an access to users' mobile phone and computer system through a remote access system.

Tips to keep in mind for enhancing your e- wallet security

1 Enable Passwords on Your Devices:
Enable passwords on your phones, tablets, and other devices that you use. Use the benefits of security settings provided by these devices.



2 Don't save your cards
While doing transactions through your e-wallet, you should never save the details of your credit or debit cards.



Available on the App Store

Get it on Google play

3 Install apps from sources you trust:
Apps are not always what they appear to be. A free game might not be just a game, but an app designed to illegally collect personal data from you. Reading the user ratings and reviews can provide some clues about the integrity of the app.

4 Keep Your Private Stuff Private:
Never share sensitive data with those you don't trust. Banks will never ask for private information such as passwords or account numbers.

5 Keep Login Credential Secure:
Avoid writing down information used to access the digital wallets or storing in an unprotected file. Easy access to them might result in the misuse of your data and credentials.

6 Create a Unique Password for Your Digital Wallet
Avoid using the same password you use for email or social networking sites. This increases the risk of unauthorized access. Instead, use an easy to remember, yet hard-to-guess password which is unique for your E-wallet. This will enhance your digital wallet security.

7 Use multi-factor authentication
While creating your profile on E-wallets, you should activate multi-factor authentication for your password. Create a strong password having the complex combination.

8 Avoid unsolicited e-mails or messages
Never click on any message that appears to be unsolicited. Don't click any link if it is not coming from the official sources.

9 Use Secure Network Connections:
Always be aware of the kind of networks you are connected to. It's important to be connected only to those networks which you can trust. Avoid the use of public Wi-Fi networks. More secure WiFi connections require passwords and are easily identified (Wi-Fi protected access) as "WPA or WPA2." Highly-insecure WiFi is wide-open for anyone to connect to and may be labeled as a "WEP" (wired equivalent privacy) connection.

CASE 1

Example 1: With the increase in e-payments and e-wallet transactions, the chances of frauds and scams have also increased. Let's see what happened with an IT manager from Thane. IT Manager of leading private bank lost Rs 24000 from his e wallet as racketeers accessed his two e-wallet accounts and transferred money from them. The victim received several email messages on October 28th 2017 about money being debited from his two different e wallet account. But he couldn't check it immediately as he was at work. Even the e wallet operators have sent him mails regarding a new login to his account and also provided with helpline numbers to contact if in case those transactions were not done by him. Later when he checked he was shocked that money was debited from his account without his knowledge. He lodged a complaint to the nearest police station.

Police could track two numbers through which transaction was carried out and have registered an offence under 419 and 420 of the IPC and also sections 66(C) and 66(D) of IT Act against two numbers. According to the police the cyber criminals used cloned debit cards or may have

Private bank techie loses Rs 24,000 to e-wallet fraud

THANE: An IT manager of a leading private bank lost nearly Rs 24,000 as racketeers accessed his two e-wallet accounts and transferred money from them.

Police said the victim, a senior manager in the IT department of the bank, received several email alerts on October 28, about money being debited from his e-wallets several times—totally Rs 13,500 from Paytm and Rs 10,500 from Mobikwik—but he didn't check them immediately as he was at work then. In fact, the e-wallet operators had even sent him emails about a new log-in from his account and provided a helpline to

fraudulently got the UPI or PIN of the victim's e-wallet and could debit the money.

Source : http://timesofindia.indiatimes.com/articleshow/62235966.cms?utm_source=contentofinterest&utm_medium=-text&utm_campaign=cppst

CASE 2

The incident took place in New Delhi when the phone was given for repair to an authorised agent. The victim has lost Rs 91,000 in a digital wallet fraud. The agent at the service centre asked the victim to remove his SIM card and leave the phone with him for a day assuring him that all his data would remain safe. Later that evening, he got a call from the service centre asking him to pick up his phone. When he inserted his SIM card into his phone, he got several messages informing him that a sum of Rs 91,000 had been transferred from his account to another account. Later he found out that all the data associated with the money transfer and the app used for the transaction had been deleted from his phone.

He registered a complaint in the police station informing them of the fraud. Furthermore, upon preliminary investigation the police found out that the victim had recently got his KYC done, which had linked his mobile wallet with his bank account. This in turn enabled the tricksters to dupe him out of the money. The police suspect that the crooks used Wi-Fi to transfer money. The police have sent the smartphone for forensic analysis and they are now trying to determine the IP address that the fraudsters used to transfer money from his mobile wallet.

- There are chances that your

News / Technology / News / Fraudsters steal Rs 91,000 from a man's e-wallet

Fraudsters steal Rs 91,000 from a man's e-wallet

The police are now trying to determine the IP address that was used to transfer money from the victim's mobile wallet

Shweta Ganjoo
New Delhi
November 5, 2018 UPDATED: November 5, 2018 12:55 IST

HIGHLIGHTS

- The incident took place on Wednesday when a Delhi based man gave his smartphone for repair at an authorised service centre
- In the evening the victim got to know that a sum of Rs 91,000 had been transfered from his account to another account
- The Police suspect that the fraudsters used Wi-Fi to transfer money

E-wallet frauds have become a fairly common phenomenon in India. Fraudsters often use creative technological measures to dupe innocent smartphone users into giving up their hard-earned money. Back in August, a Kolkata-based man lost a sum of Rs 65,000 in a case of e-wallet fraud. The victim reportedly came across a fake Facebook page that promised to refund Rs 2,400 that he had lost earlier to a nationalised bank. The page prompted victim to install an app and enable cashless payments. When he entered his details into the mobile payment app to initiate a refund of Rs 2,400, he was informed that a sum of Rs 24,000 had been transferred from his account. This went on till the victim realised that he had been duped of Rs 65,000, which is when he informed the police. And now, in a recent incident, a New Delhi based man lost Rs 91,000 in a digital wallet fraud after he gave away his phone to an authorised agent of the mobile company for repair work.

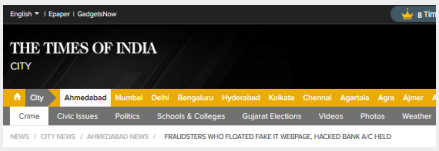
phone may fall into wrong hands, who might use it to make fraudulent transactions.

Source : https://www.indiatoday.in/technology/news/story/fraudsters-steal-rs-91-000-from-a-man-s-e-wallet-1382689-2018-11-05

CASE 3

The incident happened in Kolkata where an e-wallet user lost a sum of Rs 65,000. The victim reportedly came across a fake Facebook page that promised to refund Rs 2,400 that he had lost earlier to a nationalised bank. The page prompted victim to install an app and enable cashless payments. When he entered his details into the mobile payment app to initiate a refund of Rs 2,400, he was informed that a sum of Rs 24,000 had been transferred from his account. This went on till the victim realised that he had been duped of Rs 65,000, which is when he informed the police.

- Phishing attacks are used to steal users' login details and personal data, making e-wallet accounts susceptible to fraud.



Fraudsters who floated fake IT webpage, hacked bank a/c held

Published on : Jun 13, 2019

AHMEDABAD: Seven persons including three Nigerians have been arrested by city police for hacking into over 2,000 bank accounts and transferring crores of rupees after creating a fake webpage of the Income Tax Department.

The accused lured victims across the country by promising income tax (IT) refunds, and for the first time arrests have been made in these cases, the local cyber crime cell claimed.

The accused were arrested from Mumbai Wednesday and brought here, said assistant commissioner of police (cyber crime) J M Yadav.

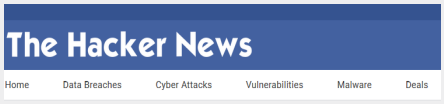
The accused allegedly targeted 4,727 people across India, of which over 2,500 were duped of crores of rupees. There were at least 57 unsolved cases of such frauds in the country, Yadav added.

Ahmedabad police started a probe after Tejas Shah, a city-based doctor, filed a complaint that over Rs 2 lakh were transferred from his account on June 22 last year.

Explaining the accused's modus operandi, Yadav said, "They first sent a web link to the victim through SMS, promising to get IT refund. When the victim clicked the link, he was directed to a `phishing' page (a fake webpage) resembling the webpage of the IT Department.

"After the victim filled in the name of his bank, he was directed to a fake webpage of the bank where he was asked to fill in all the details of his bank account," the ACP said.

Reference : https://timesofindia.indiatimes.com/city/ahmedabad/fraudsters-who-floated-fake-it-web-page-hacked-bank-a/c-held/article-show/69776395.cms?from=mdr



Beware! Playing Untrusted Videos On VLC Player Could Hack Your Computer

Published on : Jun 21, 2019

If you use VLC media player on your computer and haven't updated it recently, don't you even dare to play any untrusted, randomly downloaded video file on it.

Doing so could allow hackers to remotely take full control over your computer system.

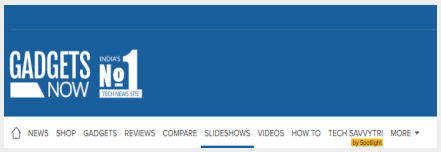
That's because VLC media player software versions prior to 3.0.7 contain two high-risk security vulnerabilities, besides many other medium- and low-severity security flaws, that could potentially lead to arbitrary code execution attacks.

With more than 3 billion downloads, VLC is a hugely popular open-source media player software that is currently being used by hundreds of millions of users worldwide on all major platforms, including Windows, macOS, Linux, as well as Android and iOS mobile platforms.

Discovered by Symeon Paraschoudis from Pen Test Partners and identified as CVE-2019-12874, the first high-severity vulnerability is a double-free issue which resides in "zlib_decompress_extra" function of VideoLAN VLC player and gets triggered when it parses a malformed MKV file type within the Matroska demuxer.

The second high-risk flaw, identified as CVE-2019-5439 and discovered by another researcher, is a read-buffer overflow issue that resides in "ReadFrame" function and can be triggered using a malformed AVI video file.

Reference : https://thehackernews.com/2019/06/vlc-media-player-hacking.html



How criminals are using these 7 Google apps to empty your bank account

Published on : Jun 25 2019

Google is omnipresent in anyone and everyone's life who uses a smartphone or a computer. The tech giant's apps and services are widely popular which also make it a target for cybercriminals. According to a new report by Kaspersky, a cybersecurity firm, online fraudsters are – or rather have been – targeting various Google services like Calendar, Drive, Photos amongst others to dupe people for money. Here we list out 7 Google apps that criminals are targeting to empty your bank account:

Scammers send users a fake invite and send reminders just before the event. Hackers add invitations to your Google Calendar account which send you a reminder suggesting that you have a wire transfer in your bank account and you are required to complete the information by adding the account PIN number.

As per Kaspersky, scammers use Google Photos to share photographs that include comments about sudden large money transfer promises. This can only be done once a user replies to a mail. "For the recipient, it looks like a harmless e-mail from Google Photos with the header "So-and-so shared a photo with you but it's actually a scam to get money from users.

While this doesn't really take money but is designed to hurt real businesses and end up confusing users as well. Fake listings are created on Google Maps and at times users might get tricked into dealing with fake business enterprises rather than real ones.

Reference : https://www.gadgetsnow.com/slideshows/how-criminals-are-using-these-7-google-apps-to-empty-your-bank-account/Google-Drive-By-using-Cloud-storage/photolist/69933530.cms

Hackers in 'SIM swap' scam arrested in city

Published on : May 29, 2019

A gang, which sent emails with spyware to hack victims' data to steal their ID first then their money, was busted by the cybercrime police on Tuesday. The police arrested all six members of the gang that would hack into a computer, use the data to forge documents and steal the victims' money from bank accounts.

The men, arrested from the city, were identified as Matadeen Sikarwar (38) of Rajasthan, and Janmohammed Khalifa (54) of Himmatnagar, Anil Joshi (39) of Malad West in Maharashtra, Arvind Patel (40) of Kutch, Rajeshgiri Goswami (55) of Vadodara and Dipakkumar Rupala (31), resident of Naroda. Police said, "Matadeen met Joshi in Kolhapur jail. After being released in 2018 they contacted the rest of the team and committed this crime."

The cops were acting on a complaint filed by Rameshkumar Shah a resident of Shahibaug. He had approached police on May 20 after Rs 82 lakh from five of his bank accounts we re stolen in aspan of one and a half days.

As his SIM card had become operational immediately before the money was transferred, Inspector V B Barad and his team realised that Shah had been targeted by SIM swap fraudsters

Reference : https://ahmedabadmirror.indiatimes.com/ahmedabad/crime/hackers-in-sim-swap-scam-arrested-in-city/articleshow/69549167.cms

HiddenWasp Linux Malware

It has been observed that a new malware named as "HiddenWasp" targeting Linux operating systems is spreading. The malware focuses primarily on gaining remote access of the infected hosts making it different from other Linux malwares which aims crypto-mining or DDoS activity. The infection vector used by the malware is not known. The malware is capable of performing the following functions:

- Gaining remote access to the infected machine.
- Evade detection from variety of antivirus solutions.
- Uses malicious code from other known malwares namely Azael Rootkit and Mirai.
- Update existing versions of HiddenWasp on the compromised machine
- Make network connections to download other malwares.
- Make use of rootkits, Trojan implants and creation of ftp user account to maintain persistence in the system.

The malware is a combined package of various open source malwares such as an initial deployment script for downloading other malwares along with updating existing threats, a rootkit using Mirai code to hook into several functions and a Trojan having features of Azael rootkit that worked with the rootkit to remain operational. Also, similarities have been found in the HiddenWasp malware and other Linux malware named as Winnti malware.

Working

Malware start its activities by execution of the initial deployment script which contains a code to create a user named as "sftp" on the compromised system with hardcoded password to maintain attacker's access to infected machine even after the malware detection and cleanup. It is shown as below:

```
21 LIBPATH="/lib/libse1inux.so"
22 PIDFILE="/tmp/libse1inux.0"
23 PROEXE="I_AM_HIDDEN=a nohup /lib/
24
25 # about user
26 FTP_USER="sftp"
27 FTP_PASSWD="e@iQN*lG"
28 FTP_FOLDER="/var/sftp"
```

Source: Intezer

For more details visit :
https://www.cyberswachhtakendra.gov.in/alerts/hiddenwasp.html

CERT-In Advisory CIAD-2019-0022

Multiple Vulnerabilities in Intel

Overview

Multiple vulnerabilities have been reported in Intel products which could be exploited by an attacker to gain escalation of privileges, denial of service condition or information disclosure on the targeted system.

Description

Multiple vulnerabilities exist in Intel products due to improper data sanitization, insufficient access control, insufficient input validation, code injection, out of bound write error, logic bug vulnerability, buffer overflow vulnerability or logic issue error.
Successful exploitation of these vulnerabilities could allow the attacker to gain escalation of privileges, denial of service condition or information disclosure on the targeted system.

For more details : https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2019-0022

CERT-In Vulnerability Note CIVN-2019-0098

Remote code execution vulnerability in Linux

Software Affected

Vim versions prior to 8.1.1365
Neovim versions prior to 0.3.6

Overview

A vulnerability has been reported in getchar.c source code file of Vim ,which could allow an authenticated, remote attacker to execute arbitrary code on the targeted system.

Description

This vulnerability exists in getchar.c source code file of Vim due to improper validation of user-supplied input by the affected software. A remote attacker could exploit this vulnerability by executing the source command in a modeline on the affected system.

Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code on the targeted system.

For more details : https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2019-0098

InfoSec QUIZ

1. The primary source of financing during the early years of e-commerce was _____?
   a) Bank Loans
   b) Large retail firms
   c) Venture capital funds
   • Initial public offerings

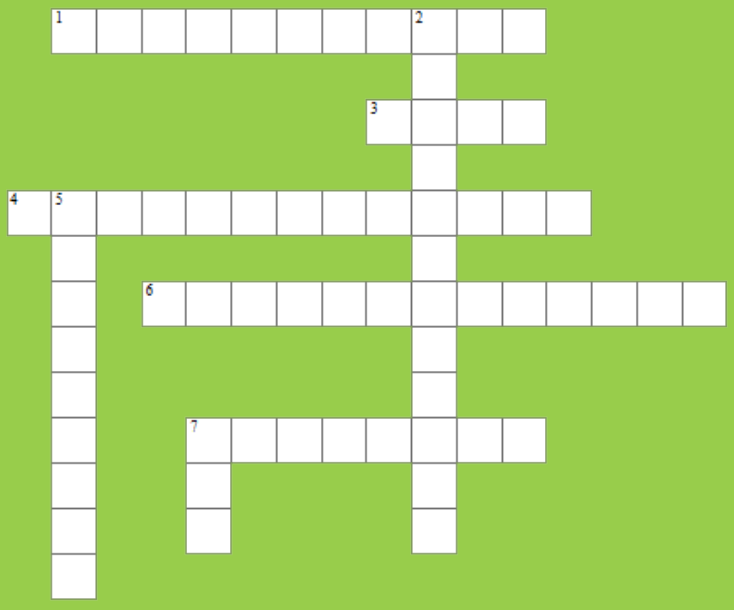
2. A _____ is the set of planned activities designed to result a profit in a market place.
   a) Business model
   b) Profit model
   c) Business plan
   d) Revenue model

3. Which segment is ebay an example?
   a) B2B
   b) C2B
   c) C2C
   d) None of the above

4. If you need to transfer money to another person via the internet, which of the following methods could you use?
   a) Financial cybermediary
   b) Electronic check
   c) Electronic bill presentment and payment
   d) All of the above

5. What is the name for direct computer-to-computer transfer of transaction information contained in standard business documents?
   a) Internet commerce
   b) E-commerce
   c) Transaction information transfer
   d) Electronic data interchange

InfoSec CROSSWORD



Across

1. The redirection of traffic from a legitimate site to an infringing site is called ___.
3. The only payment system that is instantly convertible without intermediation is _____.
4. A combination of software and information designed to provide security and information for payment is called?
6. An electronic check is one form of _____ .
7. _____ is one of the most widely used methods to commit credit card fraud by using magnetic strips in ATM machines.

Down

2. Which of the following is not a dimension of e-commerce security provided by encryption?
5. Accuracy and consistency of data is called
7. The most common form of securing channels is through _____

Logon to

www.infosecawareness.in

to participate in
InfoSec Contest and win Prizes

To Share Tips / Latest News, mail us to

isea@cdac.in

About ISEA

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project by Ministry of Electronics & Information Technology, Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events all over India.

About C-DAC

C-DAC established its Hyderabad Centre in the year 1999 to work in Research, Development and Training activities embracing the latest Hardware & Software Technologies. The centre is a Knowledge Centre with the components of Knowledge Creation, Knowledge Dissemination and Knowledge Application to grow in the areas of Research & Development, Training and Business respectively. The R & D areas of the centre are e-Security, Embedded Systems, Ubiquitous Computing, e-Learning and ICT for Rural Development. The centre has developed over a period of time a number of products and solutions and has established a number of labs in cutting edge technologies. In line with these R&D strengths, the centre also offers Post Graduate level diploma courses. Centre is also actively involved in organizing faculty training programs. The centre regularly conducts skill based training and information security awareness programmes. InDG portal is hosted and maintained to facilitate rural development through provision of relevant information, products and services in local languages.

BOOK POST

For queries on Information security

Call us on Toll Free No.

1800 425 6235

between 10.00 AM to 6.00 PM
or give us a missed call
we will call you back within 24 hrs

ISEA Whatsapp Number for Incident Reporting

+91 9490771800

Between 9.00 AM to 5.30 PM

Subscribe us on

https://www.youtube.com/c/InformationSecurityEducationandAwareness

Follow us on

https://twitter.com/InfoSecAwa

Connect us with

https://www.facebook.com/infosecawareness

Ministry of Electronics & Information Technology
Government of India

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India

Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 501510, Telangana(India)

Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)