Information Security Education & Awareness
Department of Electronics & Information Technology,
Ministry of Communications & Information Technology,
Government of India.

InfoSec Newsletter
January 2015

InfoSec Tools 7

Top Android Security Apps

M-Kavach

InfoSec Concept 4:

Mobile Phone Security

www.infosecawareness.in

Participate in InfoSec

Quiz

Crossword

Guess the tip

For Virus Alerts, Incident & Vulnerability Reporting
cert-in
Handling Computer Security Incidents

सीडैक
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
Nalanda Building, Road No : 1, Shivbagh, Near Satyam Theatre, Ameerpet, Hyderabad - 500016
E-mail : isea@cdac.in

InfoSec

Newsletter

January - 2015

Credits

Editorial Committee

Shri.Sanjay Kumar Vyas
Joint Director, DeitY

E.Magesh,Director
Mr.Ch.A S Murty,
Mrs.Indraveni K,
Shri G.V.Raghunathan
(C-DAC Hyderabad)

Design Team
K.IndraKeerthi
S.Om Aarathi

Action Group Members

Dr.Kamlesh Bajaj
Data Security Council of India
Shri.Sitaram Chamarthy
Principal Consultant, TCS
Dr.Dhiren R Patel
Professor of Computer Engineering,
NIT Surat
Dr.N. Sarat Chandra Babu
Executive Director,
C-DAC Bangalore
&
HOD, HRD Division
DeitY, Government of India

Acknowledgement

HRD Division
Department of Electronics
& Information Technology
Ministry of Communications
and Information Technology
Government of India

Comments & Feedback
mail us to
isea@cdac.in

INFOSEC QUIZ

It is one of the malware
(a)gossips (b)threat (c)vulnerability (d)ransomware

We can click on the links received from known or unknown emails ID's
(a)True (b)False

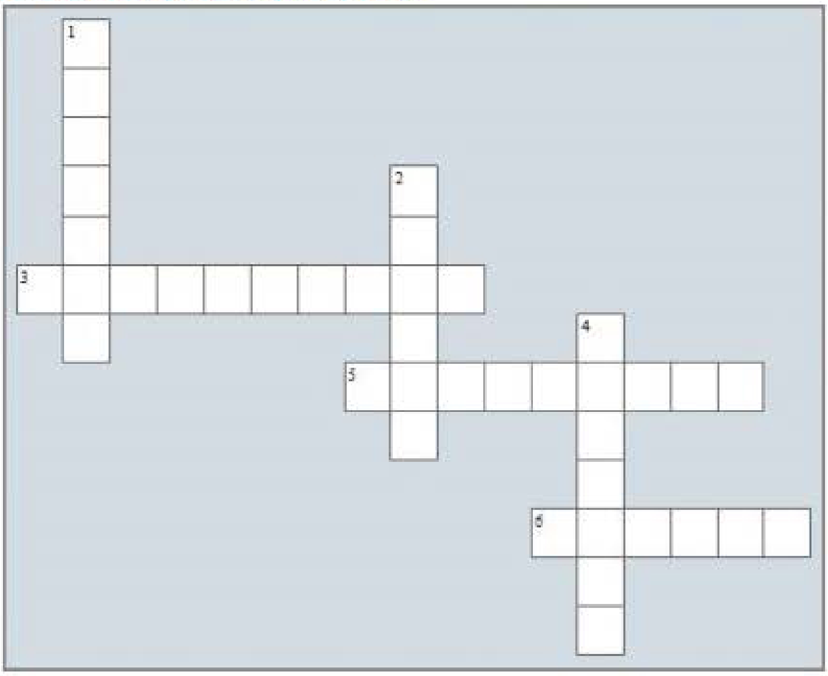
We can copy the content available over internet and we cannot be sued for copyright violations
(a)True (b)False

A Hacked computer can be used to
(a)Infect other systems (b)Harm your system by malware
(c)Help your system with latest updates (d)Both a and b

My email is private and no one can look into it
(a)True (b)False

logon to
www.infosecawareness.in
to participate in Infosec Contest and win prizes

INFOSEC CROSSWORD



Across:

3. uses an algorithm that transforms information and making it unreadable & inaccessible to anyone except for those who have the appropriate credentials
5. restrict network activity to known applications, and prevent malicious people and programs from exploiting holes in operating systems and other software applications
6. ensures that the information you need is there when you need it and it can recovered if the information is damaged in the system.

Down:

1. It is one of the methods of social engineering
2. The information stored on client computer by a webserver is called a
4. Is harmful software, usually installed without your knowledge

INFOSEC GUESS TIP

Guess the Tip which best suits the cartoon by logging in to http://www.infosecawareness.in

InfoSec Tip

Do not pursue links that offer free Anti-Virus or Anti-Spyware software.

Malware: Malware in short known for malicious software. It is a software designed to infiltrate a computer system without the owner's informed consent.Malware includes computer viruses, worms, trojan horses, rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software.Around 80% of malware today is designed to find and steal confidential information stored on your computer. This type of malware is sometimes called "crimeware."Malware can invade your machine through infected email attachments, "bots" that crawl the Internet looking for unprotected computers, and visits to "hostile" Web sites.

Virus: A computer virus is a program which is able to replicate and attach itself to a program or files infecting the system without our knowledge. The software programs that hide on your computer and cause mischief or damage.

Spyware: Spyware is a generic term for malicious software which ends up on your computer, and is used to gather information about you and other files on your computer and passes it over internet to others.Generally speaking, spyware is software that hides on your computer, tracks what you're doing online, and then sends that information over the Internet. Some types of spyware, called "keystroke loggers" actually record and send everything you type on your computer.Spyware software can sneak onto your computer when you download unsafe software and files—or even visit a hostile Web page.One major source of spyware is the peer-to-peer file sharing software commonly used to share music and videos online.

Worm: Worms can replicate themselves from one machine to another without the need of downloading them from the internet. They often send themselves as attachments in emails they generate from their infected host computer and it may do so without any user intervention. This is due to security shortcomings on the target computer or by exploiting vulnerabilities in operating systems. Worms almost always cause at least some harm to the network.

Trojan: It is a non-self-replicating malware that appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system.Trojans are backdoors in to your computer in which access is gained by hackers and gain remote access to a target computer system to perform various operations.The operations that a hacker can perform are limited by user privileges on the target computer system and the design of the Trojan horse on the internet to either gather information from your computer or to use your computer.

MOBILE PHONE SECURITY

Mobile phones are becoming ever more popular and are rapidly becoming attractive targets for malicious attacks. Mobile phones face the same security challenges as traditional desktop computers, but their mobility means they are also exposed to a set of risks quite different to those of a computer in a fixed location. Mobile phones can be infected with worms, trojan horses or other virus families, which can compromise your security and privacy or even gain complete control over the device. This guide provides the necessary steps, do's, don'ts & tips to secure your mobile devices.

Be aware of social engineering attacks on mobile and Bluetooth devices.

Mobile Phone Security Threats Categories:

- Mobile Device and Data Security Threats
  - Threats related to unauthorised or intentional physical access to mobile phone and Lost or Stolen mobile phones.
- Mobile Connectivity Security Threats
  - Threats related to mobile phone connectivity to unknown systems, phones and networks using technologies like Bluetooth, WiFi, USB etc.
- Mobile Application and Operating System Security Threats
  - Threats arising from vulnerabilities in Mobile Applications and Operating Systems.

Typical impact of attacks against Mobile Phones:

- Exposure or Loss of user's personal Information/ Data, stored/transmitted through mobile phone.
- Monetary Loss due to malicious software
- unknowingly utilizing premium and highly priced SMS and Call Services.
- Privacy attacks which includes the tracing of mobile phone location along with private SMSs and calls without user's knowledge.
- Loosing control over mobile phone and unknowingly becoming zombie for targeted attacks.

Mitigation against Mobile Device and Data Security Attacks:

Do's for Mobile Device

- **Record IMEI number:** Record the unique 15 digit IMEI number. In case Mobile phone is stolen/ lost, this IMEI number is required for registering complaint at Police station and may help in tracking your mobile phone through service provider.

- **Enable Device locking:** Use autolock to automatically lock the phone or keypad lock protected by passcode/ security patterns to restrict acess to your mobile phone.

- **Use a PIN to lock SIM card:** Use a PIN (Personal Identification Number) for SIM (Subscriber Identity Module) card to prevent people from making use of it when stolen. After turning on SIM security, each time phone starts it will prompt to enter SIM PIN.

- Use password to protect information on the memory card.

Report lost or stolen devices

- Report lost or stolen devices immediately to the nearest Police Station and concerned service provider. Use mobile tracking feature.
- Use the feature of Mobile Tracking which could help if the mobile phone is lost/stolen. Every time a new SIM card is inserted,in the mobile phone, it would automatically,send messages to two preselected,phone numbers of your choice, so,that you can track your Mobile device.

Dont's for Mobile Device

- Never leave your mobile device unattended.
- Turn off applications [camera, audio/ video players] and connections [Bluetooth, infrared, Wi-Fi] when not in use. Keeping the connections on may pose security issues and also cause to drain out the battery.

Do's for Data Security:

- **Backup data regularly** : Backup data regularly and set up your phone such that it backs up your data when you sync it. You can also back up data on a separate memory card. This can be done by using the Vendor's document backup procedure.
- **Reset to factory settings:** Make sure to reset to factory settings when a phone is permanently given to another user to on sure that personal data in the phone is wiped out.

Providing mobile PC or mobiles to access internet for official purpose's remote access to all business applications may put a personal or organization's vital information at risk. For professionals or individual users, using mobile or mobile PC, there are plenty of benefits such as work from anywhere, etc...The mobile devices have their own characteristics but also with security concerns such as sensitive information access with mobiles.

Mitigation against Mobile Connectivity Security Attacks

- **Bluetooth:** Bluetooth is a wireless technology that allows different devices to connect to one another and share data, such as ringtones or photos. Wireless signals transmitted with Bluetooth cover short distanes, typically 30 feet (10 meters).

Do's:

- Use Bluetooth in hidden mode so that even if the device is using Bluetooth it is not visible to oth- ers.
- Change the name of the device to a different name to avoid recognition of

your Mobile phone model.

Note: The default name will be the mobile model number for Bluetooth devices.

- Put a password while pairing with other devices. The devices with the same password can connect to your computer
- Disable Bluetooth when it is not actively transmitting information.
- Use Bluetooth with temporary time limit after which it automatically disables so that the device is not available continuously for others.

- Never forward the virus affected data to other Mobiles.

Mitigation against Mobile Application and Operating System Attacks

Application and Mobile Operating System:

- Update the mobile operating system regularly.
- Upgrade the operating system to its latest version.
- Always install applications from trusted sources.
- Consider installing security software from a reputable provider and update them regularly.
- Check the features before downloading an application.Some applications may use your personal data.
- If you're downloading an app from a third party, do a little research to make sure the app is reputable.

Enable Bluetooth only when you need it.

Don'ts:

- Never allow unknown devices to connect through Bluetooth.
- Never put Bluetooth in always discoverable mode.

  Note: Attackers can take advantage of its default always-on, always discoverable settings to launch attacks.
- Never leave the Bluetooth switch on continuously.

- **Wi-Fi:** Wi-Fi is short for "Wireless Fidelity."Wi-Fi refers to wireless networking technology that allows computers and other devices to communicate over a wireless signal. Many mobile devices, video game systems, and other standalone devices also include Wi-Fi capability, enabling them to connect to wireless networks. These devices may be able to connect to the Internet using Wi-Fi.

Do's:

- Connect only to the trusted networks.
- Use Wi-Fi only when required. It is advisable to switch off the service when not in use.
- Beware while connecting to public networks, as they may not be secure.

Don'ts:

- Never connect to unknown networks or
- untrusted networks.

- **Mobile as USB:** The mobile phones can be used as USB memory devices when connected to a computer. A USB cable is provided with the mobile phone to connect to computer. Your mobile's phone memory and memory stick can be accessed as USB devices. Your mobile's phone memory and memory stick can be accessed as USB devices.

Do's:

- When a mobile phone is connected to a personal computer, scan the external phone memory and memory card using an updated anti virus.
- Take regular backup of your phone and external memory card because if an event like a system crash or malware penetration occurs, at least your data is safe.
- Before transferring the data to Mobile from computer, the data should be scanned with latest Antivirus with all updates.

Don'ts:

- Never keep sensitive information like user names/passwords on mobile phones.

Change your default administrator passwords and usernames for your mobile devices and Wi-Fi devices.

Security Concerns

Exposure of critical information

Small amounts of WLAN signals can travel significant distance, and it's possible to peep into these signals using a wireless sniffer. A wireless intruder could expose critical information if sufficient security isn't implemented.

Mobile Viruses

Mobile Viruses can be major threat, particularly with devices that have significant computational capabilities. Mobile devices, in general are susceptible to Viruses in several ways. Viruses can take advantage of security holes in applications or in applications or in the underlying Operating System and cause damage. Applications downloaded to a mobile device can be as Virus-prone as desktop applications. In some mobile OS, malformed SMS messages can crash the device.

Dial 112
Your mobile will search any existing network to establish the emergency number for you

Interestingly this number 112 can be dialed even if the keypad is locked

E-mail Viruses

E-mail Viruses affect PDAs in much the same way regular e-mail Viruses affect PCs. These Viruses are costly to enterprises and interrupt normal business too. PalmOS / LibertyCrack is an example of a PDA e-mail virus. It's a known Trojan horse that can delete all applications on a Palm PDA.

Bluesnarfing

Bluesnarfing is the theft of data from a Bluetooth phone. Like Bluejacking, Bluesnarfing depends on the ability of Bluetooth-enabled devices to detect and contact others nearby. In theory, a Bluetooth user running the right software on a laptop can discover a near by phone, connect to it without your confirmation, and download your phonebook,

pictures of contacts and calendar. Your mobile phone's serial number can also be downloaded and used to clone the phone. You should turn off Bluetooth or set it to "undiscoverable". The undiscoverable setting allows you to continue using Bluetooth products like headsets, but means that your phone is not visible to others.

Malicious soft wares like Worms, Spywares and Trojans

Worms may disturb the phone network by spreading from one mobile to other mobile through Bluetooth transfer, Infrared transfer or through MMS attachments. Spyware that has entered into the mobile phone through Bluetooth may transfer the personal information to the outside network. The Trojan which got installed along with the game application in the mobile may send SMS messages to expansible members and may increase the phone bill.

Reject all the unexpected pairing requests for Bluetooth devices.

Bluejacking

Bluejacking is sending nameless, unwanted messages to other users with Bluetooth enabled mobile phones or laptops. Bluejacking depends on the capability of Bluetooth phones to detect and contact another Bluetooth enabled device . The Bluejacker uses a feature originally proposed for exchanging contact details or electronic business cards. He or she adds a new entry in the phone's address book, types in a

message, and chooses to send it via Bluetooth. The phone searches for other Bluetooth phones and, if it finds one, sends the message. Despite its name, Bluejacking is essentially harmless. The Bluejacker does not steal personal information or take control of your phone. Bluejacking can be a problem if it is used to send obscene or threatening messages or images, or to send advertising. If you want to avoid such messages, you can turn off Bluetooth, or set it to "undiscoverable".

Delete the MMS (Multimedia Messaging Service)message received from an unknown user without opening it.

Guidelines for securing mobile devices

- Be careful while downloading applications through Bluetooth or as MMS attachments.They may contain some harmful software, which will affect the mobile phone.
- Keep the Bluetooth connection in an invisible mode, unless you need some user to access your mobile phone or laptops. If an unknown user tries to access the mobile phone or laptop through blue tooth, move away from the coverage area of blue tooth so that it automatically gets disconnected.
- Avoid downloading the content into mobile phone or laptop from an untrusted source.
- Read the mobile phone's operating instructions carefully mainly regarding the security settings, pin code settings, Bluetooth settings, infrared settings and procedure to download an application. This will help in making your mobile phone secure from malicious programs.
- Activate the pin code request for mobile phone access. Choose a pin, which is unpredictable and which is easy to remember for you.
- Use the call barring and restriction services provided by operators, to prevent the applications that are not used by you or by your family members.
- Don't make you mobile phone as a source for your personal data, which is dangerous if it falls in to the hands of strangers. It is advisable not to store important information like credit card and bank cards passwords, etc in a mobile phone.
- Regularly, backup important data in the mobile phone or laptop by following the instructions in the manual.
- Define your own trusted devices that can be connected to mobile phone or laptop through Bluetooth.
- Use free cleansing tools, which are available in the Internet to make your mobile work normally, when ever it is affected by malicious soft wares.

TOP ANDROID SECURITY APPS

360 Mobile Security (Free)

A major player in China, developer Qihu burst onto the scene and claimed the top spot in AV-Test's September 2013 report with a virtually flawless detection rate of 99.9 percent, the highest of any of the security apps tested. In the latest March 2014 report it achieved a detection rate of 100 percent. The focus with 360 Mobile Security is firmly on detecting and nullifying threats to your system. It has a very streamlined, elegant design. It's extremely lightweight, and it's completely free.

A standard real-time scan will safeguard your device from malware, spyware, and the threat of infection. It's also capable of detecting and fixing system vulnerabilities and cleaning up idle background apps to help your phone run more efficiently. There's a privacy advisor and a tool to clear your usage history.

This app eschews a laundry list of extras in favor of a light touch. The only additional features you'll find are call blocking options, some shortcut toggles, and safe browsing protection. There's no anti-theft component or backup option.

For a good blend of usability and strong protection, you should think about 360 Mobile Security. If you're more concerned about smooth performance than extra features, it is bound to appeal

Avast Mobile Security

As a genuinely free app for the Android platform, Avast! Mobile Security is offering an impressive range of tools. It has antivirus protection, it scans your apps to provide details on what they are doing, and it has a Web shield that scans URLs for malware.

There are various additional tools in the package and the best of the bunch is the anti-theft component. The app is actually based on an old app called Theft Aware which Avast acquired.

The anti-theft feature is hidden and allows you to remote control your smartphone using SMS. So if you lose your phone, you can remotely lock it, locate it, or wipe it. You can make it play a siren sound, lock down the SIM card, and prevent USB debugging as well. It's a comprehensive solution for theft protection.

If you have a rooted device then there's also a firewall that allows you to control network traffic. You can block access to Wi-Fi or the network for specific apps which is handy for security and potentially saving on battery juice as well.

According to the latest AV-Test report of 31 popular Android security apps, Avast is a solid option with an overall detection rate of 99.9 percent. Although it is not top of the charts in terms of malware detection, the extra functionality (including the anti-theft tools and a firewall for rooted devices) still make it worth considering. It has a light footprint with no discernible drain on battery life and no impact on general performance. It also returned no false positives.

The fact this app is completely free, has a wide range of features, and offers protection for rooted devices, makes it a strong contender. If you're looking for a security solution for your Android smartphone, and your primary concern is malware and safe browsing, then this could be the right app for you. Avast Marketing Director, Milos Korenko, has assured us that "There might be a paid version in the future but that won't have an impact on the free version. It will continue to be available and loaded with features."

ESET Mobile Security & Antivirus

This is a new entry for our top five and it deserves its place with a 100 percen detection rate in the latest AV-Test report and an easy-to-use interface. The basic app is completely free and it provides real-time scanning of apps to detect malware and potentially dodgy apps trying to send texts or make premium rate calls.

The free version also includes a suite of anti-theft tools. You can remotely locate and lock your smartphone or tablet, and you can prevent anyone from uninstalling apps by using password protection.

If you want remote wipe or SIM guard capabilities then you have to spring for the premium version at $20 per year, but it also delivers anti-phishing protection, an app audit feature, device monitoring for unwarranted use of data, and advanced call blocking.

Avira Antivirus Security

With a 100 percent detection rate and no false positives, you can trust the free version of Avira to keep your Android smartphone or tablet safe. It has a light footprint in terms of performance and a sleek, minimalist design that fits in well with the Android platform.

Avira allows you to scan apps for potential trouble and it scans new apps or updates automatically. There's also the usual batch of anti-theft tools, to help you find your device remotely, lock it, wipe it, or trigger an alarm. There's an additional tool that claims to be able to tell you whether your email account has been hacked and tell you what action to take if it has. A decent range of blacklisting options rounds off this app, so you can block problem callers or nuisance spam.

There is a premium version that adds anti-phishing, more regular updates, and better support, but the free version covers enough bases for most people.

AVL

Some of you are probably just looking for malware protection that's as barebones as possible. If you don't want anti-theft tools, or identity protection, or any of the other possibly superfluous features that come in many security apps then AVL will suit you.

This app scored a 100 percent detection rate with no false positives and AV-Test found performance was good with no undue impact on speed or battery life. AVL can scan a variety of file formats beyond APKs and it's designed to be fast and efficient.

Android Security Evaluation Framework: ASEF

Have you ever looked at your Android applications and wondered if they are watching you?

Whether it's a bandwidth-hogging app, aggressive adware or even malware, it would be interesting to know if they are doing more than what they are supposed to and if your personal information is exposed. Is there really a way to automatically evaluate all your apps, even hundreds of them, to harvest their behavioral data, analyze their run pattern, and at the same time provide an interface to facilitate a vast majority of evolving security tests with most practical solutions?

To answer these questions, I created the Android Security Evaluation Framework (ASEF) to perform this analysis while alerting you about other possible issues. Use it to become aware of unusual activities of your apps, expose vulnerable components and help narrow down suspicious apps for further manual research.

ASEF Framework

The framework takes a set of apps, either pre-installed on a device or as individual APK files, and migrates them to the test suite which runs through test cycles on a pre-configured Android Virtual Device (AVD). The technique is to simulate the entire lifecycle of an Android app on an Android device (virtual/physical) and collect data while triggering behavioral aspects of it. In simple words, download an Android app from an internet, install it on an Android device, launch it and mess with it (e.g clicking different buttons, scrolling up/down, swipe etc..) While doing so, collect an activity log using adb (Android debug bridge utility which is available as a part of an Android SDK) and network traffic using tcpdump (a widely used packet capturing tool)

Behavioral Analysis

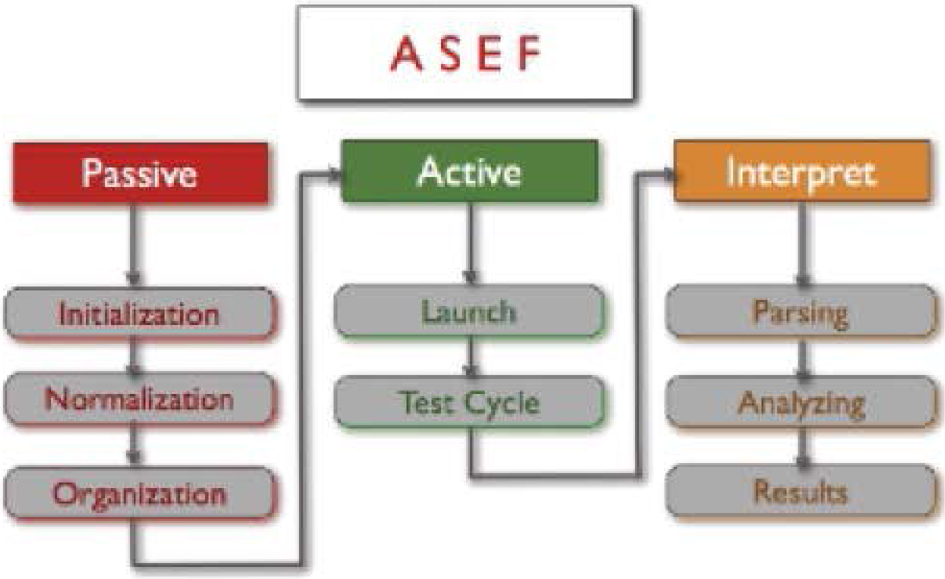
During such a simple yet thorough approach of performing a behavioral analysis for various apps, interesting results were found about apps leaking sensitive information like IMEI, IMSI, SIM card or a phone number of a device. Some malicious apps might just send this data in clear text over the Internet and are much easier to be caught by analyzing collected behavioral data. However some malicious apps can be sophisticated enough to detect the default settings of a virtual Android device and might behave differently in such settings. In order to overcome such limitations, a virtual device can be custom built by fine-tuning the kernel and also altering default settings to emulate a real device or it can be replaced by a physical Android device.

Open Source

ASEF is now available as open source at http://code.google.com/p/asef/. With it, users can gain access to security aspects of android apps by using this tool with its default settings. An advanced user can fine-tune this, expand upon this idea by easily integrating more test scenarios, or even find patterns out of the data it already collects. ASEF will provide automated application testing and facilitate a plug and play kind of environment to keep up with the dynamic field of Android Security.

At Black Hat

If you are at Black Hat USA 2012 and/or B-Sides Las Vegas, come to my talk where I discuss the test cycles and results so far. And if not, read the A S E F Getting Started guide for an architectural overview of the framework and more details on the motivations behind the project.



mKavach

Mobile Device Security Solution

Standalone Features

- Remote Wipe/Lock
  # SMS based
- Track Lost/Stolen Device Location
  # SMS based
- Secure Backup & Restore
  # Local on SDCard
- SIM Binding
- Secure Storage on Mobile Device
  # Selective Encryption
- Protection against JavaScript Malwares
  # JS Guard Browser Plugin
- Application Management
  # Secure List, White List and Black List
- CAll/SMS Filter
  # Blocking unwanted calls and SMS
  # Secure storage of SMS
- Password protected Bluetooth & Wi-Fi Access

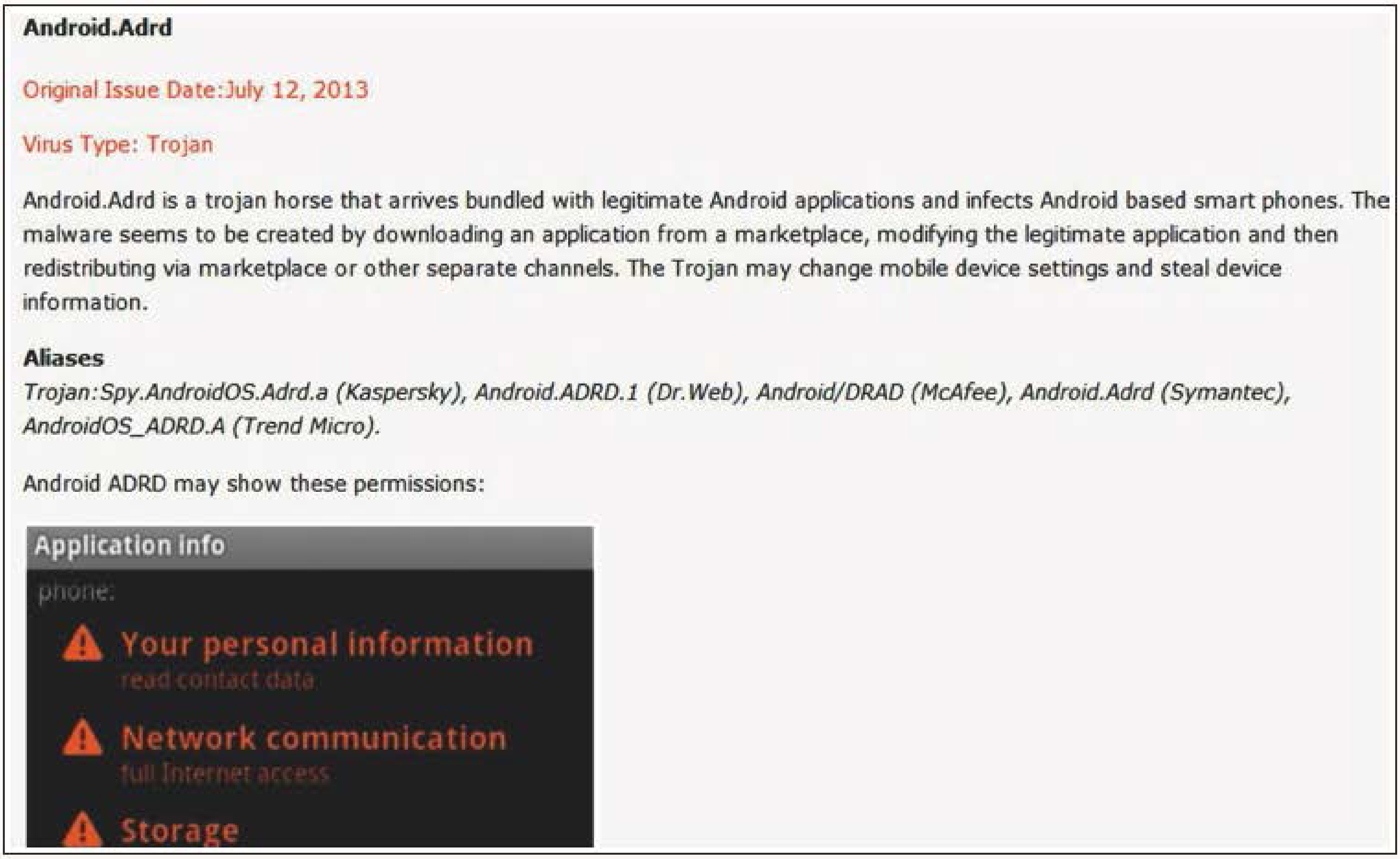
Supported Mobile Platforms for Standalone & Enterprise
Android 2.3 (Gingerbread) to 4.4 (Kitkat)
Supported Mobile Platforms for Enterprise-Pro
Android 4.3 (Jelly Bean to 4.4 (KitKat)

Enterprise Features

- Remote Wipe/Lock
  # Web and SMS based
- Track Lost/Stolen Device Location
  # Web and SMS based
- Secure Backup & Restore
  # Local and Remote
- SIM Binding
- Secure Storage on Mobile Device
  # Selective Encryption
- Protection against JavaScript Malwares
  # JS Guard Browser Plugin
- Application Management
  # Secure List, White List and Black List
- CAll/SMS Filter
  # Blocking unwanted calls and SMS
  # Secure storage of SMS
- Password protected Bluetooth & Wi-Fi Access
- Dual Authentication : User and Device
  # IMEI, IMSI, OS version
- Web-based Management Console
- Enterprise Application Catalog

InfoSec Cartoon

Never download/forward any files received from from strangers.



Android.Adrd

Original Issue Date:July 12, 2013

Virus Type: Trojan

Android.Adrd is a trojan horse that arrives bundled with legitimate Android applications and infects Android based smart phones. The malware seems to be created by downloading an application from a marketplace, modifying the legitimate application and then redistributing via marketplace or other separate channels. The Trojan may change mobile device settings and steal device information.

Aliases
Trojan:Spy.AndroidOS.Adrd.a (Kaspersky), Android.ADRD.1 (Dr.Web), Android/DRAD (McAfee), Android.Adrd (Symantec), AndroidOS_ADRD.A (Trend Micro).

Android ADRD may show these permissions:

Application info

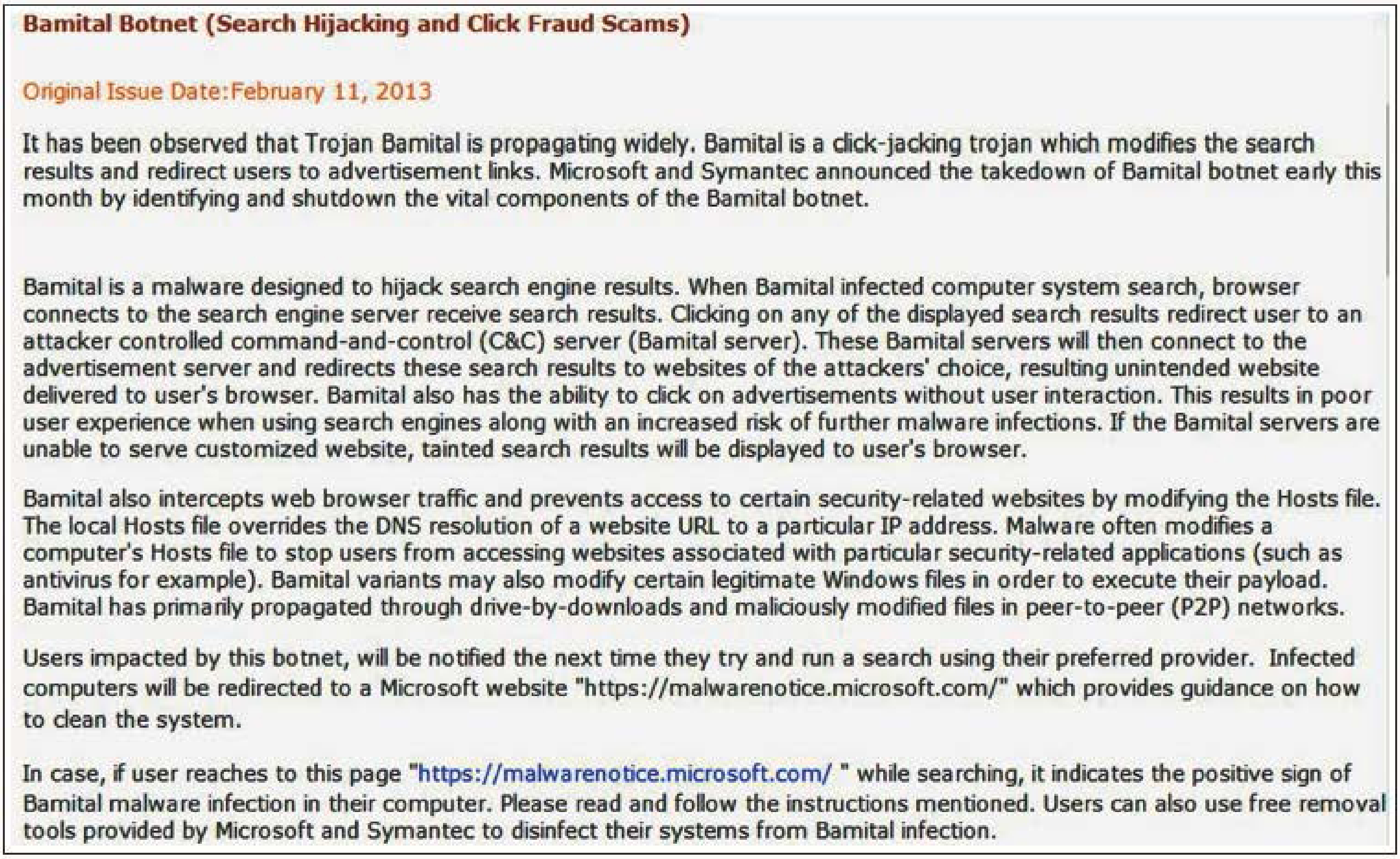
phone:

⚠ Your personal information
read contact data

⚠ Network communication
full Internet access

⚠ Storage

For more detials visit : ***www.cert-in.org.in***



Bamital Botnet (Search Hijacking and Click Fraud Scams)

Original Issue Date:February 11, 2013

It has been observed that Trojan Bamital is propagating widely. Bamital is a click-jacking trojan which modifies the search results and redirect users to advertisement links. Microsoft and Symantec announced the takedown of Bamital botnet early this month by identifying and shutdown the vital components of the Bamital botnet.

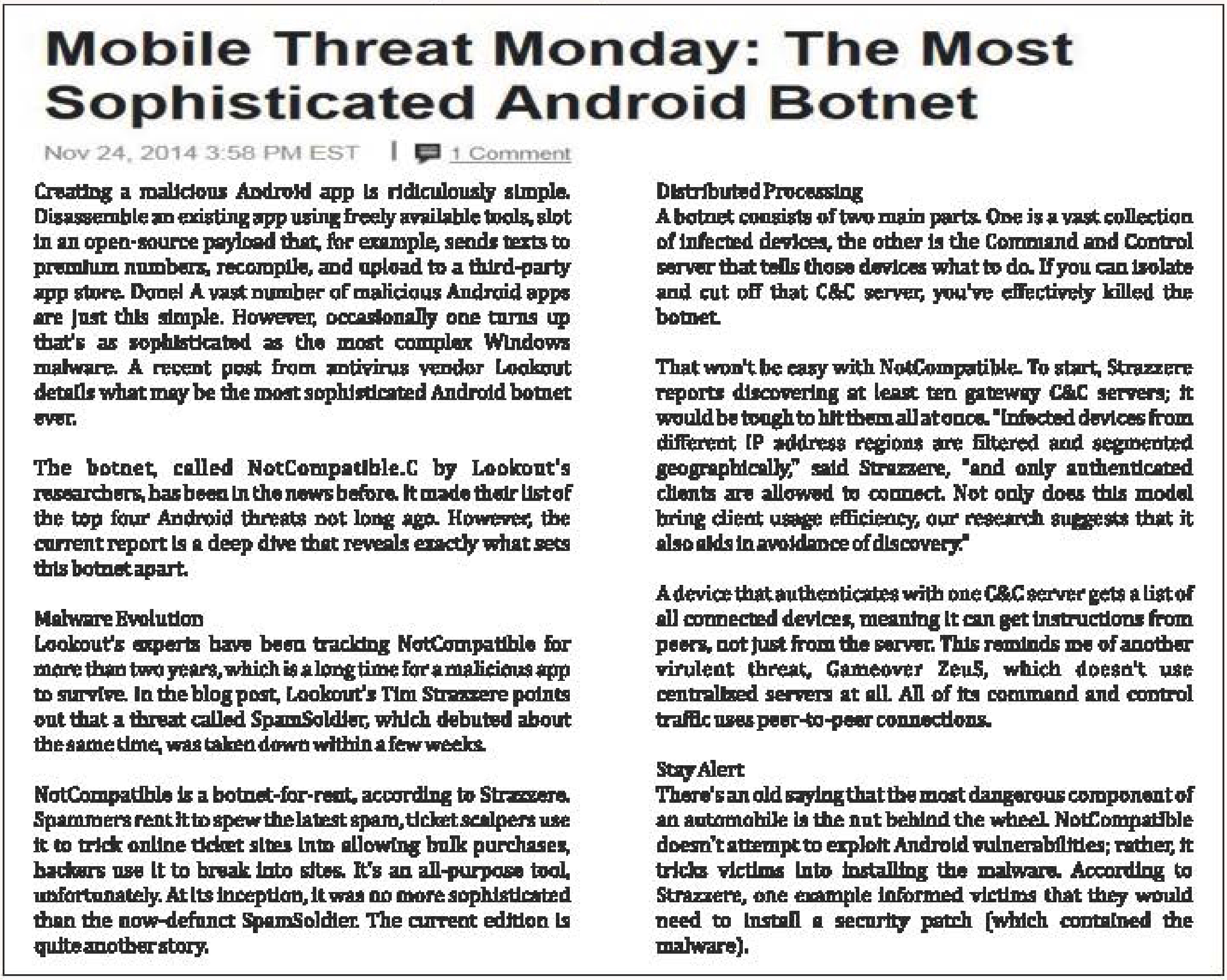
Bamital is a malware designed to hijack search engine results. When Bamital infected computer system search, browser connects to the search engine server receive search results. Clicking on any of the displayed search results redirect user to an attacker controlled command-and-control (C&C) server (Bamital server). These Bamital servers will then connect to the advertisement server and redirects these search results to websites of the attackers' choice, resulting unintended website delivered to user's browser. Bamital also has the ability to click on advertisements without user interaction. This results in poor user experience when using search engines along with an increased risk of further malware infections. If the Bamital servers are unable to serve customized website, tainted search results will be displayed to user's browser.

Bamital also intercepts web browser traffic and prevents access to certain security-related websites by modifying the Hosts file. The local Hosts file overrides the DNS resolution of a website URL to a particular IP address. Malware often modifies a computer's Hosts file to stop users from accessing websites associated with particular security-related applications (such as antivirus for example). Bamital variants may also modify certain legitimate Windows files in order to execute their payload. Bamital has primarily propagated through drive-by-downloads and maliciously modified files in peer-to-peer (P2P) networks.

Users impacted by this botnet, will be notified the next time they try and run a search using their preferred provider. Infected computers will be redirected to a Microsoft website "https://malwarenotice.microsoft.com/" which provides guidance on how to clean the system.

In case, if user reaches to this page "https://malwarenotice.microsoft.com/ " while searching, it indicates the positive sign of Bamital malware infection in their computer. Please read and follow the instructions mentioned. Users can also use free removal tools provided by Microsoft and Symantec to disinfect their systems from Bamital infection.

http://securitywatch.pcmag.com/malware/329827-mobile-threat-monday-the-most-sophisticated-android-botnet



Mobile Threat Monday: The Most Sophisticated Android Botnet

Nov 24, 2014 3:58 PM EST | 1 Comment

Creating a malicious Android app is ridiculously simple. Disassemble an existing app using freely available tools, slot in an open-source payload that, for example, sends texts to premium numbers, recompile, and upload to a third-party app store. Done! A vast number of malicious Android apps are just this simple. However, occasionally one turns up that's as sophisticated as the most complex Windows malware. A recent post from antivirus vendor Lookout details what may be the most sophisticated Android botnet ever.

The botnet, called NotCompatible.C by Lookout's researchers, has been in the news before. It made their list of the top four Android threats not long ago. However, the current report is a deep dive that reveals exactly what sets this botnet apart.

Malware Evolution

Lookout's experts have been tracking NotCompatible for more than two years, which is a long time for a malicious app to survive. In the blog post, Lookout's Tim Strazzere points out that a threat called SpamSoldier, which debuted about the same time, was taken down within a few weeks.

NotCompatible is a botnet-for-rent, according to Strazzere. Spammers rent it to spew the latest spam, ticket scalpers use it to trick online ticket sites into allowing bulk purchases, hackers use it to break into sites. It's an all-purpose tool, unfortunately. At its inception, it was no more sophisticated than the now-defunct SpamSoldier. The current edition is quite another story.

Distributed Processing

A botnet consists of two main parts. One is a vast collection of infected devices, the other is the Command and Control server that tells those devices what to do. If you can isolate and cut off that C&C server, you've effectively killed the botnet.

That won't be easy with NotCompatible. To start, Strazzere reports discovering at least ten gateway C&C servers; it would be tough to hit them all at once. "Infected devices from different IP address regions are filtered and segmented geographically," said Strazzere, "and only authenticated clients are allowed to connect. Not only does this model bring client usage efficiency, our research suggests that it also aids in avoidance of discovery."

A device that authenticates with one C&C server gets a list of all connected devices, meaning it can get instructions from peers, not just from the server. This reminds me of another virulent threat, Gameover ZeuS, which doesn't use centralized servers at all. All of its command and control traffic uses peer-to-peer connections.

Stay Alert

There's an old saying that the most dangerous component of an automobile is the nut behind the wheel. NotCompatible doesn't attempt to exploit Android vulnerabilities; rather, it tricks victims into installing the malware. According to Strazzere, one example informed victims that they would need to install a security patch (which contained the malware).

The members of the Nigerian gang who were arrested by the Cyberabad police cover their faces.

Nigerian gang cons bizman over BMW car sale, busted

DC CORRESPONDENT
HYDERABAD, NOV. 27

A Mumbai-based, five-member gang run by Nigerian nationals fleeced a businessman from LB Nagar by promising to sell him a BMW car imported from the US. The fraudsters, claiming to be US consulate officials, put up a car sale advertisement on *quikr.com* and convinced the victim, Sheik Jeelani Basha, by sending him customs receipts, etc. A Mumbai-based woman and a West Godavari native, a part of the gang, posed as Mumbai custom officials and took lakhs of rupees from him.

Cybercrime sleuths of Cyberabad have busted the gang in Mumbai, which is suspected to be involved in a Nigerian lottery scam, RBI scam and other fraudulent activities.

The accused have been identified as Talla Mojesh alias Venkat, a native of West Godavari and currently settled in Mumbai; Pascal Emmanuel alias George Frideric, 34; Paul Osemweigie, 43; Oluikpe Sunday Onyegbula, 29; and Sajida Abdul Hamid, a Mumbai native.

Cyberabad Additional DCP of Crime B. Srinivas Reddy revealed that the fraudsters had looted ₹18.63 lakh as car price, demurrage charges, other customs clearance charges, etc. The woman member in the gang, Sajida, pretending as a customs official, contacted the victim frequently over phone and made him deposit money in various bank accounts.

The businessman, Mr Shaik Jeelani Basha, who runs a building and interior designing firm, jumped at the opportunity of buying the car priced at ₹14 lakh on the online platform, as the rate appeared lower. "After Mr Basha responded to the online ad, Emmanuel contacted him, introducing himself as a Dr George Frideric, working with the US consulate and wanting to sell his car as he was leaving for the US soon. After clinching the deal, he asked the victim to deposit ₹1.5 lakh in a bank account as demurrage charges and sent some fake receipts in return. As the victim got convinced, other gang members, pretending to be customs officials, made him deposit more money in various accounts, citing different charges," said Mr Srinivas Reddy.

Basha realised he was being duped as they asked more money from him. He later approached the police and lodged a complaint

http://epaper.deccanchronicle.com/epaper_main.aspx?id=HYD

For more details visit

www.infosecawareness.in

Supported by

Department of Electronics & Information Technology
Government of India

Executed by

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
Nalanda Building, Road No : 1, Shivbagh, Near Satyam Theatre, Ameerpet, Hyderabad - 500016
E-mail : isea@cdac.in