

**Quick Heal**

*Security Simplified*

# Quick Heal Security Threat Report 2014



[www.quickheal.com](http://www.quickheal.com)



# TABLE OF CONTENTS



01	<b>Foreword</b>
02	<b>Introduction: Malware Mutates and gets Versatile</b>
03	<b>Windows: Still Stealing the Limelight</b>
04	Top 20 Malware
12	Botnets: More Resilient and Dangerous
15	Web-based Malware Deployments: Watering Hole vs. Phishing
19	Application Vulnerabilities
22	<b>Android: Growth of Smarter and Tougher to Detect Attacks</b>
23	Top 20 Android Malware
30	Giving the Farm Away to the Hackers
32	Mobile Malware Authors Quickly Adapt to Mobile-friendly Ecosystems
33	App Stores – Still a Loophole Here and There
33	User Data Leakages
34	Android Security - Some More Facts
36	<b>Trends to Watch Out for In 2014</b>
38	<b>Conclusion</b>



*2013 saw constant innovation from malware authors. While Internet becomes ubiquitous with its need in business, and private life, cybercrime and espionage adapt to new methods.*

*The growing acceptance of the "Internet of things" has created new attack platforms and critical infrastructure vulnerabilities stand out like a sore thumb. The threat scenario doesn't leave us with the assumption that security could be a choice, it has become essential.*

Cybercriminals have continued to develop new and innovative ways to bilk innocent victims and state sponsored cybercrime continues to create spying networks and steal information.

The way information technology is used in business and in personal life has brought about tremendous changes in the threat landscape. BYOD (Bring Your Own Device) and use of cloud services has data being transferred beyond the traditional firewall. Companies big and small need to evaluate their security and that of the vendor or associated companies.

Zero-day attacks continue to grow and multiply as older non-patched vulnerabilities compromise the systems. Malware authors are now focussed on stealth attacks that elude identification, and rely heavily on cryptography. Advanced persistent threats (APTs) is one of the most malicious forms of stealth attacks. While the attack focuses on gathering sensitive information and data, its target can vary from individuals to governments. Increasingly Small and Medium businesses (SMBs) are on the forefront of these attacks as they have fewer resources to fight back. In these cases, often an attack on an SMB is used as a catalyst to trigger an even bigger attack.

The increasing dependency on mobile devices has given a new lease to the criminals who now design attacks for the most widely used platforms such as the Android. With mobile devices it's always the openness of the platform, and multiple distribution methods available to malicious applications that appeals to the malware authors.

The popularity of social networks has given malware authors new ways to steal personal information and infect the devices with malware.

2013 saw a new version of ransomware called Cryptolocker. While ransomware is almost a decade old, Cryptolocker has managed to up the game by using resilient encryption that makes the victim's file inaccessible and extort money.

Today's attacks are mostly a combination of complex attacks and spread rapidly. In such a case, depending only on an anti-virus is grossly inadequate. For example, a counterattack for APTs is a complex task, and requires a well-coordinated effort of defence technologies at different levels. Awareness should be created on all levels. Security must be considered from the very beginning and should not be the last resort.

Botnets have become more resilient and disguised. While users have stopped responding to a fake antivirus alert or scams, more and more botnets are dropping ransomware instead.

Sincerely,



Sanjay Katkar

Co-Founder & CTO, Quick Heal Technologies

# Malware Mutates and gets Versatile

Malware has come a long way from the first Internet worm. It is now being used by both Governments and black hat hackers for stealing sensitive information whether be it personal, financial, or business related.

Since the widespread use of Internet, malware has been specially designed for profit. Of late, cybercriminals have become more adept at obscure attacks that rely heavily on cryptography basing their attack methods on knowledge picked up from the experiences of their predecessors.

Unfortunately, the malware proliferation doesn't stop at that. The catachresis of malware is being carried out by both state and non-state players where the objectives vary from

monetization to creation of espionage networks and stealing of information.

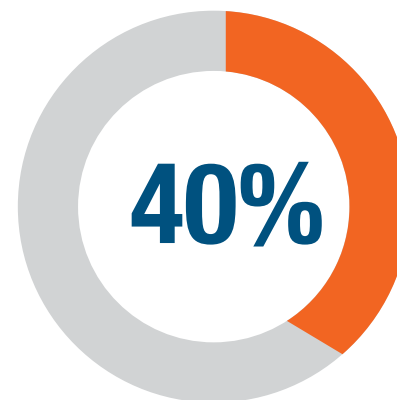
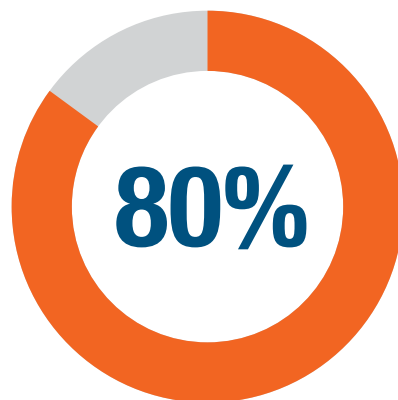
As the use of smart mobile devices and the "Internet of Things" grows, so do the attacks that flock all platforms and spaces that have a good audience.

2013 also witnessed a new version of ransomware named as CryptoLocker. The modus operandi of this revamped version uses strong encryption to make the victim's files inaccessible and hold them to a ransom.

The Threat Research and Response Team at our Research and Development Lab reported an 80 percent increase in the attacks to Windows platforms. A whopping 800 percent increase of malware samples received was reported for the Android platform.

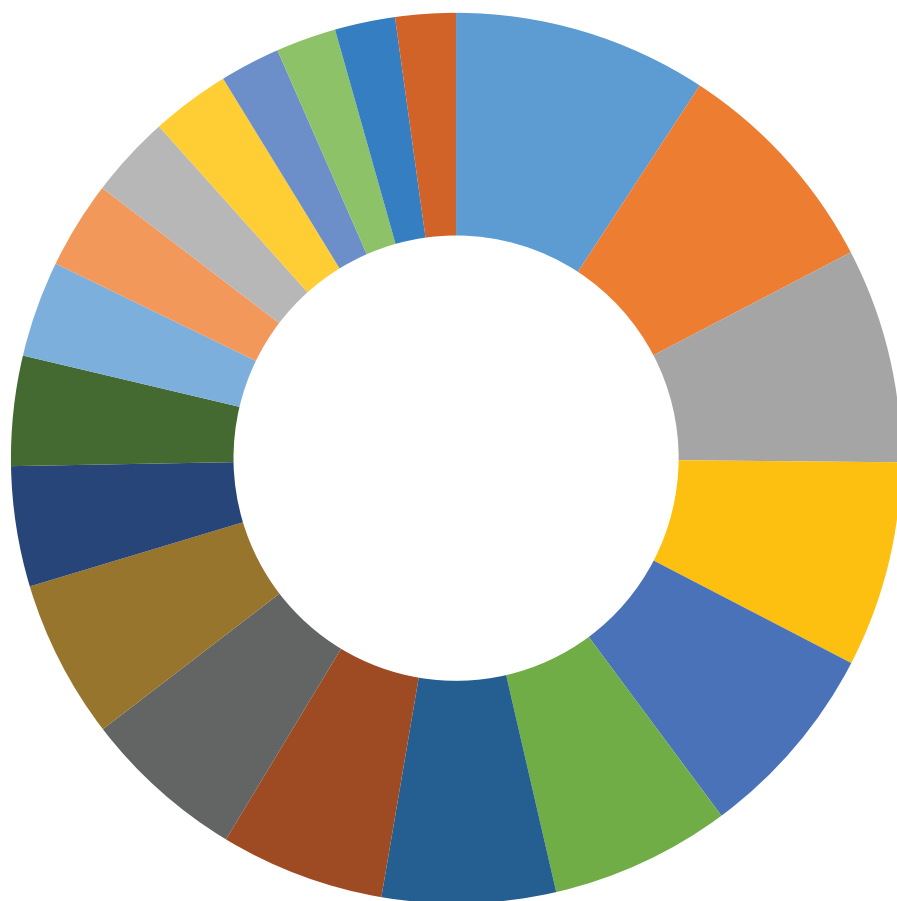
But seen in the perspective of the multitude of "zero-day" attacks that may crop up once the Windows support for older OS like XP and Office 2003 ends, these figures become almost instantly diminutive.

While malware mutations and complexities grow, our progressive researchers work towards creating new techniques that address and neutralize. Whether you are a valued end user, an Enterprise or a Government institution, our commitment to provide solutions that are effective and simple to use, stands unabated.

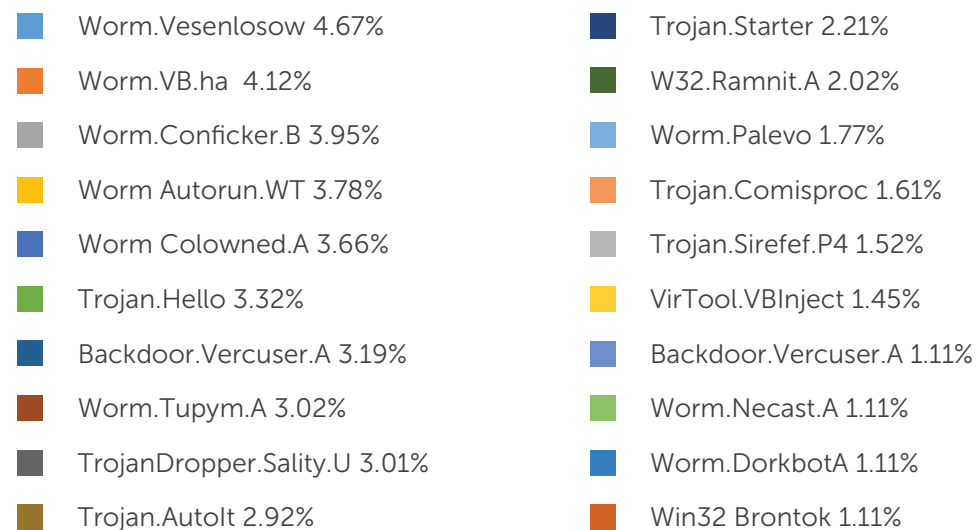


## Still Stealing the Limelight

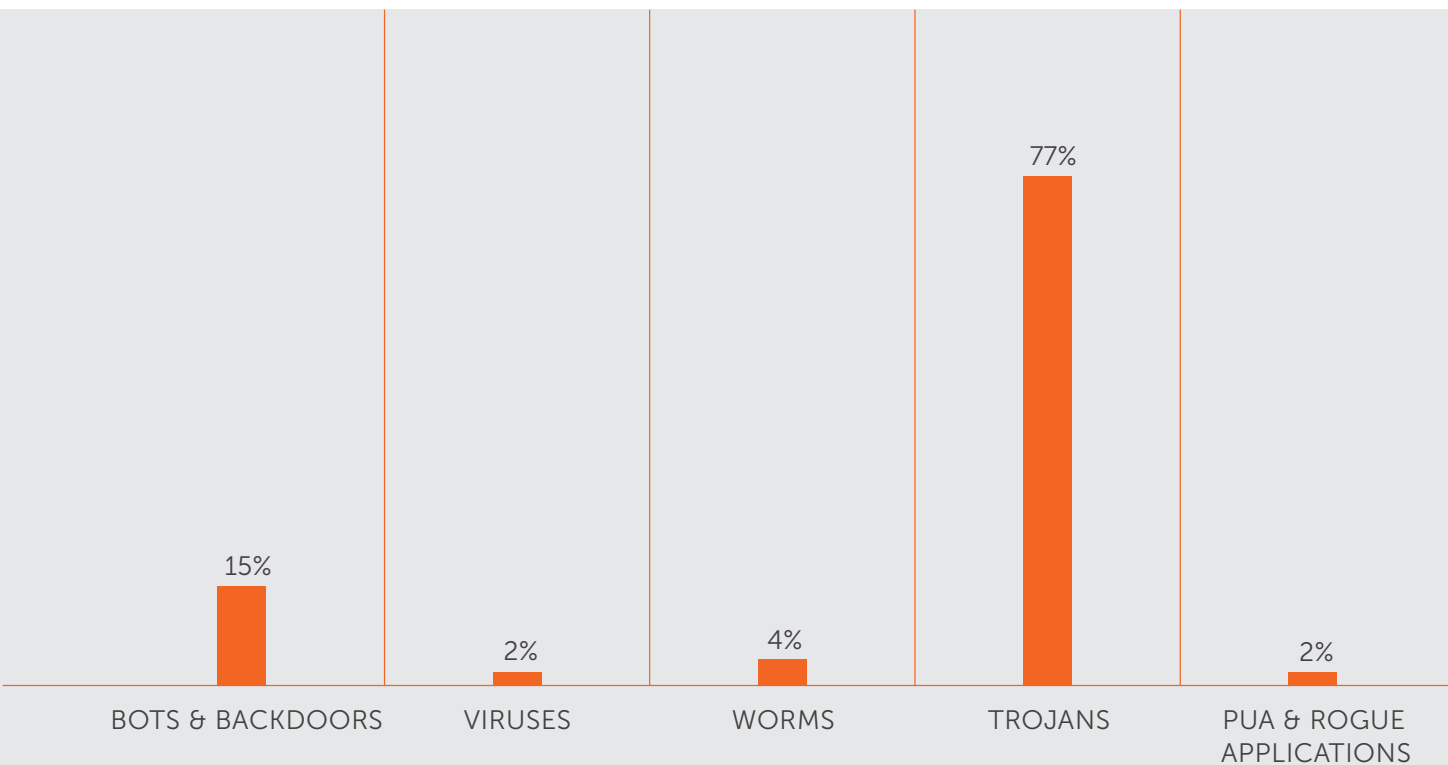
2013 Windows malware saw a rise of 80% in samples that were received at the Quick Heal Research and Development Lab. As compared to 2012, there has been 40 percent rise in new and unique malware.



## Percentage of Detection



While Trojans grabbed the major share of the pie at 77 percent of reported detections, Bots and Backdoors stole the next chunk at 15%.



The figures clearly indicate that Botnets have grown in size and are seeking new targets. Botmasters are now exploring more flexibility in spreading DDOS (Distributed Denial-Of-Service) attacks. One of the tactics being used is the integration of multiple backup forms of command and control.

The top 20 malware as detected by our Research and Development lab have been highlighted below:

## 01. **Worm.Vesenlosow.AJ7**

### What is it?

- It is a family of worms. It uses the icons of genuine tools such as Freegate tool, Suduko solver, and UltraSurf.
- It spreads via removable drives.
- It may also spread by infecting files on a network file system or a file system that is shared by another computer.

### What does it do?

It collects information about the infected computer without the user's knowledge.

## 02. **Worm.VB.ha**

### What is it?

It is a family of worms that spreads by copying itself to removable drives. It copies itself as forever.exe on the root of all accessible drives.

### What does it do?

It modifies the infected computer's host's file and downloads files which have hidden attributes.

## 03. **Win32.Worm.Conficker.B.3**

### What is it?

It is a family of worms that spreads by infecting computers on a network, removable drives, and those with weak passwords.

### What does it do?

A computer that gets infected by Conficker, might not be able to connect to websites related to security applications and services that can help remove it. The worm can also disable important system services and security products.

## 04. **Worm Autorun.WT**

### What is it?

It is a family of worms spreading via removable and network drives.

### What does it do?

After infection, the worm writes an Autorun configuration file named "autorun.inf". When the drive is accessed from a computer supporting the Autorun feature, the worm is launched automatically.

It also modifies registry data to block the viewing of files with hidden and system file attributes, if the option is enabled in Windows Explorer.



## 05. **Worm Colowned.A**

### What is it?

This family is classified as a backdoor Trojan.

### What does it do?

- It allows attackers to remotely access an infected system.
- Systems infected by this worm can be used to launch distributed denial of service (DDoS) attacks.
- It may be used to install additional Trojan malware or other forms of malicious software.
- It might also open ports on the affected system and thus potentially lead to further attacks by other hackers.

## 06. **Trojan.Hello.A1**

### What is it?

It is classified as an MSN-Trojan.

### What does it do?

- It is specifically built to target the MSN messenger and steal confidential user data.
- It can easily record user's keystrokes and steal their MSN password. Thereafter, the Trojan sends the stolen data to the attacker.

## 07. **Backdoor.Vercuser.A**

### What is it?

It is a backdoor Trojan.

### What does it do?

- Once it infects the targeted system, it redirects Google and Yahoo Searches.
- The Trojan changes the desktop background image, and browser homepage settings.
- It slows down infected computers significantly, besides displaying unwanted popup ads.
- The malware can also change the system's registry settings and other important windows system files.
- Backdoor.Vercuser.A infections can steal data such as passwords, credit card, bank account information, etc.
- The infection can display fake malware infection and scare the victim into buying software to remove the infection.

## 08. **Worm.Tupym.A5**

### What is it?

It is a family of worms.

### What does it do?

It creates a scheduled Windows task that runs the worm at specific time every day. It attempts to copy itself to all removable drives and available networks.

## 09. TrojanDropper.Sality.U

### What is it?

It is a Trojan horse.

### What does it do?

- It is designed to install and launch other programs on the infected machine without the user's knowledge.
- The program itself is a Windows PE DLL file. It is written in C++. Once launched, the Trojan creates a unique identifier named "op1mutx9" in order to flag its presence in the system.

## 10. Trojan.AutoIt.gen

### What is it?

It is a Trojan horse.

### What does it do?

- It executes additional actions without the user's knowledge or permission.
- AutoIt Trojans are typically distributed as files attached to fake Instant Messenger (IM) messages, or fake e-mail messages.
- Variants in the Autoit family attempt to download and install other malware on the compromised system (Trojan-Downloader Autoit).
- Most variants also try to change the startup and default search pages for the web browser (typically, Internet Explorer).

## 11. Trojan.Starter.yy4

### What is it?

It is a Trojan horse.

### What does it do?

- The Trojan creates an unauthorized user account on the compromised system and adds that account to the administrator group as a "Remote Service Account".
- It drops a batch file that does the following:
- Stops r\_server service (Remote administrator server).
- Launches svchost.exe (note that, this is a different file from the legitimate Microsoft svchost.exe).

## 12. W32.Ramnit.A

### What is it?

It is a virus. It spreads by exploiting vulnerability in the operating system of the targeted machine.

### What does it do?

- The Windows Shell allows local users or remote attackers to execute arbitrary code via a crafted \*.lnk, \*.pif shortcut file when its icon is displayed. No further user interaction is required to execute arbitrary code.
- The virus searches local drives for files with certain file extensions, and copies itself in certain locations. Certain registries are created which allows the virus to be executed every time the system starts. The virus creates and runs a new thread with its own program code within the svchost.exe process.

## 13. Worm.Palevo

### What is it?

- WORM\_PALEVO is the component of the Mariposa botnet.
- Typical of a worm, PALEVO malware are commonly spread via removal drives.
- The worm may be instructed to spread via MSN Messenger and other specific P2P applications by attackers who control botnets' command-and-control (C&C) servers

### What does it do?

- The PALEVO malware family is basically a downloader. However, it can be instructed to perform other malicious activities such as stealing login credentials, online banking information, including corporate and personal data.
- It can be used to launch distributed denial-of-service (DDoS) attacks.
- The malware connects to specific sites to send and receive commands from C&C servers that are under the attackers' control. Attackers can instruct the malware to perform the following actions:
  - Downloading files
  - Initiating IM applications
  - Propagating via P2P sites and via removable drives
  - Harvesting passwords from specific Web browsers
  - Performing UDP and TCP flooding
  - Scanning ports
  - Pushing adware to other infected systems

- The malware can steal passwords (for social media sites, banking and ecommerce sites) stored on browsers, particularly IE and Mozilla Firefox.

## 14. Trojan.Comisproc.AZ4

### What is it?

It is a Trojan horse.

### What does it do?

- The Trojan may not come alone but may arrive bundled with additional harmful parasites, which may cause additional damage to the infected system.
- It is powerful enough to be able to insert certain coding into system processes, as well as create its very own registry entries. This way, it can run the moment the infected system boots.

## 15. VirTool.VBInject

### What is it?

It is a malicious file that is written in Visual Basic. Its malicious code is encrypted to evade detection by antivirus software.

### What does it do?

- This malicious program can have virtually any purpose.
- It is used by other malware families to hide from security analysis.

- When this malware is run, its code is decrypted and injected into the current process or may be injected into a clean process. In this way, the resulting code is never written to the disk, in an attempt to avoid detection by security software.

## 16. Worm.Necast.A3

### What is it?

It is a .NET compiled worm. It spreads to all accessible drives of the infected system.

### What does it do?

- The worm can steal sensitive information such as:
  - Stored user names, passwords and URLs (Chrome, Firefox, and Opera).
  - Windows Live, Hotmail, Yahoo accountsno-ip.com domain accounts, FileZilla account details (URLs, port, user names, passwords), and hard disk Serial ID.
- The malware can create registry data in order to run at each Windows startup.
- The malware can modify certain registry entries data that can disable the LUA (Least Privileged User Account), also known as the "administrator in Admin Approval Mode". Once LUA is disabled, all applications in the infected system are run with administrative privileges by default, without the user being prompted for explicit consent. In this way, the malware can cause significant damage to the compromised machine.

## 17. Worm.Dorkbot.A

### What is it?

It belongs to the family of IRC-based worms called Dorkbot. It is spread via

removable drives and instant messaging programs.

### What does it do?

- It downloads malware that targets Skype account which allows it to spread to other contacts by sending a malicious link to the victim's Skype contacts.
- The worm hides in the %TEMP% as a file name such as skype-img-<MM\_DD-YYYY>.exe
- When it runs, it copies itself to the %APPDATA% directory using a randomly generated 16-character file name.
- It modifies certain registry entries to ensure it runs each time the infected machine is started.

## 18. Win32 Brontok

### What is it?

It is a family of mass-mailing e-mail worms. It copies itself to removable drives.

### What does it do?

- The worm uses file names that may be similar to certain Windows system file names. These include csrss.exe, lsass.exe, services.exe, smss.exe, or winlogon.exe.
- In most cases, it uses the Windows 'New folder' icon for the worm files, and by default, its variants hide their executable file extensions. In this way, the malware can pose as a new folder rather than an executable file.
- An unsuspecting user may click the "folder" to view its contents and may inadvertently install the worm on the machine.

### What does it do?

- The worm uses file names that may be similar to certain Windows system file names. These include csrss.exe, lsass.exe, services.exe, smss.exe, or winlogon.exe.
- In most cases, it uses the Windows 'New folder' icon for the worm files, and by default, its variants hide their executable file extensions. In this way, the malware can pose as a new folder rather than an executable file.
- An unsuspecting user may click the "folder" to view its contents and may inadvertently install the worm on the machine.
- To further convince the victim that the worm file is actually a folder, a new Explorer window is also opened when the worm is executed.
- The malware may also attempt to lower the security settings of the infected system.

## 19. Trojan.Sirefef.P4

### What is it?

It is a Trojan horse. It uses stealth technique to hide itself in the compromised computer.

### What does it do?

- Downloads and runs other files in the computer without the user's knowledge.
- Contacts remote hosts.
- Keeps security features of the computer from functioning properly thus lowering down the defense system.
- The Trojan can also modify search results in order to generate money for the attacker.

- Sirefef variants have been observed copying themselves as GoogleUpdate.exe and dropping the file into certain folders on the affected system.

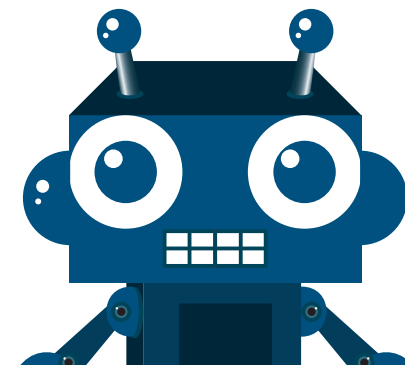
## 20. I-Worm.Kido.ih

### What is it?

It is a family of worms. It spreads to other computers across a network by exploiting a vulnerability in the Windows Server service (SVCHOST.EXE). It may also spread via removable drives and weak administrator passwords.

### What does it do?

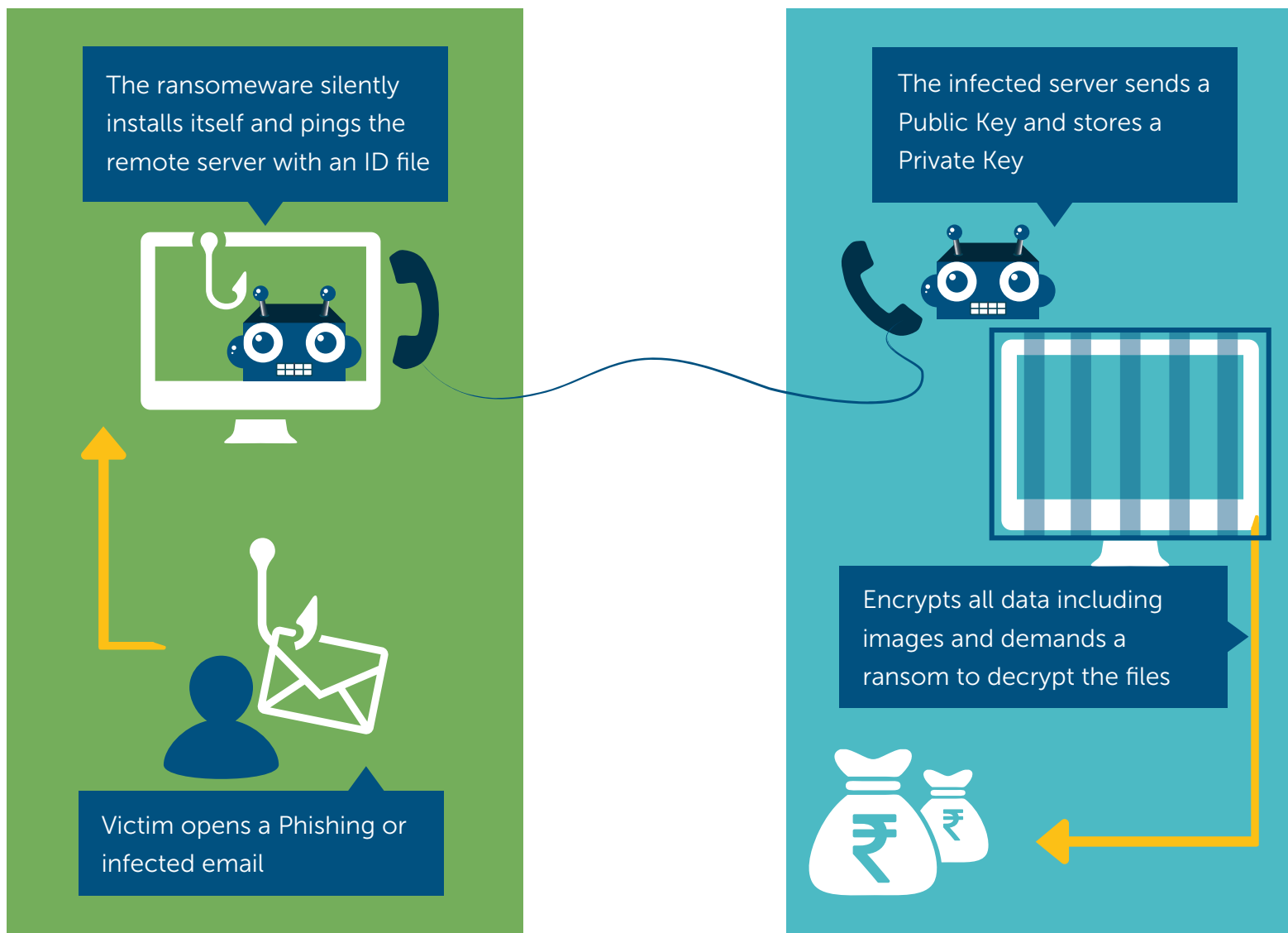
- Once the worm gains entry into the targeted machine, it can allow remote code execution when file sharing is enabled.
- This worm can delete any System Restore points created by the user.
- It can also disable several important system services and security products installed on the compromised machine.



## More Resilient and Dangerous

The most notable botnet incident of 2013 was the birth of the CryptoLocker. While PC users are becoming more and more aware of fake anti-virus and alerts, CryptoLocker took all by surprise. Delivered by botnets and devised to extort money by encrypting files and holding them on ransom, this ransomware adds itself to the list of Windows startup programmes. Once active it tracks down an infected server, uploads an ID file from the infected system and retrieves a public key from that infected server (which stores a matching private key), then encrypts all the data, including image files on the infected system.

# HOW CRYPTOLOCKER WORKS



# Cryptolocker ups its Extortion Game

# Alert: Ransomware are on the loose!

If you already purchased private key using CryptoLocker, than you can download private key and decrypter for FREE.

---

Select any encrypted file and click 'Upload' button.  
The first 1024 bytes of the file will be uploaded to the server for search the associated private key. The search can take up tp 24 hours.

Choose File **No file chosen**

**Upload**

---

IMMEDIATELY AFTER UPLOADING FILE TO THE SERVER, YOU RECEIVE YOUR ORDER NUMBER. YOU CAN USE THIS NUMBER TO CHECK STATUS OF ORDER.

---

OR if you already know your order number, you may enter it into the form below.

**Check Status**

---

This service accessible through the Tor network:  
<http://f2d2v7soksbskekh.onion/>

**CryptoLocker**

## Your personal files are encrypted!

Your important **files encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will **allow** you to decrypt the files, located on a secret server on the Internet; the server **will destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

**To obtain** the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

**Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.**

Private key will be destroyed on  
**9/23/2013  
5:59 PM**

Time left  
**71 : 59 : 07**

**Next >>**



# Web-based Malware Deployments: Watering Hole vs. Phishing

## MALWARE

A new breed of online fraud called “watering hole attack” made its presence felt last year. It is an evolved form of spear-phishing. While spear-phishing is sending malware-infested emails generally targeted towards luring victims into giving away confidential information, a watering hole on the other hand infects an entire website.

A compromised system can give the attacker a freeway to carry out a host of activities, including reading emails, viewing stored data, stealing username and passwords, or installing key loggers.

# PHASES

The attack usually consists of three phases:

1. The attacker collects insight regarding the kind and the websites that the target individual, company or organization visits.
2. One or more of these websites are then infected with malware.
3. Wait and watch till the target visits the infected website – the “watering hole”, their system is scanned for software vulnerabilities (old and/or new) corresponding to the injected exploit. When a vulnerability is found, the exploit drops malware onto it, allowing the attacker to initiate malicious activities. In most cases, the malware might be a remote access Trojan, which can invite other malware to enter the system.

What makes a watering hole attack uniquely successful is the fact that the attacker studies the frequently visited sites. These could be anything from the local weather forecasts to a trusted online store. These attacks are also neatly focussed on “zero-day” vulnerabilities that are yet to get fixes or patches.

These attacks are mostly targeted towards:

- Defence sectors
- Academic sectors
- Government organisations
- Financial services
- Healthcare industry
- Utilities sectors

## A Watering Hole Attack

### STEP 1

Hacker does homework on their intended targets and websites they mostly visit.



### STEP 2

Hacker finds a vulnerable website, and poisons it with an exploit.



### STEP 3

When the victim visits the poisoned site, the exploit infects their system with a malware. This malware gives the hacker unauthorized access to the victim's system.



Some of the notable companies like Facebook, Twitter (the attack compromised 250,000 account credentials), Microsoft, Apple, etc. have faced the brunt of such attacks.

Reportedly, India happens to be the 4th most favorite target of cyber criminals when it comes to phishing attacks.

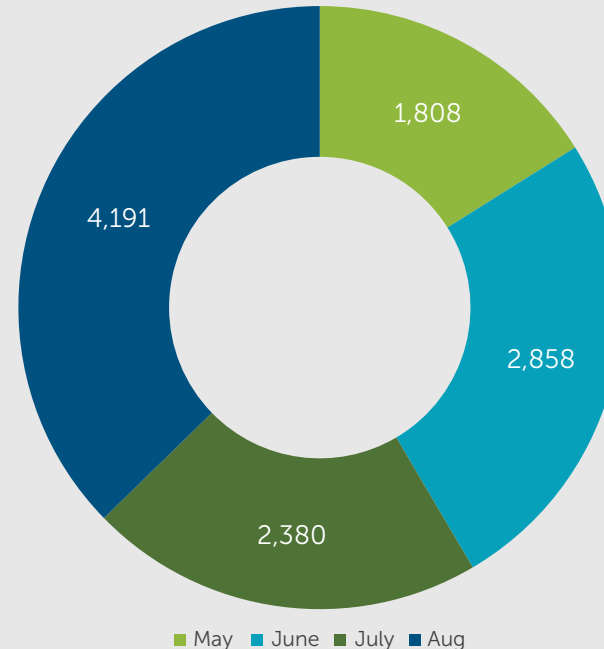
According to Indian Computer Emergency Response Team (CERT-In) number of Indian Websites defaced and hacked in 2013:

- August – 4,191
- July – 2,380
- June – 2,858
- May – 1,808

List of Offenders

Some of the main cyber crooks that India is dealing with presently are:

- SA3D HaCk3D
- h4x0r HuSsY
- SanFour2S
- BD GREY HAT HACKERS
- Suwario
- SpyDy
- hasnain haxor
- CouCouM



## Cyber Crimes against India

Increasing in Leaps and Bounds

### Identity Theft Tariff

Name ..... \$\$  
Address ..... \$\$  
CC No. .... \$\$  
SS No. .... \$\$  
Bank A/C ..... \$\$

Phishing is usually carried out by email hoaxes or instant messaging, and it often points users to enter details at a fake website whose look and feel are almost identical to the legitimate one. These fake websites are designed to make victims enter personal information, passwords, credit card details and bank credentials.

## Your Identity is Online Black Market's Prized Possession

If you thought there is only a black market for stolen mobile phones, drugs, pirated software, etc., then you could be wrong. Online black market is something that is taking root across the world, and one of its most lucrative commodities is your personal identity information.

More advanced forms of Phishing now include counterfeit emails and spoofed links posted on social media sites. If an attacker manages to gain access to a social media account, the phishing emails can then be spread using the victims account. A message that comes from a friend appears to be more reliable and trustworthy, than a message passed on by an absolute stranger.

## Obama's Speech Spreads Malware

In late April, there was a surge in unsolicited emails showing circulating the news "Obama speech to urge 'refocus' on economy". The email contained a link that was designed to take the victim to malware-infected websites.

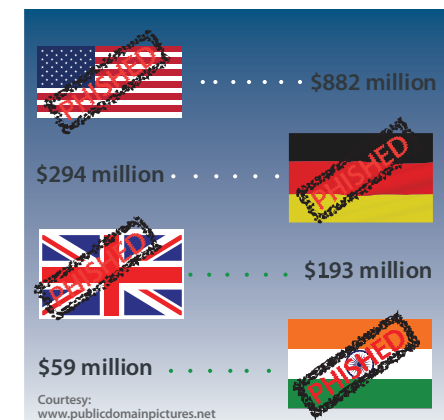


## India – the 4th Most Targeted Nation by Phishers!

In Q3 of 2013 (July – September), about 1,25,212 phishing attacks occurred globally. Out of that, 3% was directed against India. This amounted to a loss of a whopping INR 328 crore (\$53 million). Apparently, the country ranks 4th in the hit list of phishers; according to a report presented by RSA.

## Work from Home Scam

Work from home scams are mostly linked to people who are unemployed and look for jobs that can be carried out from the comforts of home. Such jobs promise attractive salary and purport better work life. With Internet reaching to every nook and corner of the world, scammers do not have to sweat to lure people into such scams.





Post April 2014, no new patches will be available for Windows XP and Office 2003. Windows XP is still the second-most used OS on non-mobile computers. The 12 year old XP that debuted in 2001, has seen wide adaptability.

Unpatched systems could pose as a serious issue for especially those that handle financial and credit details such as those deployed at Point of Sale. An increase in zero-day attacks that target such vulnerabilities make it easy for malware authors to target millions of PCs.

But Windows XP isn't the only one that gets canned in April 2014, Microsoft Office 2003 will too. What is really worrisome is the fact that Office 2003 also runs on Vista and Windows 2007. There could be a possibility that even if one is using a fully-patched version of Windows, there could still be a risk of a zero-day attack exploiting a new Office vulnerability. And what is even stranger is that more often than not these vulnerabilities are not new ones.

# Zero-day Vulnerability Hits Microsoft Office

A pre-existing vulnerability in some versions of Microsoft office was discovered in early in the month of November 2013. This vulnerability was a flaw in the way Microsoft Graphics components handle graphical images. A hacker can exploit this flaw to remotely take over the victim's computer and gain the user's current rights.



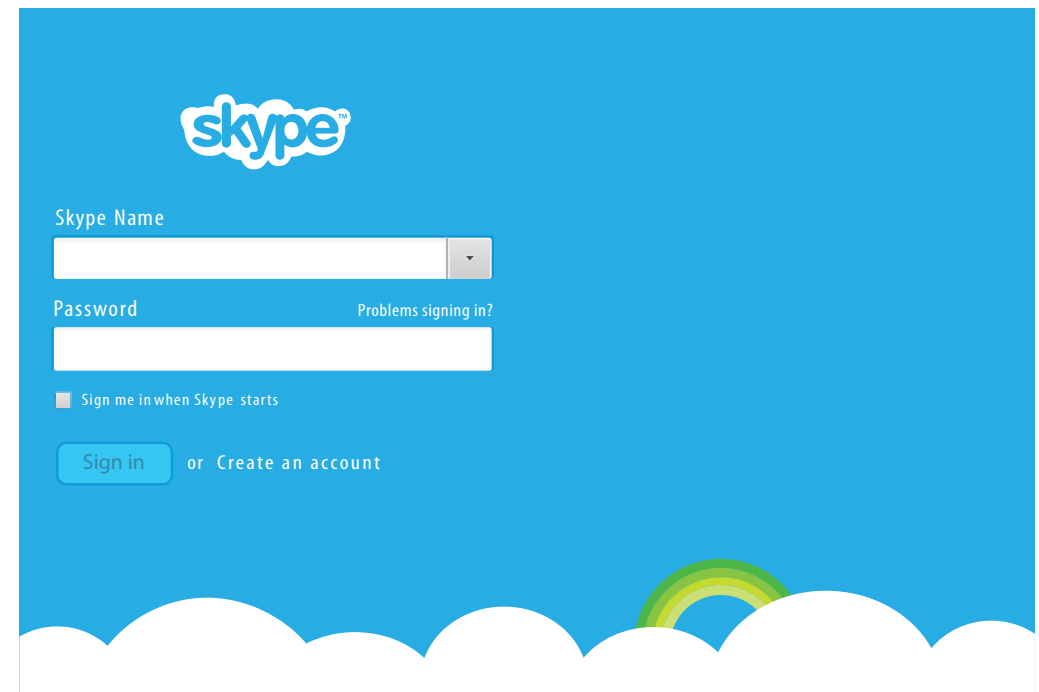
**Get Microsoft's Fix it Tool  
to deal with zero-day vulnerability  
in MS Office, MS Windows, and MS Lync.**

As another Java flaw is discovered, is it time to disable Java completely?



After a massive Java 0-day vulnerability surfaced in August 2012, Oracle released an out-of-cycle update to combat the exploit. However, we advised our readers to simply disable Java on their web browsers to avoid the threat. Java has now become a highly vulnerable program that causes more trouble than it is worth and this is highlighted by the fact that yet another 0-day Java vulnerability surfaced in January, 2013.

Microsoft in News for all the Wrong Reasons and now it's the recently acquired Skype



Are Your Messages on Skype Private?

## ANDROID

# Growth of Smarter and Tougher to Detect Attacks



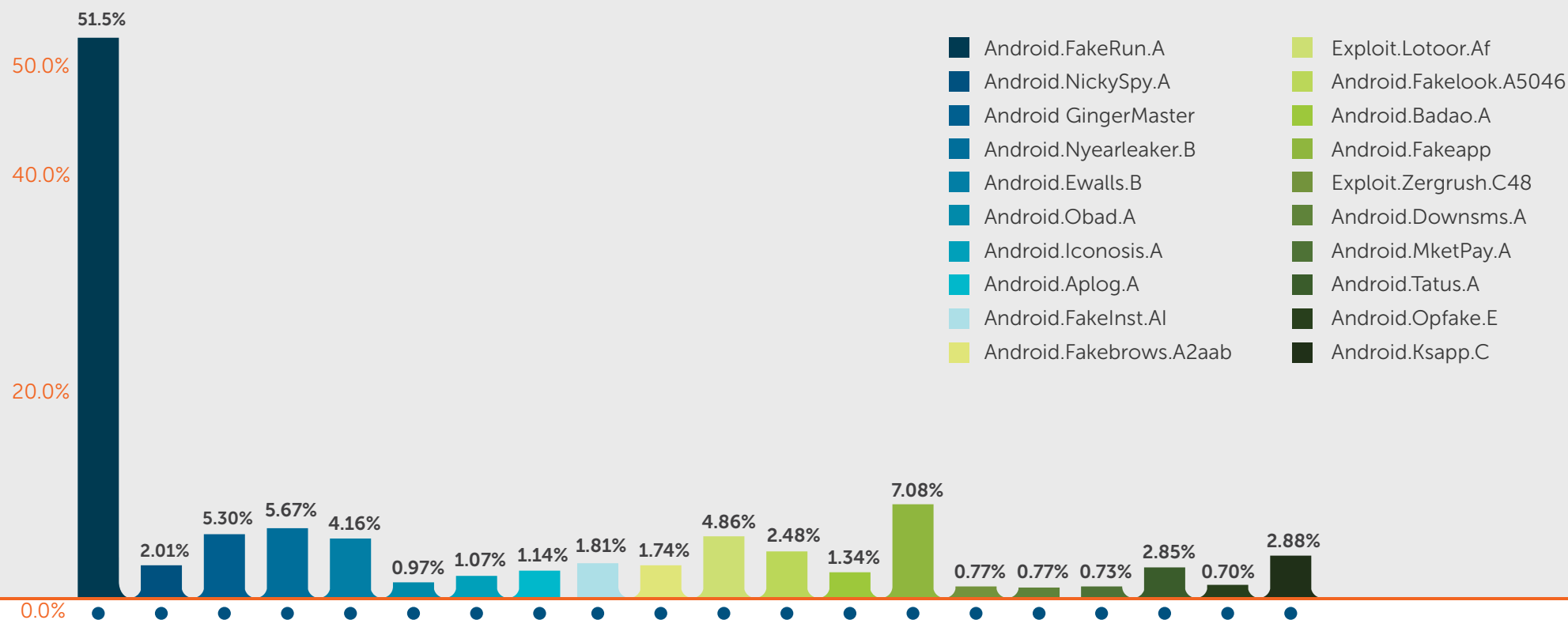
Since the time Android made its entry into the Smartphone arena, it ruffled quite a few players; even the big ones. At present time, Google Android grips a tight 51.6% of the US market share (source: [www.androidcentral.com](http://www.androidcentral.com), report as of August 2013). Android as versatile and popular the platform maybe has its own share of woes to deal with and most of it being related to the use of it to spread malware that can hide and counter detection.



# TOP 20 ANDROID MALWARE

The open source nature of the Android has made it the most popular mobile platform in the world. But as they, every Dr. Jekyll has a Mr. Hide with it. The overwhelming popularity of the green droid, and its staggering market share has placed it on a mantle in the house of hackers. This is easily evident by the fact that 99.9% of new mobile malware that are spewed by hackers, are designed to target Android. And with the ever increasing use of mobile Internet, Android has easily attracted the attention of budding and seasoned malware authors.

Our Threat Research and Response Lab report a whopping 800% surge in Android malware samples received.



## 01. Android.FakeRun.A

- Android FakeRun.A is an Android Trojan horse.
- It is designed to display ads on the infected device, to earn money for the malware author.
- The ad urges the user to give it a 5 star rating and increase its popularity.
- The Trojan also prompts the user to share information about the app on their Facebook accounts, even before it starts.
- This Trojan is mostly relevant in the US.

## 02. Android.NickySpy.A

- Android.NickySpy.A is an Android Trojan horse.
- The malware steals information from the infected device and sends it to an external server
- Once it gets installed, it hides itself; it get installed as "Android System Message"
- The malware:
  - Records the victim's telephone calls.
  - Keeps track of the location.
  - Send SMS to premim-rate numbers.

## 03. Android GingerMaster

- Android GingerMaster is an Android Trojan horse.
- It is mainly embedded with a fake version of a popular game.
- Once installed the application gains admin rights.

- It send confidential data to external servers.
- The malware can also download additional applications in the background without the user's knowledge.
- The Trojan can give remote access of the device to the hacker.

Android.Obad and Android.Fakedefender are two sophisticated Android malware families. These malware can exploit "Device Admin Privileges", which boost their stealth level after they get installed in a device. Once they gain admin privileges, it is difficult to remove them manually.



## 04. Android.Nyearleaker.B

- Android.Nyearleaker.B is an Android Trojan horse.
- This malware comes in the form a live wallpaper application that steals information.
- Once installed, the malware performs the following function:

- Fetches information about the device's WiFi connectivity
- Checks for running applications in the device
- Collects country code, email, address, Android IDIt sends the stolen data to its own server.

## 05. **Android.Ewalls.B**

- Android.Ewalls.B is an Android Trojan Horse
- It poses itself a wallpaper application, and steals information of the infected device.
- The malware steals the following information, once the user installs it in their phone:
  - SIM details
  - Operator name
  - Device's serial number (IMEI)
  - Model and build detail
- It sends the collected data to a live server.

## 06. **Android.Obad.A**

- Android.Obad.A is one of the most sophisticated Android malware that gain admin privileges.
- Once it gains admin rights, it cannot be deleted manually.
- It opens a backdoor in the infected device, downloads files and steals information.
- The malware also sends SMSs to premium-rate numbers, and can allow the hacker to gain complete control of the device.

## 07. **Android.Iconosis.A**

- Android.Iconosis.A is a Trojan horse designed to steal information infected Android devices.
- Once installed, the malware collects the phone number of the compromised device.
- Every time it is executed, it sends an SMS to the number.
- It also collects the IMEI number of the device, and sends the data to an external server.

## 08. **Android.Aplog.A**

- Android.Aplog.A is an Android Trojan.
- It is usually detected as a fake version of legitimate games; Temple Run is one of them.
- This application once installed, keep tracks of the infected phone's WiFi.
- The malware gathers information about the installation and uninstallation of applications in the device.
- Later it sends all such information to an external server.

## 09. **Android.FakeInst.AI**

- Android.FakeInst.AI is a Trojan horse.
- This malware can allow a hacker to manipulate SMSs in the compromised Android device.

- It can be used to manipulate user location and gain access to private information.
- Manipulate SMSs can be sent to premium-rate number.
- The malware can read the phone state of the user.

## 10. **Android.Fakebrows.A2aab**

- Android.Fakebrows.A2aab is a Trojan Android.
- The malware disguises itself as a legitimate app.
- It asks the user for a phone number when it runs for the first time.
- It monitors incoming SMSs to the compromised device, and forwards the same to the number that was set during its first running.

## 11. **Exploit.Lotoor.Af**

- Exploit.Lotoor.Af is an exploit designed to gain root privileges on Android devices.

This type of application has four .png files which are bundled along with the application. Their names are :

gbfm.png

install.png

installsoft.png

runme.png

As malicious applications run then rename the .png extension to .sh extension and execute the exploit as shell script.

When the device is successfully rooted, it will run the "install.sh" script which will set the file permissions to the system partition and then it copies the shell

from the bin folder "/system/bin/sh" to the folder created by the malicious application "/system/xbin/appmaster" so that, the shell can be easily accessed whenever it wishes and the system partition is remounted.

The exploit will work only when the device has an SD card mounted on it. If not, it simply refuses to run.

## 12. **Android.Fakelook.A5046**

- This malware hides itself from the Application List
- Once executed, this Android malware collects the following information:
  - Identity of the compromised device
  - SMSs
  - Files list from the SD card on the device

## 13. **Android.Badao.A**

- When Android.Badao.A is launched for the first time, an SMS message is sent to a particular number.
- After the first launch the application icon automatically disappears.
- Whenever the victim's phone receives any new SMS, it is hidden or removed from the user and the original message is sent to the attacker's server.

## 14. **Android.Fakeapp**

- Android.Fakeapp is a Trojan horse designed for Android devices.
- The malware displays ads by downloading configuration files without the user's knowledge
- It collects the compromised device's IMEI number and phone number.
- It sends the stolen information to an external server.

## 15. **Exploit.Zergrush.C48**

- Exploit.Zergrush.C48 attacks any vulnerability present in the targeted Android device, to gain root privileges.
- This type of application sets the property "ro.kernal.qemu" to 1 which makes the infected device run like an emulator.
- This category of application copy itself to /data/local/tmp/boomsh and change its privilege.
- It copies shell from "/system/bin/sh" to "/data/local/tmp/sh".

## 16. **Android.Downsms.A**

- Android.Downsms.A is an Android Trojan.
- Once installed, it sends SMSs to premium-rate numbers, and even removes sent messages.
- It can write to external storage.
- The malware can open network socket.

## 17. **Android.MketPay.A**

- Android.MketPay.A is a Trojan, found repacked in legitimate applications available in several Chinese markets.

- The malware performs the following functions:
  - Sends SMSs
  - Collects IMEI number and phone number of the compromised Android phone.
  - Automatically places orders for buying apps, without the user's consent.
  - Intercepts, blocks, and deletes incoming SMSs
- Sends stolen information to a remote server.

## 18. **Android.Tatus.A**

- Android.Tatus.A is a Trojan
- It sends SMSs.
- It can read the state of the compromised phone.
- Keeps a record of applications installed in the device, and sends this data to a remote server.

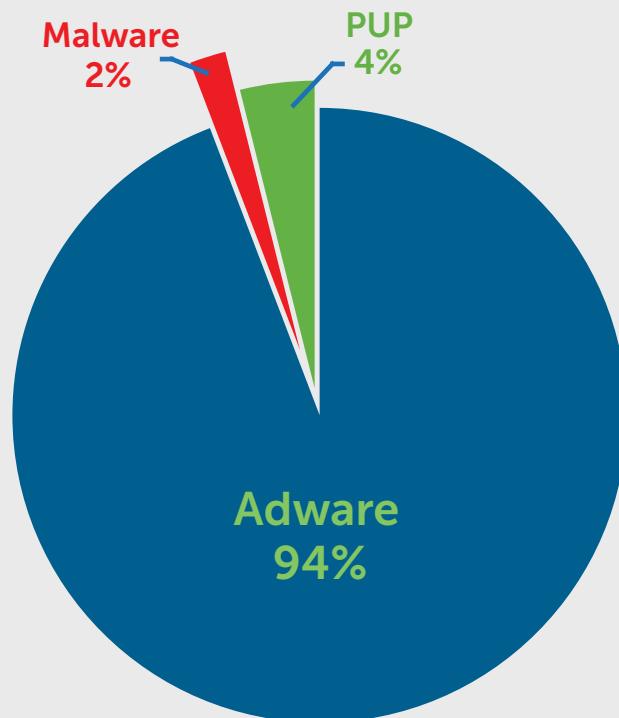
## 19. **Android.Opfake.E**

- Android.Opfake.E is a Trojan horse detected on Android devices.
- It comes bundled with a legitimate version of the Opera mobile browser.
- The malware collects data such as IMEI number, operator name, phone type, OS version, and country location.
- It sends SMSs to premium-rate numbers without the victim's knowledge.

- The malware connects to a command-and-control server to receive instructions.

## 20. **Android.Ksapp.C**

- Android.Ksapp.C is an Android Trojan.
- This Trojan is repackaged from a legitimate application. This application contains configuration file.
- It steals sensitive information and sends the gathered information to a remote server.
- This malware also downloads apk files.



## Android Malware Detection by Quick Heal

Total malicious programs detected - 431397

- Adware – 94%
- Malware – 2%
- Potential unwanted programs (PUP) – 4%



## Some Quick Facts about Mobile Security

- Most Android apps ask for too much permission even to do the basic thing.
- Many cyberattacks on mobile phones occur through compromised applications or exploited mobile web browsers.
- Since 2012, malware that target the Android platform has shot up by 600%.
- Reportedly, Jelly Bean seems to have a tighter security compared to the previous versions of the Android OS. However, about 36.5% per cent of Android devices are running Jelly Bean.
- Android malware has already hit the one million mark. This is in stark contrast with PC malware that took almost 10 years to reach this level.
- Smishing is a variant of phishing, where phishers use SMSs to trick their targets. It is an identity theft scheme that attempts to steal sensitive information from the target. This is done either by tricking the victim into visiting a fake website or call a phone number. In some cases, smishing scams also attempt to drop malware on targeted devices.
- Mobile users are more susceptible to phishing attacks than desktop users. This is because, people readily read text or email messages as soon as they hit the inbox.

# Giving the Farm Away To Hackers



99% of new mobile malware targets the Android platform

01

Ransomware will start targeting mobile devices in 2014

02

Android malware samples have grown by 800%

03

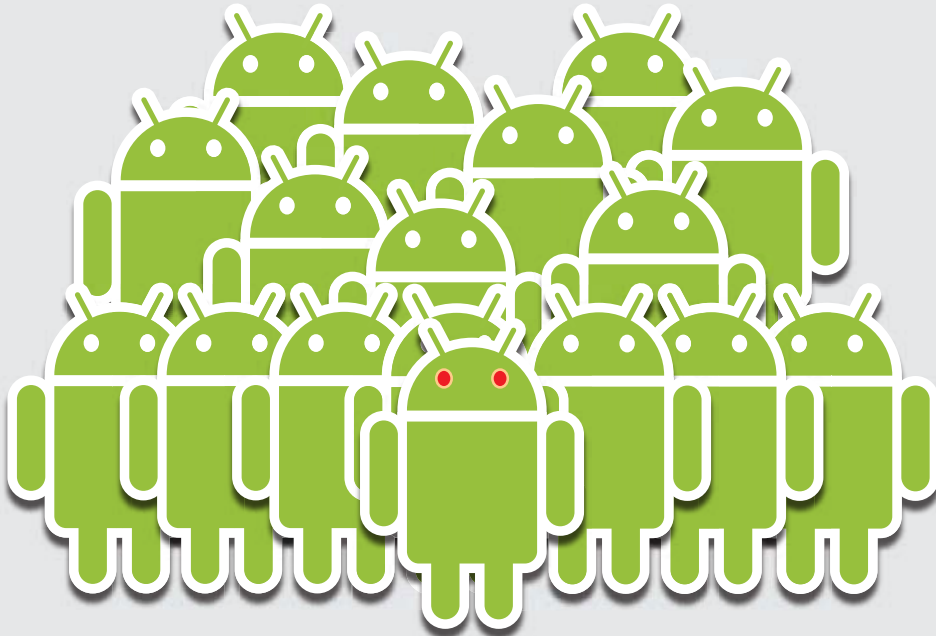
Over 7000 malicious apps are present in third party Android stores

04



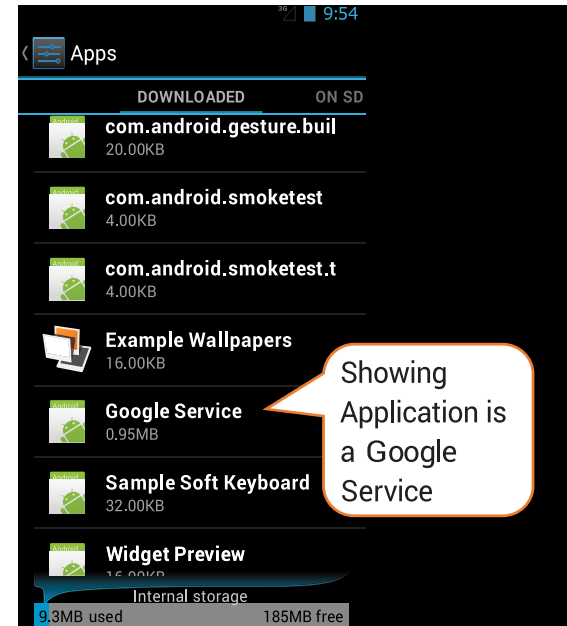
## Massive Android botnet invades China

# BOTNETS



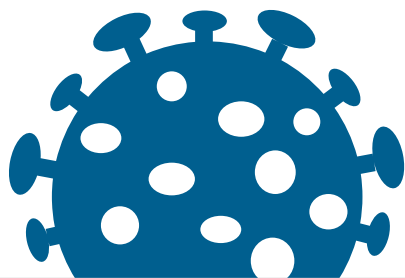
A massive Trojan botnet Andr/GGSmart-A, was discovered in Android devices in China. The discovery served as a timely reminder of the growing vulnerability of the Android platform. Staggeringly, this botnet has infected more than 1 million Android devices that function in China at that time.

## The Android Malware that exploits Simple Mail Transfer Protocol



The malware uses Simple Mail Transfer Protocol (SMTP) servers to send stolen information to the malware author

# Attackers Adapt to a Mobile-friendly Ecosystem



By the end of this year, the Internet connected mobile devices will outgrow the entire population of planet earth! Already the trends are being defined by mobile devices and on-the-move efficiency.

Man-in-the-middle-attacks are increasing because mobile users are typically less aware of the consequences of connecting to untrusted networks and Wi-Fi hotspots.

As more and more employees, bring in their personal devices to work, the task at hand would be to take a combination of approaches to restrict data breaches that would be the most serious of consequences.

## App Stores – Still a Loophole Here and There

### Watch out for Fake BBM apps for Android

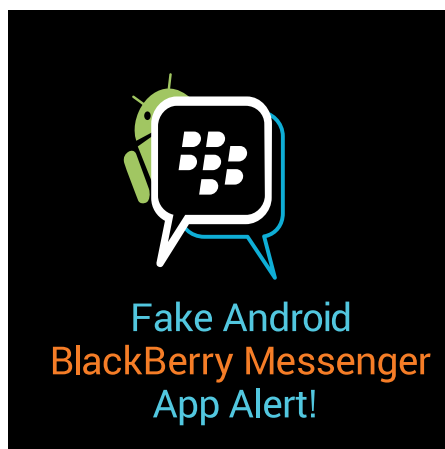
BlackBerry halted its global release of BBM (BlackBerry Messenger) version for Android and iPhone platforms. This was because of a fake (probably malicious) BBM application was released online.

### Whatsapp Hoax (fake) Messages Doing the Rounds Again

In late June 2013, we came across a fake message that was being actively circulated in Whatsapp. The miscreant's motive was to trick users to spread the message among their contacts.

## User Data Leakages






User data collected through malicious app are highly priced in black markets. Given the fact that mobile devices with all their geolocation facilities and gamut of apps, prove to be veritable sources of data, a lot of application developers regularly collect user data.



UR1994 KB1212 RJ1708 Send this message to 10 people. As soon as all of them have read your message, you will get an SMS from Whatsapp, with an activation code. Once you enter the activation code, you will no longer have to pay to use Whatsapp, which is going to charge for messages from new year 2013.

9:42am

# ANDROID SECURITY – SOME MORE FACTS


		Malware are rogue applications that do not like to rest. They keep running in the background, and this drains the battery of the infected phone. This is especially true for adware that keep showing ads. So, if you observe that your Android phone is losing out on battery juice, even without heavy usage, then odds are, it has a malware issue.	
Draining battery		Malware do not invade your phone just to sit and do nothing. Some of them like to eat up on the device's Internet data. Malware that steal information, usually send the same to remote servers. For this, they might use your phone's data connectivity. And this may result in abnormal upload and download, which will be evident from abnormally high data bills.	
Abnormal Data Usage		A malware-infected Android will have a hard time performing its tasks, sometimes even the basic ones like loading the camera, phone list or inbox. A malware that runs continuously in the background, stealing, monitoring, reading, sending information, etc., can suck off the phone's processing power big time. So, just run a check on the running applications on your phone. If there aren't many, and your phone runs like a 200 year old tortoise, then suspect a malware invasion.	
Poor Performance		Most Android malware are designed to send SMSs to premium-rate numbers without the victim's knowledge. And by the time the user realizes this, they might be slapped with an outrageously high phone bill.	
5 Signs that Say your Mobile Phone is infected	High Phone Bills		It is not unusual to experience drop calls. But if it occurs frequently, and your mobile carrier has no knowledge of it, then you can blame it on a malware infection. In this case, the malware could be an eavesdropper.
	Frequent Call Drops		


01

### Lock it!

Unless you are completely sure that you never leave your phone unattended or always carry it with you (yes, even to the washroom!) kindly set up a screen lock. You can either go for pin, pattern, password, or the face unlock feature.

**Go to Settings » Security » Screen Lock**





### Let Google Scan your Apps...


To reduce Android malware threat, it is always a safe bet to install apps only from Google Play. Installing third party apps can be risky. That's why, whenever you get such apps, Google asks your permission to scan them. All you have to do is tap "OK".


02

03

### Exploit The Android Device Manager

Misplaced your Android somewhere, lost it, or has it been stolen? Android Device Manager lets you see your phone's recent location on a map, make it ring at maximum volume, and even wipe its entire data. Take that "Find my iPhone"!



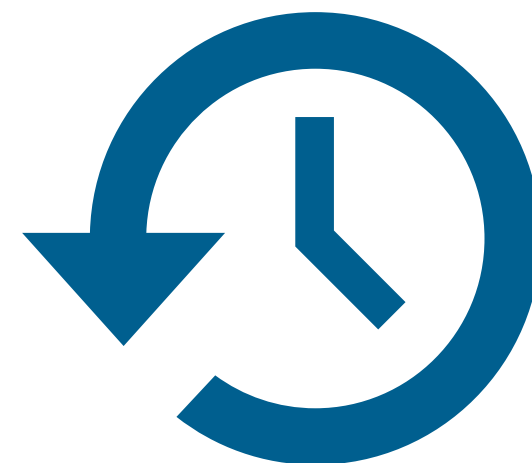


### Install a reliable Security Software

Android malware is spreading like wild fire. Make Quick Heal Mobile Security your phone's knight in shining armor. It's light, intelligent, and the easiest way to protect your Android. If you want it, then look no further than your own Google Play Store. Simply search for Quick Heal, and you are good to go.

04

## TRENDS

Trends to  
Watch Out  
For in 2014

We wish we could go by the quote "Live for the moment". Whatever data we have inferred from our observations and research over the past 12 months, we intend to use it to spread awareness and educate. It is important that both individuals and organizations small and big realize the importance of data and confidential information for these are assets that will be highly sought after by the cyber criminals. There is need for effective security. Security that is scalable and not restricted to the stereotypical antivirus.

## No new patches will be available for Windows XP and Office 2003 post April 2014

With Windows XP and Office 2003 support rapidly reaching the end of the line, the imminent exposure of unpatched systems to zero-day attacks is cause of serious concern. Windows XP being one of the most popular OS currently has a market share close to 30%. There are numerous small and medium businesses and enterprises that are yet to upgrade to Windows 7/8. Once Microsoft withdraws the support, these insecure machines will represent a serious danger to the security of the networks that they are connected to and the internet in general. This would also encompass any high-tech infrastructure that is directly or indirectly exposed. The concern here lies in the fact that, just a single zero-day vulnerability post April 8, could wreak havoc.

## Social Media will continue to be a prime hunting area.

Social networking sites have several elements that work together. They act as communications platform, as an advertising board and are mobile device friendly. This allures malware authors to devise tactics that include social engineering, malware, spam and phishing attacks.

## APTs will increase and might go hand-in-glove with money-making malware.

Advanced Persistent Threats (APTs) have been used for carrying out industrial espionage. Traditional malware authors might borrow components and delivery methods used by APTs.

Situation in windows malware might worsen post Windows XP and we will witness more targeted attacks on Govt. agencies and other critical service organization.

## Ransomware might make its presence felt on Mobile platforms.

Tackling ransomware will be on top priority list of IT security companies. These attacks might get more difficult to rectify. Once the success rate of these attacks is measured, malware authors can cash in on the opportunity to create variations

of this malware that not only threatens but might delete contents of the system.

## More Mac OS and iOS attacks

In February 2013, Reuters carried a news that read that Apple employees Macs were compromised by a zero-day attack that targeted a java vulnerability. As these platforms become more popular, they will be targeted more often.

## The Internet-of-Things will be threatened by the increasing use of insecure devices.

By the end of 2014 there will be more Internet connected devices than people on the planet. Yet as more and more devices connect to this growing network, the security and privacy of data in such an environment remains questionable.

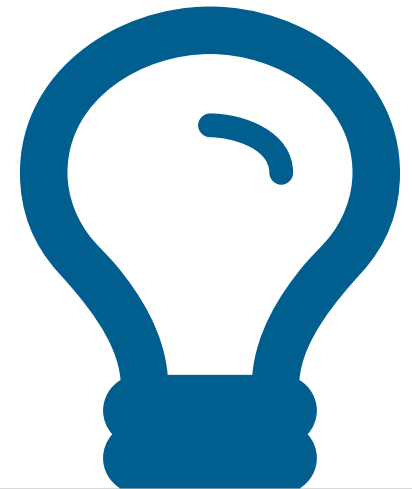
These interconnected devices can be used as avenues for attacks.

## Future Watch VII: War-texting threatens the future of Internet of things

War-texting can be described as the incessant sending out of SMS texts to utility devices that pair with smartphones. The term was coined by a team of researchers who also provided a live demonstration of this technique.

## Supply Chain attacks are for real and looking for the needle in the haystack continues to be difficult.

Detecting malware infected devices is cumbersome and difficult. But these are actual security concerns that need thorough thinking and implementation.



The diversification of devices continues to be a source of concern. Most of these devices store valuable data and are everywhere, in our homes, offices and even connected to the infrastructure. Anyone with a malicious intent can actually rig these devices and cause harm.

The key here is to be aware and be secure. Understand what needs to be protected and use it wisely. Brush-up on your security basics like having strong passwords, differentiate a genuine Facebook post from a social engineering snare and so on.

The fight against cyber crime is not going to end anytime soon. Cyber criminals are getting smarter and have been refurbishing old techniques to use against new unsuspecting targets. At Quick Heal, we work towards understanding how these threats can be obliterated and how we can deliver real-time updates.