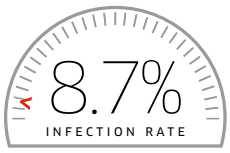
# KINDSIGHT SECURITY LABS MALWARE REPORT – Q4 2013

Alcatel·Lucent

# TABLE OF CONTENTS

# INTRODUCTION

The Alcatel-Lucent Kindsight Security Labs Q4 2013 Malware Report examines general trends for malware infections in home networks and infections in mobile devices and computers connected through mobile adapters. The data in this report is aggregated across the networks that deploy Kindsight Solutions.





## 2013 HIGHLIGHTS

- On the mobile side, infections increased 20% in 2013 with an infection rate of 0.55% at the end of Q4. Based on this, we estimate that at any time over 11.6 million mobile devices are infected by malware. Of these, 60% are Android smartphones.
- The overall residential infection rate in fixed networks dropped from 9.6% in October to 8.7% in December.
- The number of mobile malware samples experienced exponential growth in 2013 with 20 times growth over the year.
- Six percent of broadband residential customers were infected with high-level threats such as a bots, root-kits, and banking Trojans.
- Although still number one, the ZeroAccess infection rate dropped from 0.8% to 0.4% in Q4. This decline is certainly related to the efforts of Microsoft and Symantec to disrupt the botnet's operations.

# 2013 IN REVIEW

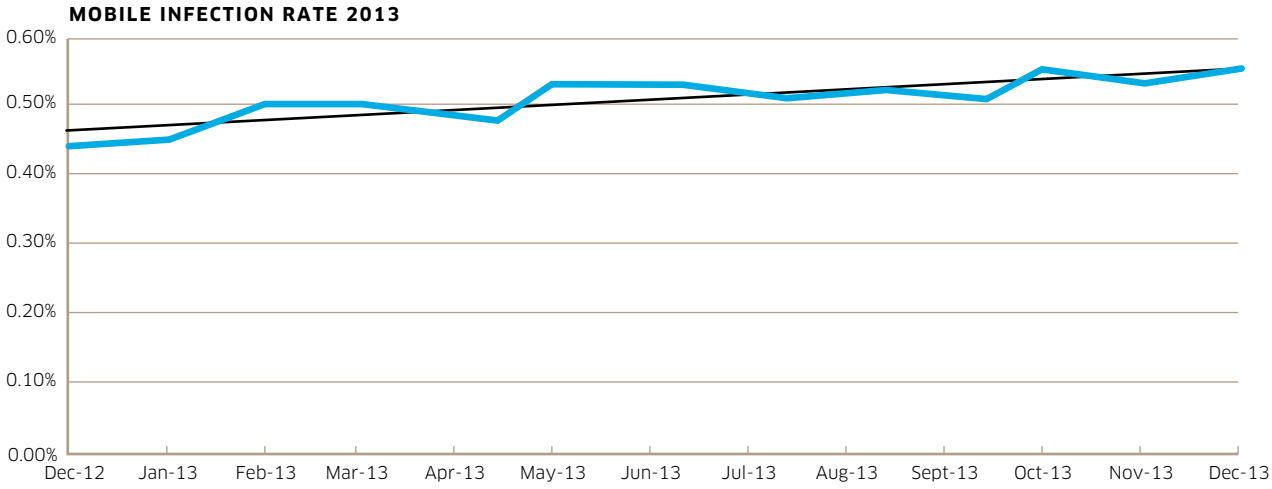
# MOBILE MALWARE IN 2013

2013 saw some significant developments in mobile malware. The overall mobile infection rate climbed to 0.55%, the number of Android malware samples continued its exponential growth, and for the first time we saw Windows/PC-style botnets make the transition to the mobile platform.

## OVER 11.6 MILLION DEVICES INFECTED

### Data from Kindsight Network Deployments

The graph below shows the percentage of infected mobile devices over the past year. This data is averaged from actual mobile deployments.




## HIGHLIGHTS

- Problem is growing (by 20% in 2013)
- LTE devices are two to three times more likely to be infected
- Currently estimate over 11.6 million infected devices world wide

It shows the measured infection percentage month by month over the year. It is currently at 0.55%. This number is calculated on a monthly basis.

We can use this percentage to estimate the number of infected smartphones worldwide. Based on this we estimate that 11.6 million mobile devices are infected at any time. (The ITU estimates that there are currently 2.1 billion smartphones in use.)

Because Alcatel-Lucent sensors are not deployed in China and Russia, where infection rates are known to be higher, our global estimate is likely on the conservative side, but it does line up with the numbers reported by other security vendors as can be seen below.

## CONFIRMATION FROM OTHER SOURCES

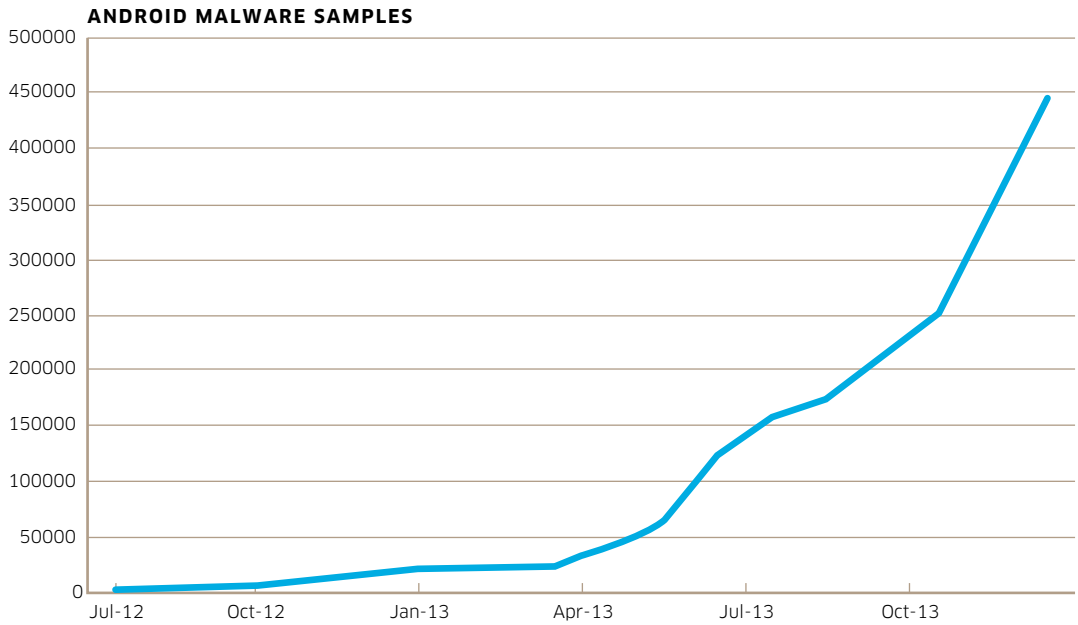
In Lookout's report "State of Mobile Security 2012," they showed the North American infection percentage to be between 0.2% and 0.4% in June 2012. This is clearly in line with what Alcatel-Lucent reports, entering 2013 at 0.45% and climbing to 0.55% as the year progressed.

In a subsequent blog entitled Mobile Threat Predictions, Lookout predicts that 18 million Android devices will encounter some form of malware between the start of 2012 and the end of 2013. Given that Alcatel-Lucent's estimate for September alone was 11.6 million, the Lookout estimate for that two-year period may be somewhat on the low side.

In the 2013 Mid Year Mobile Security Report, NQ Mobile reported that 21 million mobile devices were infected with malware in the first half of 2013. This also lines up well with the number reported by Alcatel-Lucent. As pointed out above, the Alcatel-Lucent number is based on North American observations for the month of September. NQ Mobile's figure covers half the year and includes data from China and Russia, which are known to have higher infection rates.

## ANDROID MALWARE SAMPLES GREW 20 FOLD IN 2013

An indicator of Android malware growth is the increase in the number of samples in our malware database. The chart below shows numbers since June 2012. The number of samples increased 20 fold in 2013.The number of samples doubled in Q4.

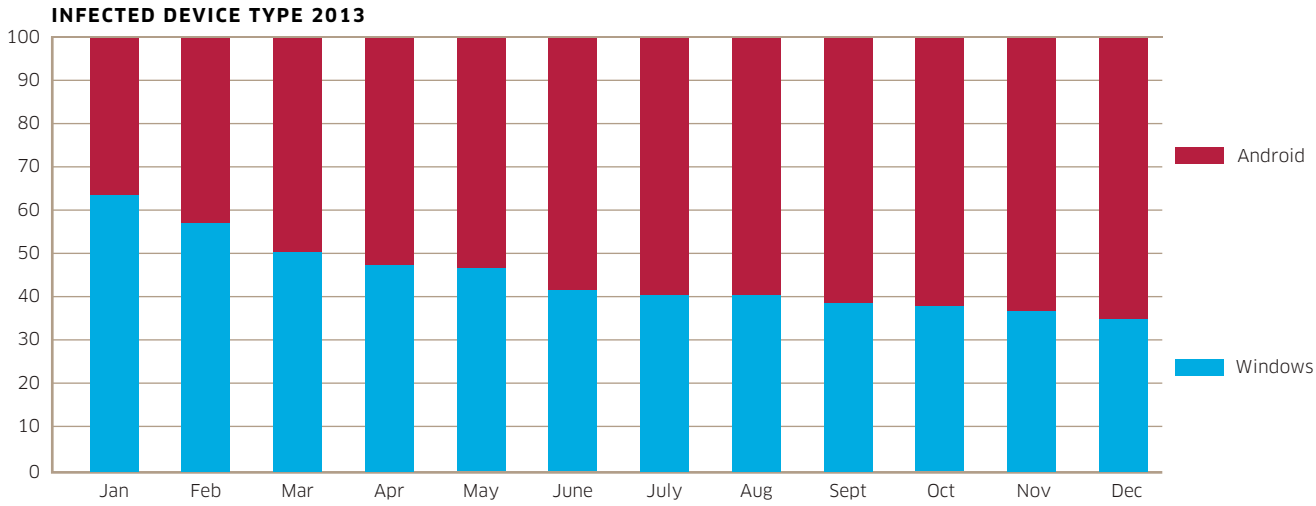



This increase is mostly due to the fact that Trojanized apps are the primary infection vector in the mobile space. The more apps the attacker can get out there, the more successful they will be in infecting the population. Often we will discover a third-party app store distributing a single malware type disguised as hundreds of different wallpaper apps.

So unlike the Windows/PC space, where cyber criminals create thousands of variants to bypass anti-virus software, in the mobile space the large number of samples currently increases the probability of the app being downloaded and installed.

Despite the great increase in numbers, the quality and sophistication of most Android malware is still a long way behind the more mature Windows/PC varieties. The command and control (C&C) mechanisms are primitive and often don't work; configurations are hard-coded and inflexible; the malware makes no serious effort to conceal itself; and attack vectors are limited to hoping someone installs the infected app. That said, 2013 saw a number of Android malware specimens that are beginning to show the sophistication that we see in their Windows cousins.

## ANDROID & WINDOW PC BIGGEST OFFENDERS




- 60% of infected devices are Android
- 40% are Windows PCs connected to the mobile network
- <1% iPhone, Blackberry, Symbian, Windows Mobile

Clearly the Android smartphone is the biggest malware target in the mobile space followed by the Windows/PCs, which are still the favorite of hard-core professional cyber criminals. The reasons for this are discussed below.

## ANDROID IS BECOMING THE WINDOWS XP OF MOBILE

Android devices are currently the most targeted, accounting for 60% of the infections observed in the mobile network. Almost all of the malware is in the form of Trojanized apps downloaded from third-party app stores or Google Play, with phishing spam campaigns luring victims to install the infected apps.

There are a number of reasons why Android has become the target of choice:

1. Android currently has the largest smartphone market share. Traditionally cyber criminals will go after low hanging fruit that will maximize their return on investment.
2. Unlike the iPhone and Blackberry, the Android offers the ability to load apps from third-party app sites. This provides the cyber criminals with an un-policed mechanism to distribute their malware.
3. It is trivial for an attacker to hijack a legitimate Android application, inject malware into it and redistribute it for consumption. There are now binder kits available that will allow an attacker to automatically inject malware into an existing application. This is only exacerbated by Android's incredibly weak app signing policy that encourages using self-signed certificates to sign applications.

The following types of malware are fairly common:

- Adware
- Information Stealers
- Spy Phone
- SMS Trojans
- Banking Trojans
- Fake Security Software

A lot of Android malware is currently fairly naïve and simplistic in its design and operation. We see very little of the sophistication that is apparent in the Windows/PC world. Often the C&C site will be hard-coded as a single IP address or domain name right. There are no sophisticated botnet rallying strategies. We often find malware samples that don't work because the C&C is no longer functional. Similarly it is rare for the malware to make any serious attempt to conceal its operation. Occasionally configuration files will be encrypted, but it's rare to find one that obfuscates its code, conceals its operation or actively avoids analysis. Very few attempt to avoid detection and removal and typically the malware can be removed by simply uninstalling the offending app.

Despite its shortcomings, Android malware does present a significant risk for the infected user. Banking Trojans go after banking credentials that can cause a significant financial loss. SMS Trojans that send messages to premium numbers can also add up to larger bills. Fake Security apps use direct extortion to make money.

## WINDOWS MALWARE IMPACTS MOBILE NETWORKS

Windows/PC malware remains the workhorse of mainstream professional cyber crime and represents 40% of the infections that we are seeing in the mobile network. The PCs are connected to the mobile network via USB dongles, MiFi or by tethering through mobile phones.

In the mobile network we see the full gambit of Windows/PC infections including the following:

- Botnets
- Rootkits
- SPAM
- Identity Theft
- Banking Trojans
- Distributed Denial of Service (DDoS)
- Ad-Click
- Anonymizing Proxy
- Bitcoin Mining
- FakeAV
- Ransomware
- Hacktivism
- Spyware

Many of these infections not only impact the user, but can also have a significant impact on the network infrastructure. For example:

- Proxy bot creates 800,000 TCP sessions and consumes 3 GB of data in a 24-hour period
- Roaming user draws botnet traffic from 4 000 botnet peers around the world, all backhauled via their home network

## WHAT'S NEXT

Cyber criminals have a huge investment in the traditional Windows/PC platform and will only move to the mobile space as business opportunities present themselves or as traditional opportunities are eroded by the new technologies. This can be seen with "green field" opportunities like SMS monetization and will accelerate as users abandon traditional PCs and laptops. In the meantime the following areas could be exploited.

### Advanced Persistent Threat

The smartphone presents an excellent platform for advanced persistent threat (APT) and cyber espionage attacks against corporate and government networks. Malware deployed on a smartphone can communicate 24/7 through the air with a remote C&C site, bypassing all corporate security measures. The attacker can monitor the phone's location, download personal information from the

phone, intercept and send SMS messages, monitor phone calls, take pictures and videos and record conversations. If the phone has access to the corporate Wi-Fi, the attacker can access internal data, probe for network vulnerabilities, compromise internal hosts and exfiltrate corporate data.

### Mobile Botnet

Mobile botnets exist today, but they are not as extensive and disruptive as the Windows/PC variety. This will change as botnets that leverage the capabilities of the mobile phone become more common.

Today there are some mobile botnets that specialize in SMS spam. They will grow significantly as cyber criminals realize that it is more cost effective to have SMS spam delivered by a botnet than a farm of real phones with unregistered SIM cards.

Botnet-based DDoS attacks have traditionally been directed at corporate or government web sites. In the mobile space, it would be possible to direct the attack at the 1-800 number used for inquiries, support and sales. SMS DDoS could also be launched as well as attacks specifically targeting the mobile infrastructure.

### Hacktivism and Cyber-Terrorism

Hacktivism is also an area that can be exploited. Imagine an underground hacktivism organization that provided their own app for Android and iPhone. The app would allow the coordination of hacktivism activities and facilitate coordinated DDoS attacks against government, industry and infrastructure. It is not inconceivable that a future “Occupy the Internet” protest movement could be based on rogue mobile apps.

The potential for cyber terrorism is also troubling. Mobile botnets have the potential for being much larger and more widespread than the traditional PC-based ones. A DDoS attack from such a botnet against mobile infrastructure could be quite devastating.

## ANDROID MALWARE AROUND THE WORLD

A big difference so far between mobile malware and the traditional malware that affects Windows/PCs is the regional variation. There is a lot more regional variation in the malware that attacks mobile devices. The following factors could be responsible for this:

1. Since apps are the main attack vector in the mobile space, apps that are regionally or culturally popular tend to be favored by the attackers. So many attacks are regionally focused simply due to the choice of which apps to infect.
2. Mobile malware is usually installed as the result of a phishing attack directed at a specific language group. On the Windows platform, language was not such an issue because the malware was usually delivered as a virus, worm or exploit where language was not an issue.
3. There are different ways for the criminals to make money in different regions. For example, in eastern Europe sending SMS messages to premium numbers is commonly used as a payment mechanism, so that is often an attack target in those regions. The same attack won’t work in North America because those premium SMS numbers don’t work. Similarly, in certain regions banks tend to use one-time transaction codes sent to mobile phones to authenticate banking transactions. Regionally focused malware can take advantage of this.
4. Third-party app stores are much more common in certain parts of the world and tend to focus on specific countries, languages and regions. Malware authors may find it easier to distribute malware in those app stores.

# MALWARE IN THE NEWS IN 2013

## ZEROACCESS TAKEDOWN ACTIVITIES

**ZeroAccess** is still the number one botnet, despite attempts by both Symantec and Microsoft to disrupt its operation. However its ability to make money through an ad-click fraud scheme appears to have been dealt a severe blow by the Microsoft activity.

There are actually four separate ZeroAccess botnets that can be distinguished by the UDP port numbers used in the C&C protocol. Two earn their living through ad-click fraud, the other two through bitcoin mining. The peer-to-peer C&C protocol is used to maintain the botnet and ensure that each bot has an up-to-date copy of the ad-click or bitcoin mining components. The ad-click and bitcoin mining activities use separate C&C protocols to support their operation.

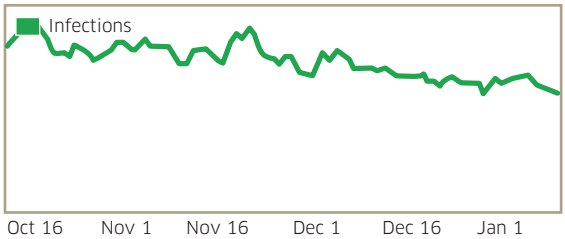
In July Symantec initiated an attempt to take down ZeroAccess by disrupting the peer-to-peer C&C protocol. This had a significant impact on the botnet, taking down nearly half a million bots, about 25% of the estimated total. It seems to have recovered somewhat from that in Q4, but is not up to its original strength.

In December Microsoft took a different approach. The botnet earns money for its operators through an ad-click fraud scheme. This uses a separate C&C infrastructure that is not peer-to-peer-based. It uses a small pool of servers with fixed IP addresses to deliver instruction to the bots on which advertisements to click on. Microsoft appears to have blocked access to these servers, destroying the ad-click fraud C&C. So the botnet still exists, but the ad-click fraud is no longer in operation.

There has been some debate in the press regarding the effectiveness of this disruption. It appears that the ad-click activities have been curtailed, but the botnet is still very much alive. Detection results from the field and recent lab tests on the malware have verified the following facts:

- The four peer-to-peer botnets are still active (see chart below).
- The ad-click operation is no longer active.
- It's not clear whether the bitcoin mining is still active.

**ZERO ACCESS ACTIVITY Q4 2013**




Another interesting aspect is that while running a lab test back in October, we noticed what appeared to be an attempted DoS attack on Microsoft's Windows Update server. A computer infected with ZeroAccess downloaded the file "/msdownload/update/v3/static/trusted/en/authrootstl.cab" from the Microsoft update server over 4 000 times in a 30-minute period. Perhaps this was part of the war between Microsoft and the ZeroAccess operators.

For more details on Zero Access see:

Alcatel-Lucent Kindsight - ZeroAccess Malware Analysis

Sophos - ZeroAccess Botnet

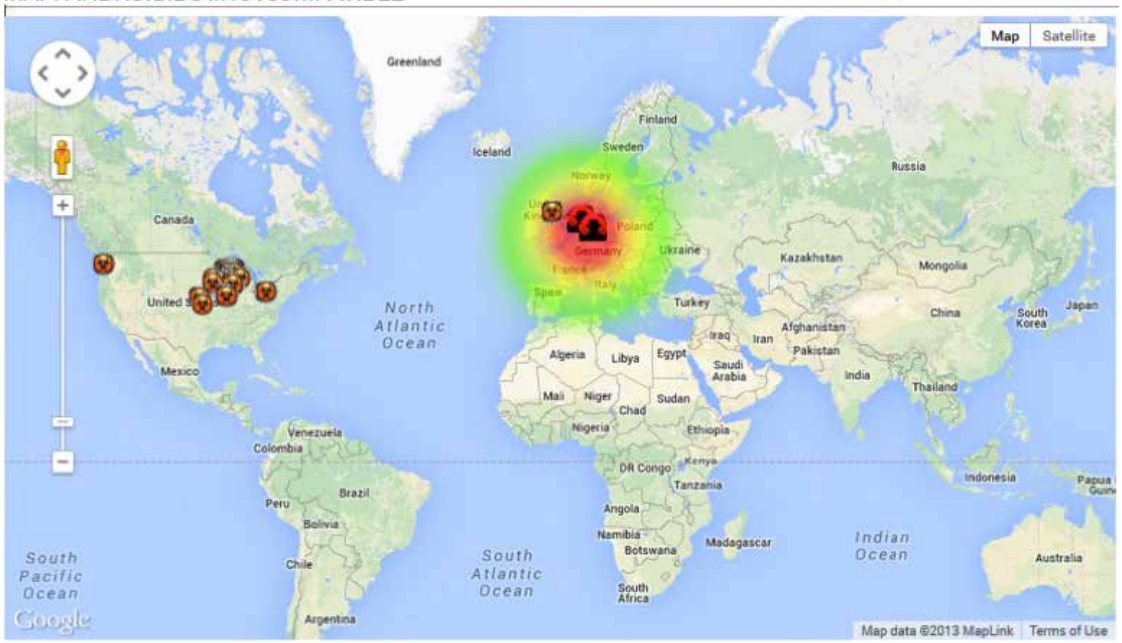
Microsoft - Zero Access Criminals Wave a white flag – The impact of partnerships on cybercrime

Symantec – Grappling with the ZeroAccess Botnet

## NOTCOMPATIBLE

Also in the news this year was **NotCompatible**. This is an Android bot that uses the infected phone to provide anonymous proxy web browsing services. This can consume large amounts of bandwidth and airtime, as the phone serves as a proxy for this illicit web browsing activity. The C&C is located in Germany and Holland. The C&C protocol is the same as a Windows-based web proxy bot. This is the first time we've seen a common C&C infrastructure shared between Windows and Android malware. The malware was first discovered in early 2012 and has had a recent resurgence due to a spam campaign to spread the malware.

MAP: ANDROID.BOT.NOTCOMPATIBLE




There are some interesting aspects of NotCompatible that make it stand out from other Android malware.

- A spam-based phishing attack lures users to infected web sites that automatically download the file Update.apk to the phone. The user must click "install" for the installation to proceed.
- The C&C and the network servers that support it are same as one used by Windows malware that provides the same proxy services. This is the first time we've seen both Windows PCs and Android phones operating as a single botnet.
- The web proxy operation can consume considerable network resources and will likely lead to large data charges, particularly for roaming users. In one instance, we saw an infected phone consuming 165 MB of web bandwidth in less than two hours across over 300,000 TCP flows. Almost all of this activity can be attributed to the web proxy activity.
- The infection rate from the field shows that 0.03% of mobile devices are infected.

The proxy can be used for a variety of purposes:

- Anonymous browsing services
- Access to restricted foreign content
- Web site optimization fraud
- Ad-click fraud
- Internal network probe and data exfiltration (Enterprise APT case)

It is likely that anonymous browsing is the most common use case for this malware. For a more in-depth analysis of NotCompatible, see the Kindsight Security Labs malware analysis report.

## GOOGOST

**Googost** infects Windows computers and provides the attacker with a web proxy that can be used for a variety of cyber criminal purposes. The C&C servers are located in Germany and the Netherlands. The infected devices connect to these C&C servers and are used to proxy web traffic, which can be used to support the following illicit operations:

- Anonymous browsing services
- Access to restricted foreign content
- Web site optimization fraud
- Ad-click fraud
- Internal network probe (Enterprise APT)

### MAP: WIN32.TOJAN.GOOGOST.A


The infected Googost device contacts a C&C server in Europe and establishes a TCP connection. When the C&C server has work, it sends the domain name and an HTTP GET request indicating what web page should be retrieved. The infected device contacts the indicated web server, issues the HTTP GET request and retrieves the results. These results are sent immediately to the C&C server via the pre-established TCP session. The C&C server then closes the TCP connection to the infected device to indicate that the request is complete. The infected device then reopens the TCP connection and repeats the process.

This can consume considerable bandwidth if the requesting host is very active. In one case we saw a single mobile device make over 800,000 web connections and consumed over 3 GB of bandwidth in a single day. In another case a device used a total of 185 MB of bandwidth in only 27 minutes. High bandwidth usage caused by malware can have a huge impact on the mobile charges for customers who don't have unlimited data plans. It can also impact network resources.

For a detailed technical analysis of Googost, see: http://resources.alcatel-lucent.com/?cid=172221

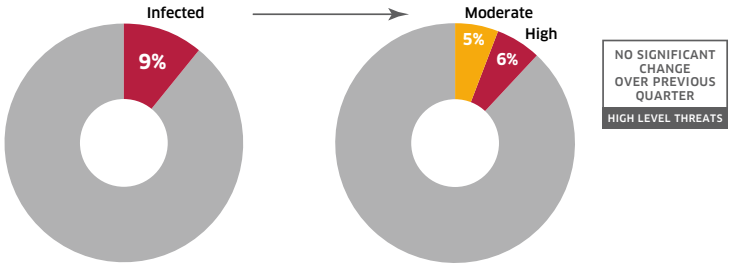
# Q4 STATISTICS

# Q4 2013 HOME NETWORK MALWARE STATISTICS

## HOME NETWORK INFECTION RATES

This quarter the infection rate for residential networks has remained relatively flat at around 9%. In September it was at 9.8%, dropping to 8.7% by December.

Six percent of households were infected by high threat level malware such as a botnet, rootkit or banking Trojan with 5% of households also infected with moderate threat level malware such as spyware, browser hijackers or adware. Some households had multiple infections including both high and moderate threat level infections.




Home networks infected with Malware

Division of infection by Threat Level

## TOP 20 HOME NETWORK INFECTIONS

The chart below shows the top home network infections detected in Kindsight deployments. The results are aggregated and the order is based on the number of infections detected over the three-month period of this report.

| RANK | NAME | THREAT LEVEL | % OF TOTAL | LAST QUARTER |
|---|---|---|---|---|
| 1 | Win32.Adware.Wajam | Moderate | 13.93 | New |
| 2 | Win32.Bot.ZeroAccess2 | High | 8.83 | 1 |
| 3 | Win32.Trackware.Binder | Moderate | 5.49 | 2 |
| 4 | Win32.Hijacker.StartPage.KS | Moderate | 4.85 | 3 |
| 5 | Win32.Adware.WebCake | Moderate | 2.99 | New |
| 6 | Win32.Bot.ZeusZbot_P2P | High | 2.84 | 8 |
| 7 | Win32.Adware.Wysotot | Moderate | 2.81 | New |
| 8 | Win32.Adware.MarketScore | Moderate | 2.77 | 9 |
| 9 | Android.Adware.Uapush.A | Moderate | 2.70 | 5 |
| 10 | Win32.AdWare.AddLyrics.T | Moderate | 2.66 | New |
| 11 | Win32.Bot.Alureon.DX | High | 2.22 | 4 |
| 12 | Win32.Bot.Alureon.A | High | 1.84 | 11 |
| 13 | Win32.BankingTrojan.Zeus | High | 1.33 | 10 |
| 14 | Android.Trojan.Coogos.A!tr | High | 1.28 | 24 |
| 15 | Win32.BankingTrojan.ZBot | High | 1.10 | 17 |
| 16 | Win32.Adware.MediaFinder | Moderate | 1.09 | 15 |
| 17 | Win32.Spyware.MyWebSearchToolb | Moderate | 0.75 | 14 |
| 18 | Win32.Trojan.Bunitu.B | High | 0.60 | 20 |
| 19 | MAC.Bot.Flashback.K/I | High | 0.59 | 19 |
| 20 | Win32.Worm.Mimail.E@mm | High | 0.57 | New |

## TOP 20 HIGH LEVEL INFECTIONS

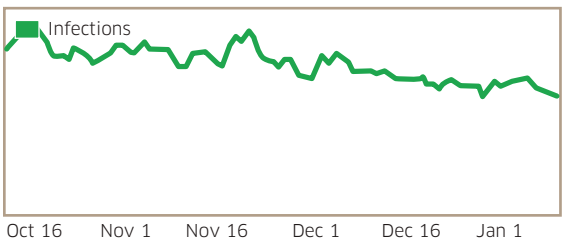
The table shows the top 20 high threat level malware infections that lead to identity theft, cyber crime or other online attacks. We'll look at the top three in more detail in the next section.

| RANK | NAME | % OF TOTAL | LAST QUARTER |
|---|---|---|---|
| 1 | Win32.Bot.ZeroAccess2 | 16.77 | 1 |
| 2 | Win32.Bot.ZeusZbot_P2P | 5.40 | 3 |
| 3 | Win32.Bot.Alureon.DX | 4.22 | 2 |
| 4 | Win32.Bot.Alureon.A | 3.50 | 6 |
| 5 | Win32.BankingTrojan.Zeus | 2.53 | 8 |
| 6 | Android.Trojan.Coogos.A!tr | 2.43 | 16 |
| 7 | Win32.BankingTrojan.ZBot | 2.09 | 7 |
| 8 | Win32.Trojan.Bunitu.B | 1.15 | 12 |
| 9 | MAC.Bot.Flashback.K/I | 1.13 | 11 |
| 10 | Win32.Worm.Mimail.E@mm | 1.09 | 33 |
| 11 | Win32.PasswordStealer.Lolyda.B | 1.04 | 13 |
| 12 | Win32.ScareWare.Somoto.AMN | 0.98 | 9 |
| 13 | Win32.BankingTrojan.Zeus/SpyEy | 0.88 | 10 |
| 14 | Win32.BankingTrojan.Carberp | 0.84 | 14 |
| 15 | Win32.Trojan.Sisproc | 0.82 | New |
| 16 | Win32.Bot.Darkness | 0.71 | 15 |
| 17 | Win32.Downloader.Obvod.K | 0.66 | 19 |
| 18 | Win32.Backdoor.Ammyy.z | 0.54 | 24 |
| 19 | Android.Trojan.Wapsx | 0.45 | 27 |
| 20 | Win32.Bot.Alureon | 0.42 | 26 |

## TOP INFECTIONS

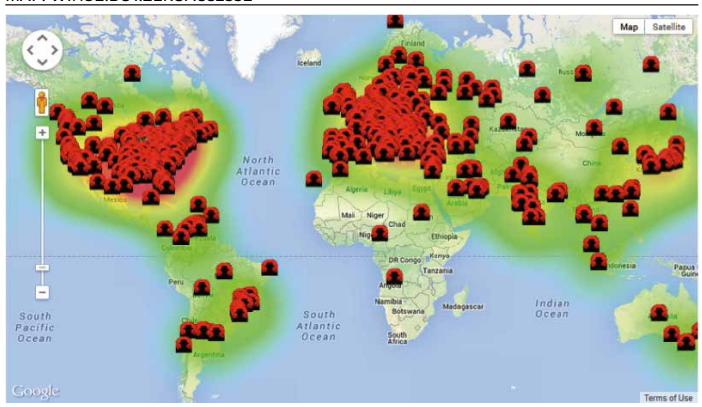
The top three infections remain the same as in Q3, the three major botnets: ZeroAccess, Alureon and Zeus.

**ZeroAccess** is a peer-to-peer (p2p) bot that uses rootkit technology to conceal its presence. It downloads additional malware that is used in a large-scale ad-click fraud. This fraud can cost Internet advertisers millions of dollars each day. The bandwidth utilization is moderate at any given time, but when aggregated over a month can be quite significant for the user. Due to the p2p nature of this infection the C&C is everywhere with heavy concentrations of infection in the US, Europe and Asia.

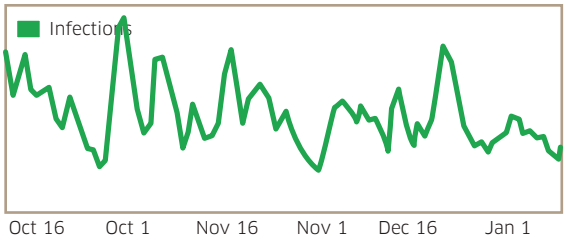



Name: Win32.Bot.ZeroAccess2
ID: 512061170
Signature State: Active
Type: Bot
Class: Cybercrime
Level: High

MAP: WIN32.BOT.ZEROACCESS2



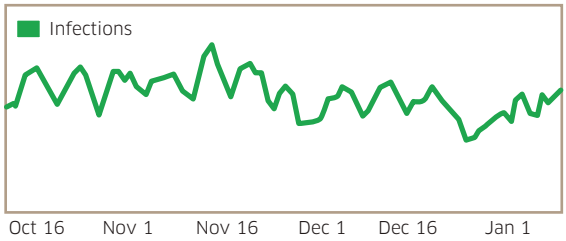
**Zeus/Zbot** is a banking Trojan that has been around in various forms since 2007. Zeus has evolved considerably since then and continues to cause havoc. The most recent version uses an encrypted p2p C&C protocol. This bot attaches itself to the victim's browser and monitors online banking activity. Banking credentials and credit card numbers are then sent back to a C&C site.




Name: Win32.BankingTrojan.Zeus/Zbot
ID: 513042480
Signature State: Active
Type: Bot
Class: Cybercrime
Level: High

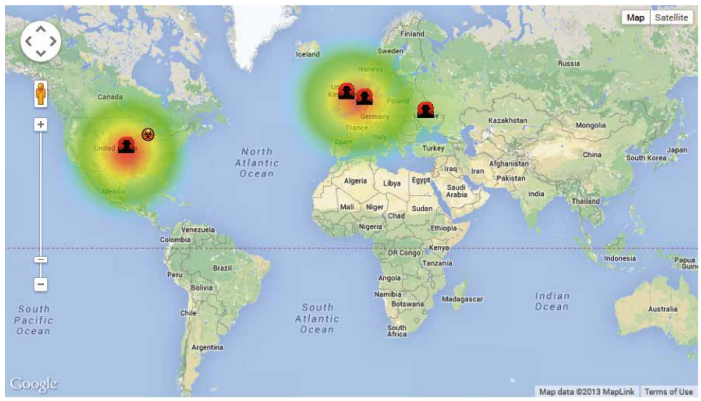
MAP: WIN32.BANKING TROJAN.ZEUS.ZBOT


**Alureon.DX** is a bootkit Trojan that steals usernames, passwords and credit card information and uploads the information to a remote C&C server. It was first seen in 2006 and has evolved through a variety of versions since then. It gets control of the device by rewriting the master boot record and actively conceals itself from antivirus software. C&C servers are located in the US, UK, Netherlands and Ukraine as shown in the map below.



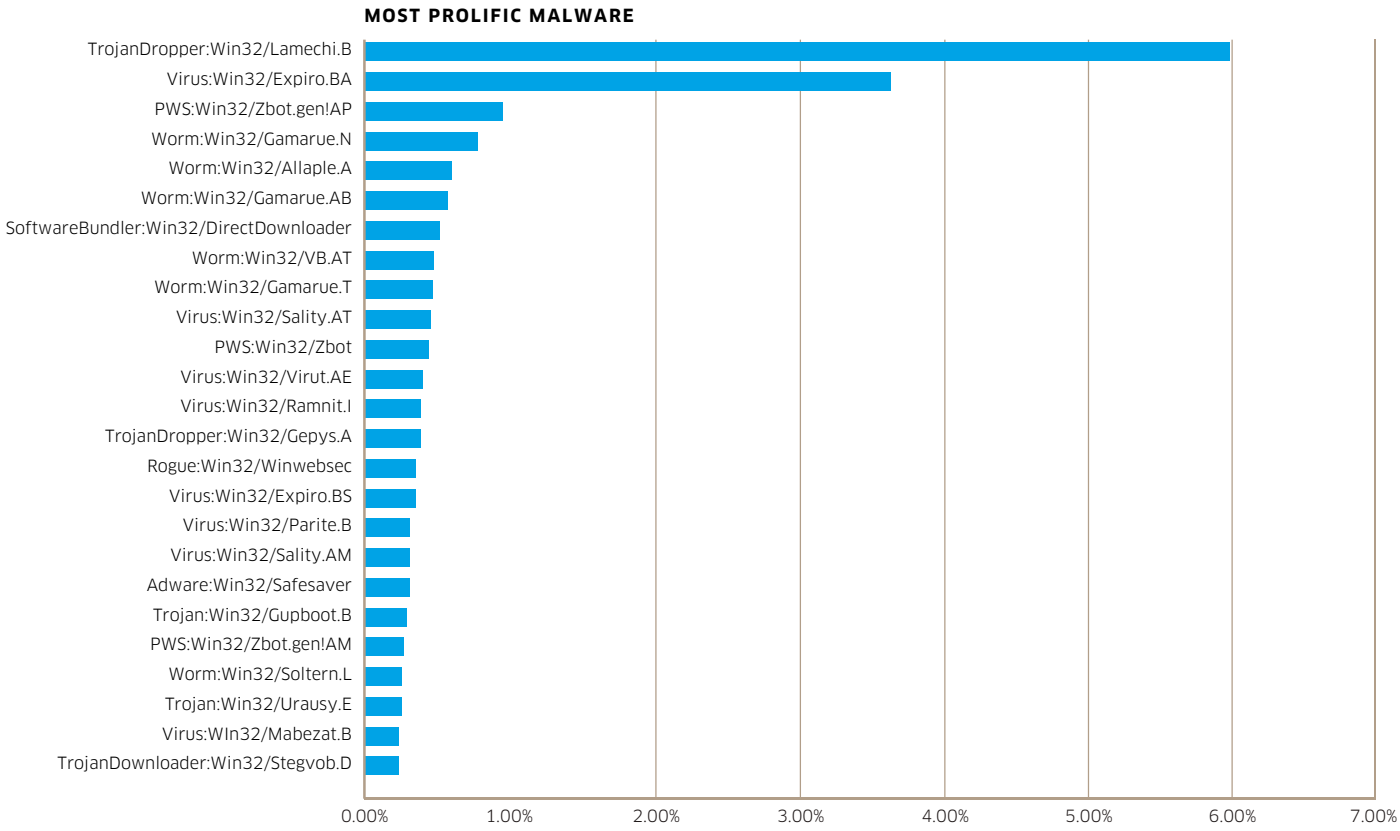

Name: Win32.Alureon.DX
ID: 511063001
Signature State: Active
Type: Bot
Class: Cybercrime
Level: High

MAP: WIN32.BOT.ALUREON.DX



## TOP 25 MOST PROLIFIC THREATS

The chart below shows the top 25 most prolific malware threats found on the Internet. The order is based on the number of distinct samples we have captured from the Internet at large. Finding a large number of samples indicates that the malware distribution is extensive and that the malware author is making a serious attempt to evade detection by antivirus products.




This quarter we saw a large number of samples of Lamechi.B and Expiro.BA. Lamechi.B is a weird one. When executed it drops multiple copies of itself in various directories on the infected device. Each copy is slightly different, which accounts for the large number of samples. It is also reported to create a back door allowing the attacker to load additional malware onto the infected system; however we have not observed any network-based activity in the lab.

Expiro is a file-infecting virus that allows the attacker to steal passwords and other personal information and provides the attacker with remote control of the infected system. Each infected file becomes a new sample of the malware. This accounts for the large number of samples.

Samples of Gamarue continue to be seen in large numbers, but not at the same levels as last quarter, where they dominated the top 25.

# Q4 2013 MOBILE MALWARE STATISTICS

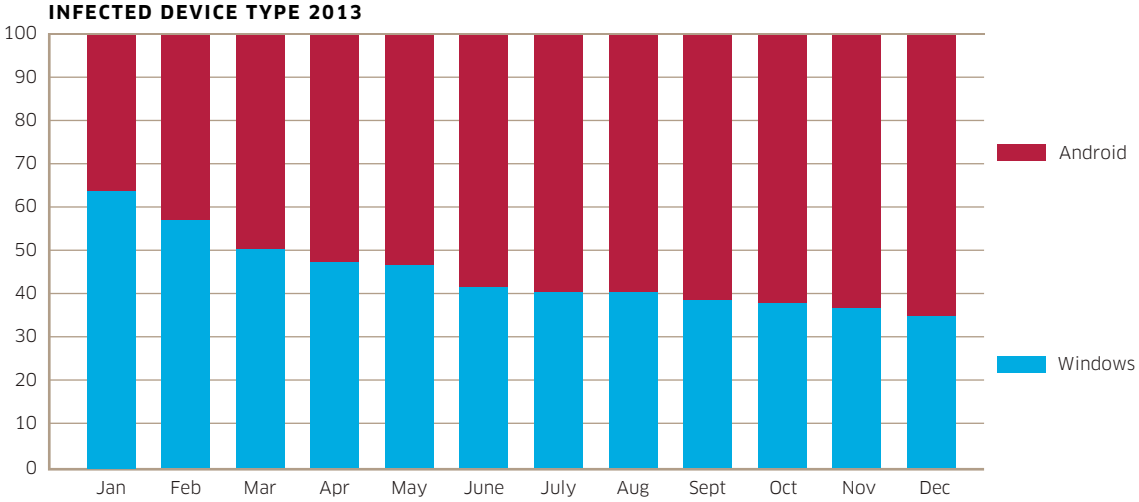
## MOBILE DEVICE INFECTION RATES

**20%**
**YEAR TO DATE IN 2013**

In mobile networks we found that 0.55% of devices were infected with high threat level malware. This is up from the 0.52% in Q2 and 0.50% in Q1. This is a 20% increase in mobile infections in 2013.

The vast majority of infected devices are either Android phones or Windows laptops tethered to a phone or connected directly through a mobile USB stick or MIFI hub. The infection rate among Android devices is actually over 1.0%.

**INFECTED DEVICE TYPE 2013**




As you can see in the chart above, Android infections are now starting to dominate. Infections on iPhone, Blackberry and other devices make up less than 1% of the infections we see in the network.

## TOP ANDROID MALWARE

The table below shows the top 20 Android malware detected in Q4 in the networks where the Kindsight Mobile Security solution is deployed.

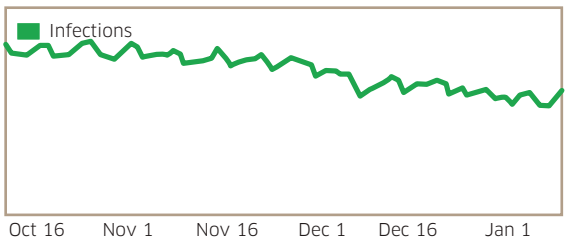
| RANK | NAME | THREAT LEVEL | % OF TOTAL | LAST QUARTER |
|---|---|---|---|---|
| 1 | Android.Adware.Uapush.A | Moderate | 52.38 | 1 |
| 2 | Android.Trojan.Coogos.A!tr | High | 16.80 | 3 |
| 3 | Android.Bot.Notcompatible | High | 9.96 | New |
| 4 | Android.Trojan.Qdplugin | High | 5.40 | 2 |
| 5 | Android.Trojan.Wapsx | High | 5.31 | 5 |
| 6 | Android.MobileSpyware.SpyBubbl | High | 2.19 | 4 |
| 7 | Android.Backdoor.Advulna | High | 1.00 | New |
| 8 | Android.MobileSpyware.SpyMob.a | High | 0.94 | 6 |
| 9 | Android.Backdoor.Ikangoo | High | 0.66 | 9 |
| 10 | Android.Trojan.Phonerecon.A | High | 0.54 | 7 |
| 11 | Android.Adware.Kuguo.A | Moderate | 0.25 | 8 |
| 12 | Android.Trojan.CoolPaperLeak | High | 0.21 | New |
| 13 | Android.MobileSpyware.Spyoo | High | 0.15 | 11 |
| 14 | Android.Bot.SmsSend | High | 0.13 | 16 |
| 15 | Android.Backdoor.Fakeinst | High | 0.10 | New |
| 16 | Android.MobileSpyware.MobileSp | Moderate | 0.08 | 10 |

| RANK | NAME | THREAT LEVEL | % OF TOTAL | LAST QUARTER |
|---|---|---|---|---|
| 17 | Android.Adware.BatteryDoctor.F | Moderate | 0.06 | 14 |
| 18 | Android.Trojan.Opfake.a | High | 0.06 | 12 |
| 19 | Android.Trojan.GGTracker | High | 0.06 | 15 |
| 20 | Android.Adware.ImadPush.A | Moderate | 0.05 | 17 |

For the most part these are all “trojanized” apps that steal information about the phone or send SMS messages, but the list also includes banking Trojans that intercept access tokens for banking web sites and spyware applications that are used to spy on family members or associates.

## TOP MOBILE THREATS

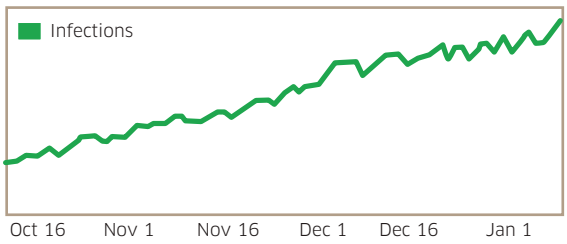
**Uapush.A** is a moderate threat level Android adware Trojan that also sends SMS messages and steals information from the compromised device. Activity on this increased steadily since in the first half of the year, but has been slowly dropping off in Q4. The malware has its web-based C&C site located in China.




Name: Android.Adware.Uapush.A
Signature ID: 2805862
Signature State: Active
Type: Adware
Class: Spyware
Level: Moderate

MAP: ANDROID.ADWARE.UAPUSH.A

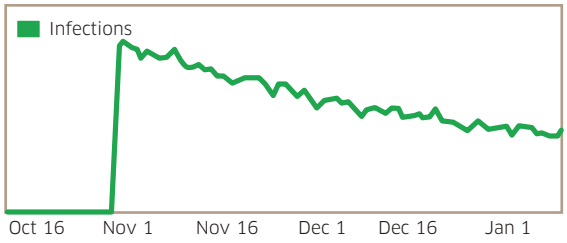

**Coogos.A!tr** is a Trojan for Android devices. It checks whether the victim’s device is rooted, and will silently and automatically download a system package onto the device. Additionally, it posts device’s identifier (IMEI) and victim’s identifier (IMSI) to a remote web server in China. This malware typically poses as active wallpaper for Android devices. Activity has increased significantly in Q4.




Name: Android.Trojan.Coogos.A!tr
Signature ID:2805902
Signature State:Active
Type:Trojan
Class:Identity Theft
Level:High

MAP: ANDROID.TROJAN.COOGOS.A!TR

**NotCompatible** is an Android bot that uses the infected phone to provide anonymous proxy web browsing services. This can consume large amounts of bandwidth and airtime, as the phone serves as a proxy for this illicit web browsing activity. The C&C is located in Germany and Holland. The C&C protocol is the same as a Windows-based web proxy bot. This is the first time we've seen a common C&C protocol between Windows and Android malware. The detection signature was introduced in late October. Activity has been declining throughout Q4.




Name: Android.Bot.Notcompatible
Signature ID: 513102890
Signature State: Active
Type: Bot
Class: Cybercrime
Level: High

MAP: ANDROID.BOT.NOTCOMPATIBLE


# CONCLUSION

On the fixed residential side, the malware infection situation is relatively stable. We have seen a consistent infection rate of around 10% throughout 2013. There was a bit of a spike in July to 13% but it returned to 10% by the end of Q3 and dropped to 9% by the end of the year. Our statistics continue to show that roughly 6% of homes are infected with a high threat level variety of malware such as a bot, rootkit or banking Trojan.

On the mobile front, infection levels increased 20% in 2013, with the average infection rate for Q4 at 0.55%. Extrapolating from this gives about 11.6 million infected mobile devices worldwide. About 60% of the infected mobile devices are Android phones, with the remaining 40% being mostly Windows computers that are tethered to the mobile network. Less that 1% of the infections are from other devices such as iPhones, BlackBerrys and Windows Phones. The number of Android malware samples in our database increased 20 fold in 2013, doubling in Q4.

The major threat continues to be from botnets, with ZeroAccess, Zeus and Alureon in the top three positions. ZeroAccess is still number one despite actions by Symantec and Microsoft to disrupt its operation. Its ad-click fraud operation appears to have been effectively disabled by Microsoft's activities.

# TERMINOLOGY AND DEFINITIONS

This section defines some of the terminology used in the report.

| TERM | DEFINITION |
|---|---|
| Advanced Persistent Threat (APT) | A targeted cyber-attack launched against a company or government department by professional hackers using state of the art tools, usually with information theft as the main motivation. |
| Infection Vector | The mechanism used to infect a computer or network device. For example, in Windows computers the most popular infection vector is web based exploit kits whereas on the Android phone it is Trojanized applications. |
| Bot | An infected computer that is part of a botnet. A botnet is a network of infected computers that controller remotely via the Internet by cyber-criminals. Botnets are used for sending spam e-email, ad-click fraud, distributed denial of service attacks, distributing additional malware, bitcoin mining and a variety of other purposes. |
| Root-kit | A malware component that compromises the computer's operating system software for the purposes of concealing the malware from anti-virus and other detection technologies. |
| Trojans | Computer programs or applications that look fine on the surface, but actually contain malware hidden inside. From the term Trojan Horse. |
| High/Moderate threat level | Kindsight splits malware into High and Moderate threat levels. High is any threat that does damage, steals personal information or steals money. A moderate threat is one that does no serious damage, but will be perceived by most as annoying and disruptive. |
| Ad-click fraud | Advertisers pay money, typically a few cents, when someone clicks on a Web based advertisement. Ad-click fraud is when someone uses software to fake these ad clicks and collect money from the advertisers for the fake clicks. Typically the ad-click software is packages as malware and distributed through a botnet that is controlled by cyber-criminals who make money from the ad-click fraud. |
| Bitcoin mining | Bit-coins are a form of virtual cyber currency that can be created through complex arithmetic calculations that take a lot of computing power to perform. The process of executing these calculations to generate new bitcoins is referred to as bitcoin mining. Cyber-criminals use large botnets to efficiently generate new bitcoins. |

# ABOUT KINDSIGHT SECURITY LABS

Kindsight Security Labs focuses on the behavior of malware communications to develop network signatures that specifically and positively detect current threats. This approach enables the detection of malware in the service provider network and the signatures developed from the foundation of Kindsight Security Analytics and Kindsight Security Services.

To accurately detect that a user is infected, our signature set looks for network behavior that provides unequivocal evidence of infection coming from the user's computer. The following are examples of such behavior:

- Malware C&C communications
- Backdoor connections
- Attempts to infect others (for example, exploits)
- Excessive e-mail
- DoS and hacking activity

There are four main activities that support our signature development and verification process.

1. Monitor information sources from major security vendors and maintain a database of currently active threats.
2. Collect malware samples (>10,000/day), classify and correlate them against the threat database.
3. Execute samples matching the top threats in a sandbox environment and compare against our current signature set.
4. Conduct a detailed analysis of the malware's behavior and build new signatures if a sample fails to trigger a signature

As an active member of the security community, Kindsight Security Labs also shares this research by publishing a list of actual threats detected and the top emerging threats on the Internet and this report.

Kindsight™

www.alcatel-lucent.com/solutions/kindsight-security


NP2014014064EN (January)

Alcatel·Lucent