Kindsight™

Malware Report

Q3 2012

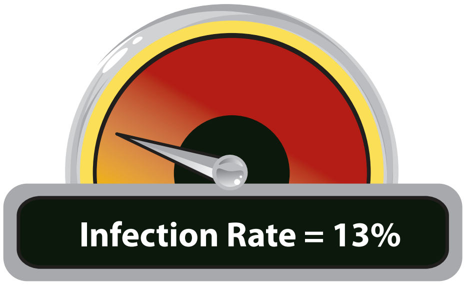
Kindsight Security Labs

Kindsight Security Labs Malware Report – Q3 2012

Contents

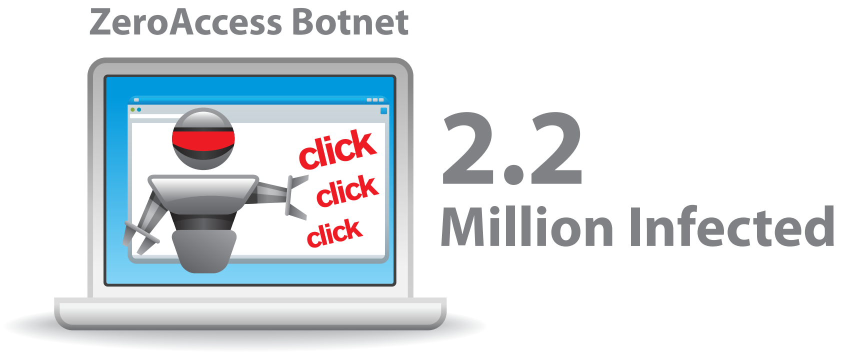
Introduction

The Kindsight Security Labs Q3 2012 Malware Report examines general trends for malware infections in home networks or infections in mobile devices and computers connected through mobile adapters. The data in this report is aggregated across the networks where Kindsight solutions are deployed.



Q3 2012 Highlights

- 13% of home networks were infected with malware in Q3/2012, that's down slightly from the 14% reported in the previous quarter.
- 6.5% of broadband customers were infected with high-level threats such as a bots, root-kits, and banking Trojans.
- ZeroAccess was the most active botnet in Q3. We estimate that there are over 2 million infected users worldwide with 685,000 in the United States alone.
- These bots are engaged in a sophisticated ad-click fraud scheme that each day generates about 140 million fraudulent ad-clicks and 260 terabytes of network traffic. ZeroAccess could be costing advertisers $900,000 per day.
- Android adware is on the rise and being distributed via Google Play. It accounts for 90% of the 3+% infection rate among mobile devices.



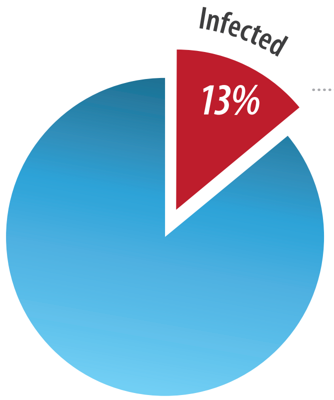
Q3 2012 Home Malware Statistics

Home Network Infection Rates

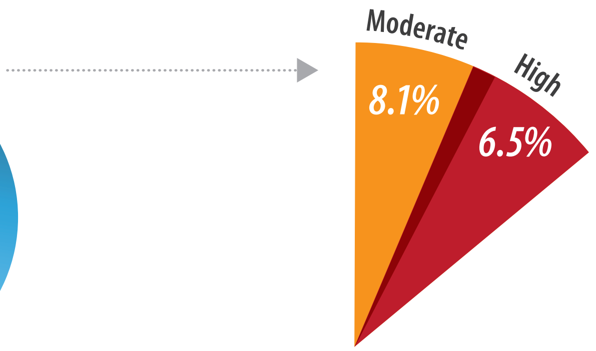
In fixed broadband deployments in Q3 2012 we found that 13% of residential households show evidence of malware infection. This has slightly decreased from 14% in Q2. 6.5% of households were infected by high-level threats such as a botnet, rootkit or banking Trojan. 8.1% of households were infected with a moderate threat level malware such as spyware, browser hijackers or adware. Some households had multiple infections including both high and moderate threat level infections.

Infection Methods

The main infection method is through malicious web sites running exploit kits such as Blackhole. When a victim lands there, it will probe their computer and attempt to infect it. Once the infection process is successful, the kit generally installs a rootkit botnet such as Alureon or ZeroAccess which is then used to coordinate additional malware activity. In some cases it will directly download fake anti-virus software, a spambot or a banking Trojan like Zeus or SpyEye. The victim is attracted to these malicious web sites either by offers of free services (sometimes of a dubious nature) or by spam e-mail messages luring victims to these sites. The victim will typically receive an e-mail message from a business or some level of government (the tax department is a good candidate) informing them of an issue with their account. It will contain a reasonable looking link a web site, which would unfortunately contain the exploit kit. It is also quite common to find malware embedded in a spam attachment.



Home Networks Infected with
Malware



Division of Infections 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.

Position	Name	Threat Level	% of Total	Last Quarter
1	Botnet.ZeroAccess	High	17.0%	9
2	Botnet.ZeroAccess2	High	11.9%	9
3	Adware.GameVance	Moderate	10.5%	4
4	Spyware.MyWebSearchToolbar	Moderate	9.4%	1
5	Backdoor.TDSS	High	5.4%	8
6	Spyware.SCN-ToolBar	Moderate	3.7%	2
7	Trackware.Binder	Moderate	2.9%	15
8	Adware.MarketScore	Moderate	2.7%	6
9	Hijacker.StartPage.KS	Moderate	2.7%	3
10	Botnet.Alureon.A	High	2.4%	13
11	Downloader.Agent.TK	High	2.3%	10
12	Hijacker.MyWebSearch	Moderate	1.7%	1
13	BankingTrojan.Zeus	High	1.4%	12
14	Trojan.Medfos.A	High	1.4%	20
15	MAC.Bot.Flashback.K/I	High	1.3%	5
16	Backdoor.Hupigon.FI	High	1.2%	-
17	Spyware.SBU-Hotbar	Moderate	0.8%	11
18	Adware.iBryte.B	Moderate	0.8%	-
19	Trojan.Obvod.K	High	0.8%	-
20	Downloader.Ponmocup.A	High	0.7%	19

Top High Level Threats

The table shows the top 20 high threat level malware that leads to identity theft, cybercrime or other online attacks. We'll look at the significant ones in more detail below.

Position	Name	% of Total	Last Quarter
1	Botnet.ZeroAccess	27.6%	2
2	Botnet.ZeroAccess2	19.3%	2
3	Backdoor.TDSS	8.8%	4
4	Trojan.Alureon.A	3.8%	7
5	Downloader.Agent.TK	3.7%	5
6	BankingTrojan.Zeus	2.4%	6
7	Trojan.Medfos.A	2.2%	14
8	MAC.Bot.Flashback.K/I	2.2%	1
9	Backdoor.Hupigon.FI	2.0%	-
10	Trojan.Obvod.K	1.3%	-
11	Downloader.Ponmocup.A	1.2%	13
12	Virus.Sality.AT	0.9%	12
13	Backdoor.Hupigon.DZ	0.7%	-
14	Trojan.Riskware/Installbrain	0.6%	-
15	Trojan.DNSchanger	0.5%	8
16	Trojan.Piptea.J/Cutwail	0.4%	-
17	Backdoor.Cycbot.B	0.4%	17
18	Trojan.Proxyier.qk	0.4%	18
19	Generic.Spambot	0.4%	19
20	Backdoor.Blackhole	0.4%	-

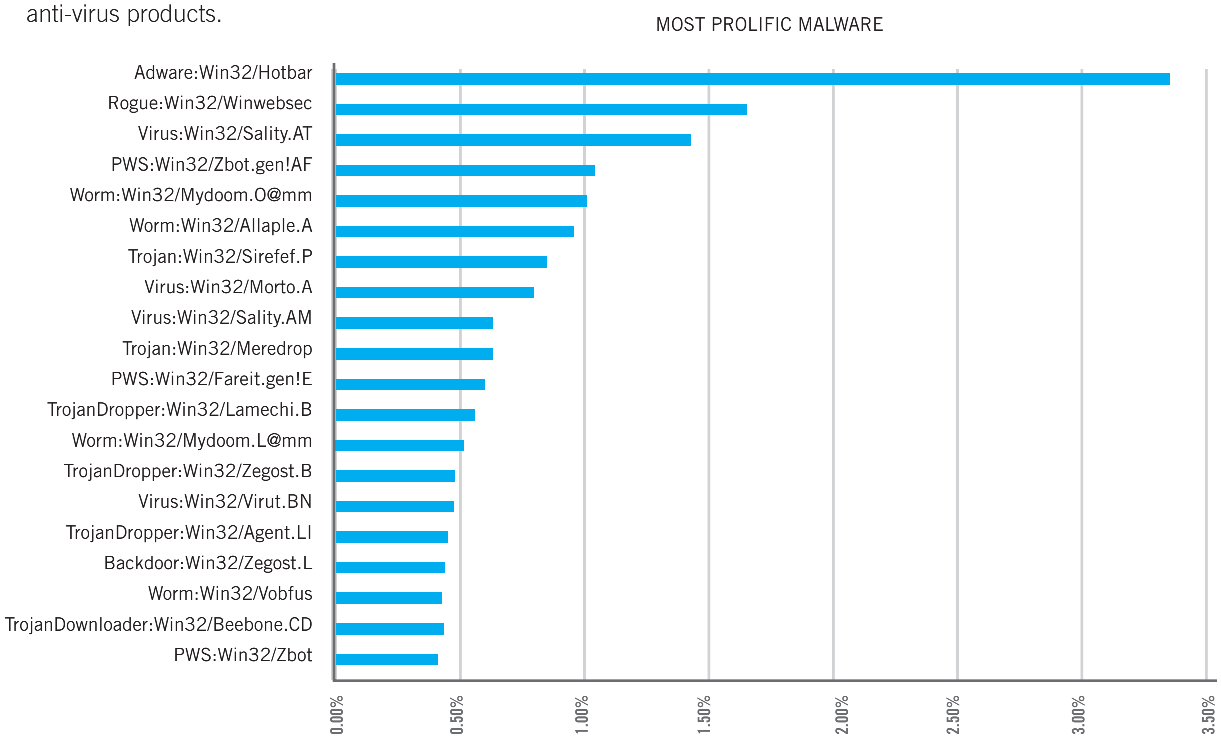
The two different versions of the **ZeroAccess** ad-click botnet head the list. These bots are engaged in a sophisticated ad-click fraud scheme that could be costing advertisers almost a million dollars each day. They also earn money through “Bitcoin mining”. Details on both these activities are provided later in the document.

The **TDSS** and **Alureon** rootkits continue to be near the top of the high threat list. These provide the attacker with a secure platform to load additional malware to monetize their botnet and are often associated with subsequent spambots, banking Trojan and identity theft infections. More details on these are also provided later in the document. The **Zeus** banking Trojan is still very active and is now leveraging peer-to-peer technology for command and control. The Mac **Flashback** bot has dropped to number 8 and **DNSchanger** is still present, but in a reduced role at number 15.

New to the top 20 list this quarter are two new versions of **Hupigon**, a bot featuring backdoor access and **Obvod**, a Trojan downloader. A new version of the **Cutwail** spambot also appeared.

Top 20 Internet Threats

The chart below shows the top 20 most prolific malware 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 anti-virus products.



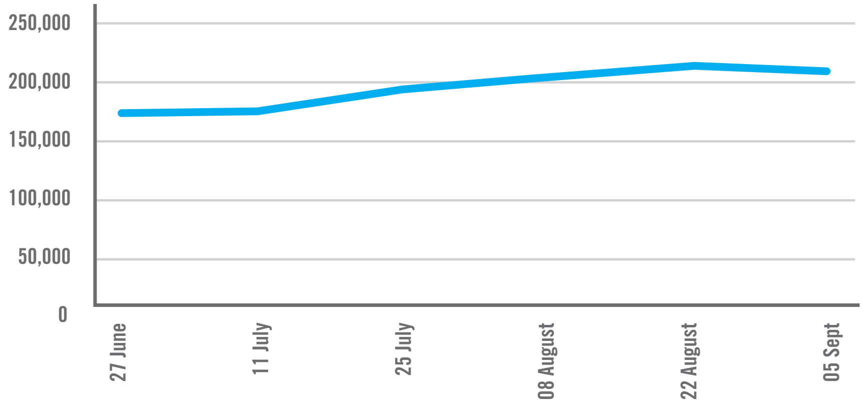
New Developments in Q3

ZeroAccess

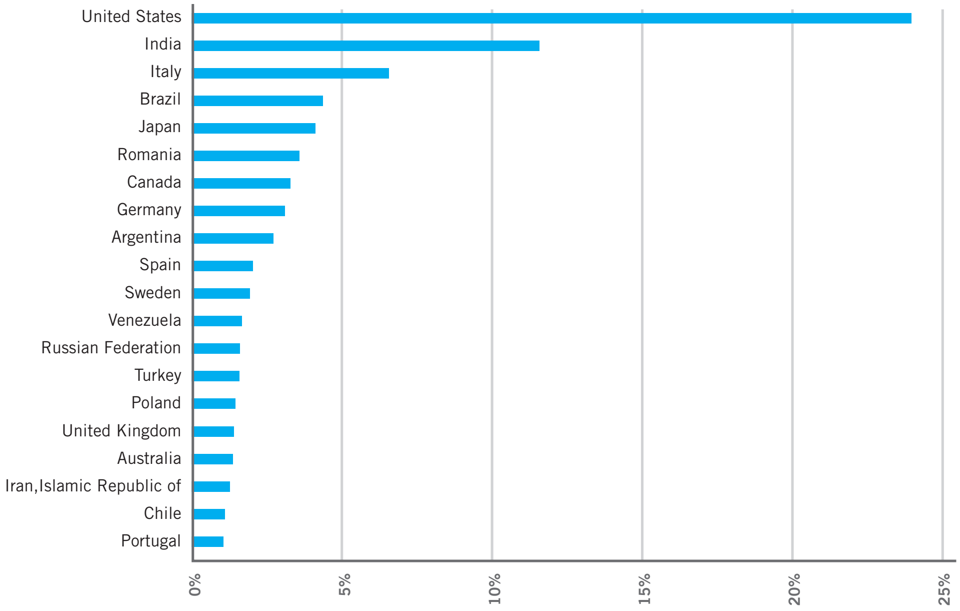
ZeroAccess continues to be the most active botnet in 2012. The main purpose of the botnet is to distribute malware responsible for a massive ad-click fraud campaign. One version also makes money through "Bitcoin mining". In February, we published a detailed analysis of its network behavior and the encrypted p2p protocol it uses to communicate with its peers. In Q2 the bot morphed (ZeroAccess2), changing its infection process and C&C protocol. A detailed description of the new C&C protocol can be found in "New C&C Protocol for ZeroAccess/Sirefef". Both versions of the bot are currently active.

ZeroAccess uses a peer-to-peer command and control protocol, where infected hosts maintain communication through super-nodes. A "super-node" is an infected host that is directly connected to the internet without an intervening home router or other network address translation (NAT) device. The Kindsight network-based malware detection technology is able to detect and map these super-nodes. The chart below shows the number of super-nodes for ZeroAccess2 detected during Q3.

ZEROACCESS2: SUPERNODES JULY - SEPT 2012



On any given day we detected communications with about 200,000 super nodes. The geographic distribution of these is shown in the chart below.



ZERO ACCESS SUPERNODES BY COUNTRY

Size of ZeroAccess Botnet

We have also monitored the percentage of households that are infected on a daily basis in a number of service providers in North America. On average this has been consistently at about 0.8% each day during Q3. Based on this we can estimate the size of the Botnet. There are a number of ways to approach this.

Based on the observed North American infection rate of 0.8% and an estimate of the number of broadband users in the United States (see Wikipedia), we can easily calculate that there are likely 685K infected households in the United States alone. If the same infection rate (0.8%) is applied to the top twenty countries hosting super nodes (table above) this gives a world-wide total of 2.21 million infected households. If we assume the international ratio of infected computers to super nodes is roughly the same as observed in North America , we come out to about 2.27M infected home networks.

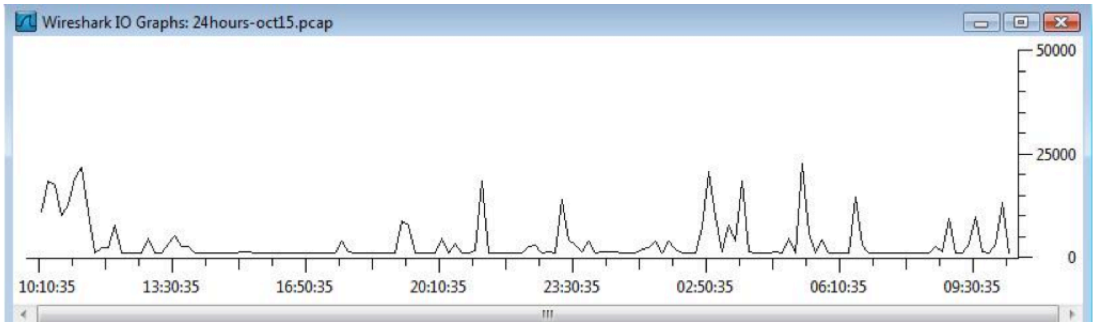
These figures are estimates of course, but they are based on two independent measurements and we can confidently say that on any given day there are at least 2.2 million active ZeroAccess bots on the Internet.

Ad-click Fraud

ZeroAccess earns money through ad-click fraud. The bot operators or their business associates have registered a large number of web sites that host pay per click advertisements. These sites are built around some standard templates that provide a search interface, display ads and offer domain names for sale. The bots are programmed to click on ads that are hosted by these sites. When the ad is clicked the owner of the web site is paid for the click.

The bots visit a C&C server periodically and are given a list of ads to click. This allows the C&C server to dynamically control which ads are chosen, how frequently they are clicked and which bots are used. Advertisers and ad networks have sophisticated mechanisms in place to detect ad-click fraud, so the C&C server balances the load between bots to make the clicking behavior look very realistic. To enhance the realism and make the clicks look like they are from a real person, the bots are programmed to follow the ad-click through to the advertiser's landing page through several layers of redirection, loading all the html, java-script and graphics components as would a regular browser. This also consumes significant bandwidth as can been seen below.

We monitored a bot for a 24 hour period to see how the clicking behavior varied over time and to get an idea of the scale of this ad-click fraud. The chart below shows the network activity starting at 10:00am and running over night to the next day.



The activity varies during the day (and night) as would be expected from a real user. In this case, in the 24 hour period, the bot clicked on 140 ads, resulting in 262MBytes of network traffic. Only half of the bots are used for ad-click fraud (the rest are used for Bitcoin mining), so if our test case is typical, then each day about one million ZeroAccess bots are responsible for fraudulently clicking on about 140 million advertisements and generating around 260 Terabytes of network traffic.

The actual dollar value of the fraud is very difficult to estimate. The ad networks use sophisticated algorithms to detect fraudulent clicks and will not charge these to the advertisers. The offending web sites will be blacklisted once the abuse is detected. In 2007 Google reported that about 10% of ad-clicks were detected as fraudulent and never charged to the advertiser and that only 0.02% of fraudulent clicks got through their filters. However, this bot is also very sophisticated and goes to great lengths to make the clicks look legitimate. The ad-click algorithm observed in this lab test is the third variation we've seen since we first observed ZeroAccess in late 2011, so the bot operators are obviously honing their skills and adapting.

We asked an Internet advertising expert to have a look at the network traffic generated by our 24 hour trial. They found that 18 out of the 140 clicks would likely have resulted in the advertiser paying for the click. Based on this analysis, the botnet could be costing advertisers $900,000 per day in ad-click fraud if we assume a low-end cost per click (CPC) of $0.05.

Bitcoin Mining

The other way ZeroAccess makes money for its operators is through Bitcoin mining. A "Bitcoin" is a form of electronic currency invented in 2009 that is managed through a peer-to-peer network. Bitcoin transactions are confirmed by complex computations that are very difficult and time consuming to perform. "Bitcoin miners" are computers that solve these computations and are rewarded in Bitcoins. About half of the ZeroAccess bots are cooperating as a Bitcoin mining pool to solve these computations and earn Bitcoins. Bitcoins are supposedly worth about $10 each and Sophos has estimated that ZeroAccess could be earning over $2.7M per year, but it is unclear if actual money is really involved, or if they are just playing a Bitcoin futures game.

TDSS/Alureon

The second most active botnet in Q3 2012 was the TDSS/Alureon family, also known as TDL-4. This is a rootkit bot that buries itself in the master boot record of the infected computer and uses various stealth techniques to hide itself from traditional antivirus software. It even goes so far as to remove competing malware from the infected computer. This provides the attacker with a secure platform to load additional malware to monetize their botnet and it is often associated with subsequent spambots, banking Trojan and identity theft infections. In the past some security experts have said that this bot is practically indestructible, although this did cause some debate.

In July a new variant was discovered that uses a domain name generation algorithm to establish its command and control network. This variant was reported to have infected at least a quarter of a million computers including computers at 9% of Fortune 500 companies. In addition to its traditional role in malware distribution, this new variant was also observed to be using ad-click fraud to make money for its operators.

Q3 2012 Mobile Malware Statistics

Mobile Device Infection Rates

In mobile networks we found that 0.3% of devices were infected with high-level threats. The infected devices include Android phones and laptops tethered to a phone on connected directly through a mobile USB stick/hub. The infection rate is low because the total device count includes a large number of feature phones that are not malware targets. However, we saw a 165% increase in the number of Android malware samples.

Top Android Malware

The table below shows the top Android malware detected in the networks where the Kindsight Mobile Security solution is deployed. The following table shows the top 10 Android infections of Q3.

Position	Name	% of Total	Last Quarter
1	Trojan.GGTracker	31.8%	1
2	Spyware.MobileSpy	26.8%	3
3	Trojan.Wapsx	13.5%	-
4	Trojan.MMarketPay.a	5.8%	-
5	Trojan.Pjapps3.A	4.5%	2
6	Spyware.FlexiSpy	4.2%	8
7	BankingTrojan.FakeToken	3.7%	6
8	Trojan.Tonclank	2.6%	-
9	Trojan.Opfake.bo	1.8%	-
10	DroidDream	1.6%	4
11	Trojan.Anserver.A	1.1%	-
12	Adware.SndApp.B	1.1%	-
13	Trojan.PJAPPS.A	0.7%	-
14	Dogowar	0.02%	-
15	Trojan.Kmin.A	0.01%	-

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

Mobile Adware

In January 2012 there was industry discussion about whether the Plankton/Apperhand advertising SDK from StartApp should be classified as malware or not. At the time, the consensus was that it was “aggressive adware” and not really malware. Many anti-virus vendors stopped detecting it as malware and the apps were made available on Google Play.

In Q3 2012 some new players have been active offering even more aggressive advertising using techniques such as push notifications and home screen icons to deliver their message. Previously ad-funded applications restricted their advertising to when the user was actually using the application. With push notification and home screen icons, the advertising shows up even when the app is not being used. Users are often unaware of the source of these messages and find it very difficult to get rid of them.

The security industry has responded by creating “Adware Detector” applications that detect and remove the offending applications. This parallels the past development of anti-spyware applications for the Windows platform to catch the adware and browser hijackers that traditional Windows anti-virus products missed. One key difference between these ad-funded Android apps and the traditional Window’s variety, is that the Android variety is being distributed from the Google Play App Store, which lends them considerable legitimacy.

To get a handle on the extent of the problem and monitor its growth, Kindsight introduced some signatures to detect these apps. The results show that about 3% of mobile devices have applications that are using this adware.

Conclusion

In this report the overall infection rate dropped slightly from 14% to 13%. ZeroAccess continued its upward trend and is now the top Botnet with 2.2 million active bots. It earns its keep through ad-click fraud and “Bitcoin” mining. The ad-click fraud alone could be costing advertisers a million dollars a day. Malware operators continue to focus on stealth and financial gain using rootkits such as Alureon and TDSS to establish secure platforms for cybercriminal activity. Spam, ad-click fraud, banking Trojans, identity theft and fake security software continue to be the big money makers. There are even fake anti-virus apps for Android now.

On the mobile front, we have seen growth in spyware apps and some additional malware, however there have not been any major malware outbreaks. We have seen significant growth in apps funded by various advertising techniques, some bordering on what has been traditionally called adware. Some security vendors have created apps which will detect and remove this adware, but the jury is still out on whether these aggressive advertising techniques should be considered malicious.

About Kindsight Security Labs

Kindsight Security Labs focuses on the behavior of malware communications to develop network signatures that positively and specifically detect current threats. This approach enables the detection of malware in the service provider network and the signatures developed form 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 device. This includes:

- Malware command and control (C&C) communications
- Backdoor connections
- Attempts to infect others (e.g. exploits)
- Excessive e-mail
- Denial of Service (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, Inc
755 Ravendale Drive, Mountain View, CA 94043 U.S.A
555 Legget Drive, Tower B, Suite 132, Ottawa, ON K2K 2X3 Canada

T: +1.650.969.7770
info@kindsight.net
www.kindsight.net