KINDSIGHT SECURITY LABS MALWARE REPORT – H1 2014

Alcatel·Lucent

TABLE OF CONTENTS

INTRODUCTION

The Kindsight Security Labs H1 2014 Malware Report examines general trends and statistics for malware infections in devices connected through mobile and fixed networks. The data in this report is aggregated across the networks where Kindsight network-based malware detection solutions are deployed.

Generally speaking, Kindsight Security Labs found that increasingly applications are spying on device owners, stealing their personal information and pirating their data minutes causing bill shock. It can go beyond an invasion of privacy to putting individuals, companies and even governments at risk of unknowingly surrendering personal, confidential and financial information. At the very least it is an annoyance for end users that can lead to sub par performance of their devices.

H1 2014 HIGHLIGHTS

- On the mobile side, infections continue to accelerate, with an increase of 17 percent in the first half of 2014, compared with 20 percent for the whole of 2013. The infection rate is currently at 0.65 percent. Based on this, we estimate that, worldwide, about 15 M mobile devices are infected by malware. Of these, 60 percent are Android smartphones
- Mobile spyware is definitely on the increase. Four of the newcomers to mobile malware top 20 list are mobile spyware. These are apps that are used to spy on the phone's owner. They track the phone's location, monitor ingoing and outgoing calls and text messages, monitor e-mail and track the victims' web browsing.
- The overall residential infection rate in fixed broadband networks jumped from an all-time low of 9 percent in December 2013 to 18 percent at the end of June 2014. This increase is mostly attributable to moderate-threat-level adware infections, that went from 5 percent in Q4 2013 to 13 percent in Q2 2014. Seven percent of broadband residential customers are infected with high-level threats such as a bots, root-kits and banking Trojans. This is up from 5 percent in Q4 2013.

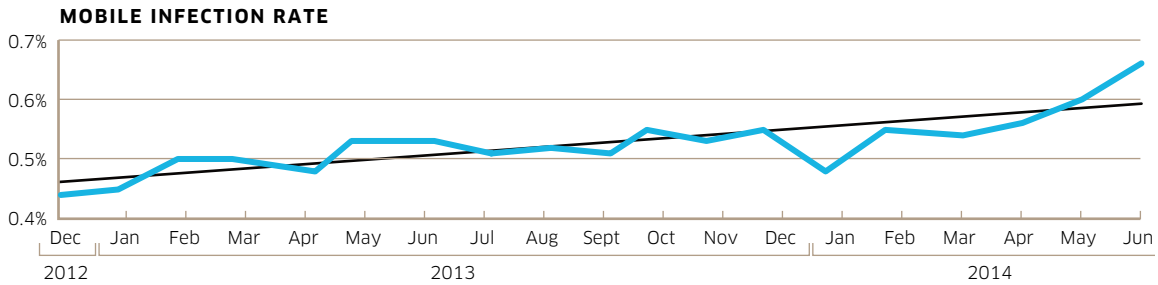
MOBILE MALWARE

H1 2014 saw some significant developments in mobile malware. The overall mobile infection rate climbed to 0.65 percent. The number of Android malware samples continued to grow significantly, but not at the exponential rates seen in 2013.

MOBILE INFECTION RATE

Figure 1 shows the percentage of infected mobile devices observed on a monthly basis since December 2013. This data is averaged from actual mobile deployments. The overall slope indicates an annual growth rate of 20 percent, but in the first half of 2014, the growth was almost double that.

FIGURE 1. MOBILE INFECTION RATE SINCE DECEMBER 2013



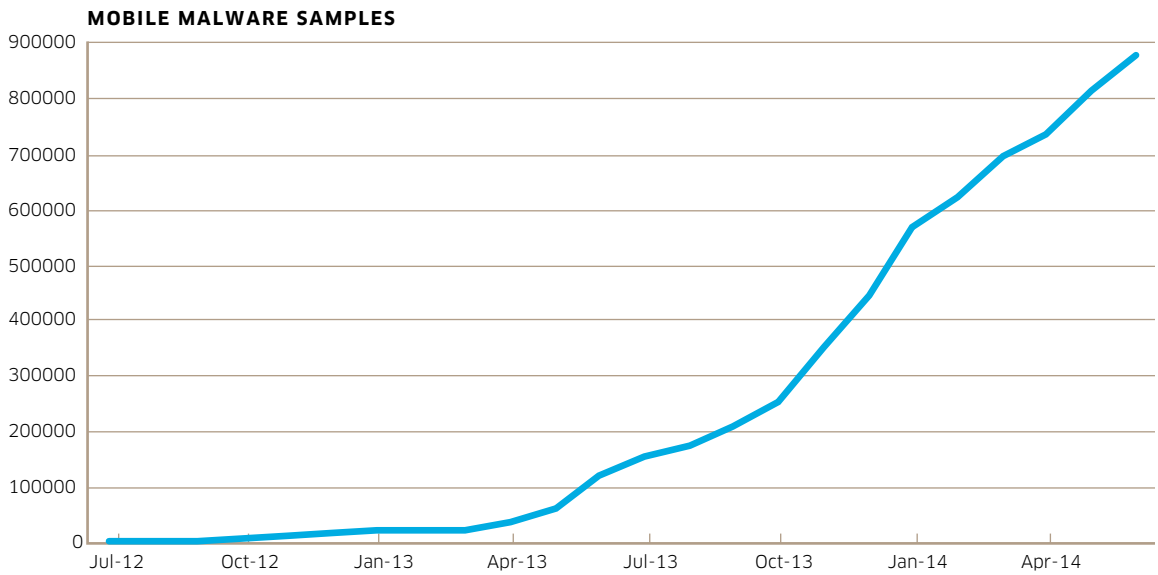
With an overall infection rate 0.65 percent, we estimate that around 15 million mobile devices are infected worldwide at any time, since the ITU estimates that there are currently 2.3 billion smartphones.

Because Alcatel-Lucent sensors are not currently deployed in areas where infection rates are known to be higher than average, such as China and Russia, our global estimate is probably on the conservative side.

ANDROID MALWARE SAMPLES CONTINUE GROWTH IN H1 2014

An indicator of Android malware growth is the increase in the number of samples in our malware database. Figure 2 shows numbers since June 2012. The number of samples grew by 83 percent in H1 2014.

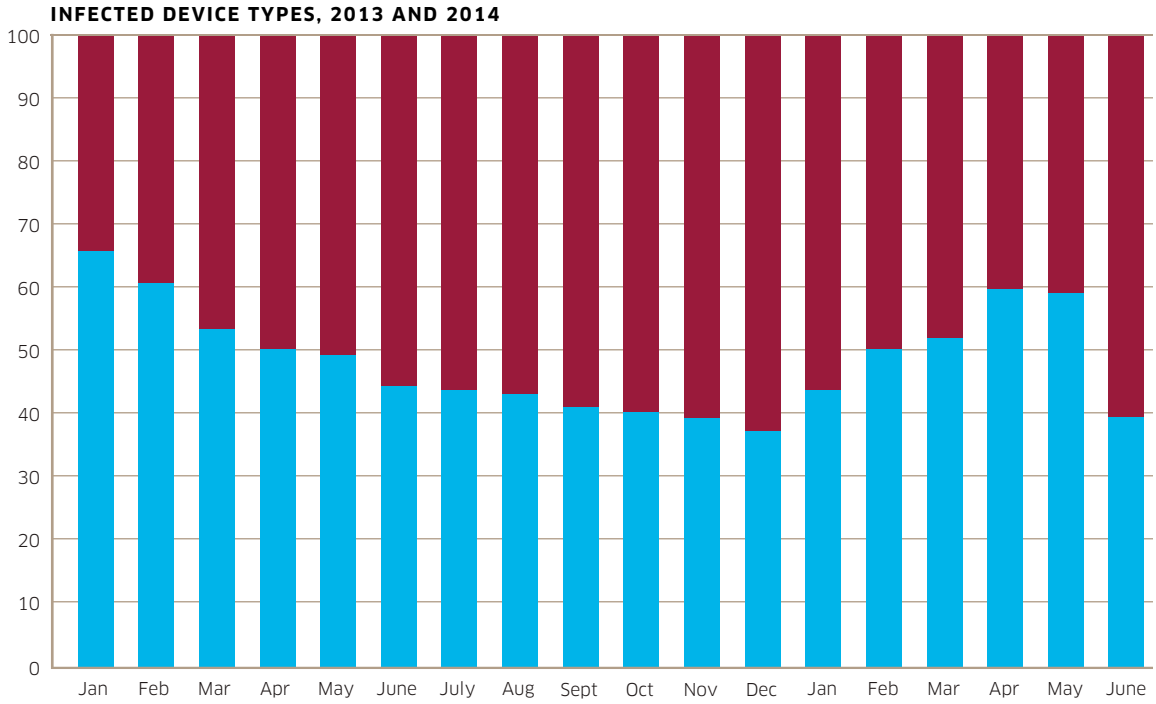
FIGURE 2. MOBILE MALWARE SAMPLES SINCE JUNE 2012



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 mechanisms (C&C) 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.

ANDROID AND WINDOWS PC BIGGEST OFFENDERS

FIGURE 3. INFECTED DEVICE TYPES IN 2013 AND 2014



- 60 percent of infected devices are Android.
- 40 percent are Windows PCs connected to the mobile network.
- Less than 1 percent of devices are iPhones, Blackberrys, Symbian and Windows Mobile.

Clearly the Android platform is the biggest malware target in the mobile space, followed by Windows PCs, which are still the favorite of hard-core professional cybercriminals.

Currently, most mobile malware is distributed as Trojanized apps, and Android offers the easiest target for this approach, because of Android's lenient security measures on the handling of apps. Specifically:

- Apps can be downloaded from third-party app stores and web sites.
- There is no control of the digital certificates used to sign Android apps. Apps are usually self signed and can't be traced to the developer.

TOP ANDROID MALWARE

Table 1 shows the top 20 Android malware we have detected in H1 2014.

TABLE 1. TOP 20 ANDROID MALWARE DETECTED IN H1 2014

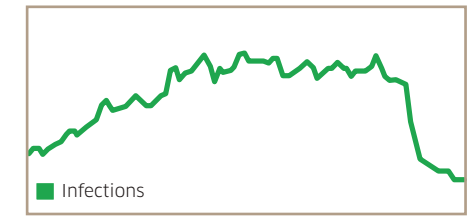
RANK	NAME	THREAT LEVEL	% OF TOTAL	LAST QUARTER
1	Android.Trojan.Coogos.A!tr	High	35.69	2
2	Android.Adware.Uapush.A	Moderate	30.45	1
3	Android.MobileSpyware.SmsTracker	High	7.25	New
4	Android.Trojan.Sms.Send.B	High	7.13	New
5	Android.Bot.Notcompatible	High	4.24	3
6	Android.MobileSpyware.Ackposts	High	4.12	New
7	Android.Trojan.Qdplugin	High	1.63	4
8	Android.Trojan.Wapsx	High	1.25	5
9	Android.MobileSpyware.SpyBubbl	High	1.18	6
10	Android.Backdoor.Advulna	High	0.77	7
11	Android.MobileSpyware.Boqx.a	High	0.68	New
12	Android.MobileSpyware.SpyMob.a	High	0.59	8
13	Android.Trojan.Phonerecon.A	High	0.41	10
14	Android.Backdoor.Fakeinst	High	0.35	15
15	Android.Adware.Kuguo.A	Moderate	0.18	11
16	Android.Backdoor.Ikangoo	High	0.06	9
17	Android.MobileSpyware.Spyoo	High	0.05	13
18	Android.Trojan.GGTracker	High	0.04	19
19	Android.Adware.ImadPush.A	Moderate	0.03	20
20	Android.Downloader.Morepaks	High	0.03	New

For the most part, the top 20 include "Trojanized" apps that steal information about the phone or send short message service (SMS) messages. Four of the five malware that are new to the top 20 list are in the mobile spyware category. These apps are used to spy on the phone's owner. They track the phone's location, monitor ingoing and outgoing calls and text messages, monitor e-mail and track the victims' web browsing.

TOP MOBILE THREATS

Coogos.A!tr is a Trojan for Android devices. It checks whether the victim's device is rooted, and it will silently and automatically download a system package on the device. Additionally, it posts the device's International Mobile Station Equipment Identity (IMEI) and the victim's International Mobile Subscriber Identity (IMSI) to a remote web server in China. In the past, this malware was distributed as active wallpaper, but a new version, packaged as a game, is much more popular, and it probably accounts for the significant increase in the infection rate over the first half of 2014. However, activity has just recently dropped off.

FIGURE 4. COOGOS.A!TR SUMMARY

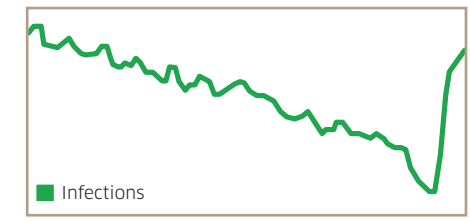


Name: Android.Trojan.Coogos.A!tr
Signature ID: 2805902
Signature State: Active
Type: Trojan
Class: Identity theft
Level: High

MAP: ANDROID.TROJAN.COOGOS.A!TR

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 malware has decreased steadily since the first half of the year, but took a sudden jump in July. The malware has its web-based C&C server located in China.

FIGURE 5. UAPUSH.A SUMMARY



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

MAP: ANDROID.ADWARE.UAPUSH.A

SMSTracker is an Android spyphone app that provides a complete, remote phone-tracking and monitoring system for Android phones. It allows the attacker to remotely track and monitor all SMS, multimedia messaging service (MMS) and text messages, as well as calls, GPS locations and browser history. The detection rule was introduced in July. This is also known as Android.Monitor.Gizmo.A.

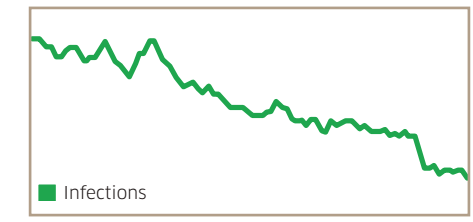
FIGURE 6. SMSTRACKER SUMMARY

Name: Android.MobileSpyware.SMSTracker
Signature ID: 2807732
Signature State: Active
Type: Spyware
Class: Identity theft
Level: High

MAP: ANDROID.TROJAN.SMSTRACKER

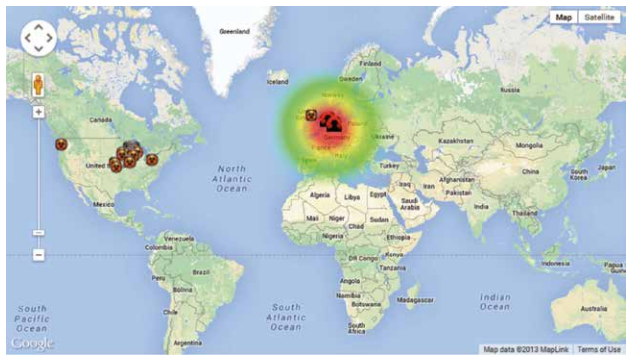
NotCompatible is an Android bot that uses the infected phone to provide anonymous proxy web-browsing services. This can consume large amounts of bandwidth and airtime, as the phone serves as a proxy for this illicit web-browsing activity. The C&C servers are located in Germany and Holland. The C&C protocol is the same used for 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 2013. Activity has been declining throughout 2014.

FIGURE 7. NOTCOMPATIBLE SUMMARY



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

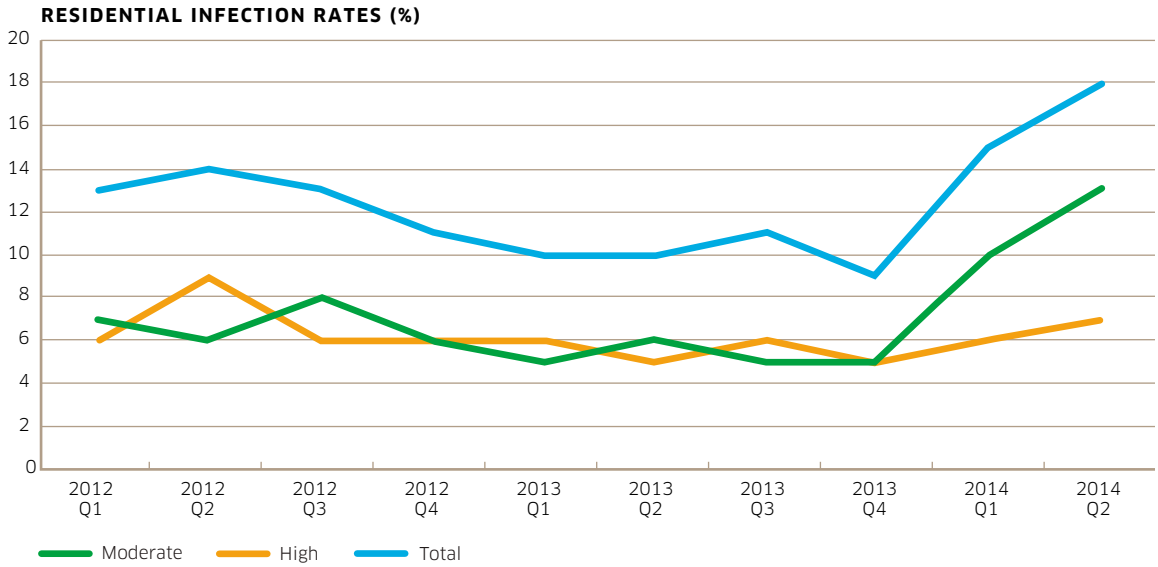
MAP: ANDROID.BOT.NOTCOMPATIBLE



RESIDENTIAL MALWARE

In the first half of 2014, the infection rates in residential networks rose significantly, as can be seen in Figure 8. The increase is almost entirely due to moderate-threat-level "adware" infections. However, there was also a slight increase in high-threat-level "botnet" infections.

FIGURE 8. RESIDENTIAL INFECTION RATES



Currently, in Q2 of 2014, 18 percent of residences had some sort of malware infection. Of these, 7 percent had a high-threat-level infection, and 13 percent had a moderate infection. (Note: The total adds up to 18 percent, not 20 percent, because 2 percent had both high and moderate infections.)

TOP 20 RESIDENTIAL NETWORK INFECTIONS

Table 2 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.

TABLE 2. TOP 20 HOME NETWORK INFECTIONS

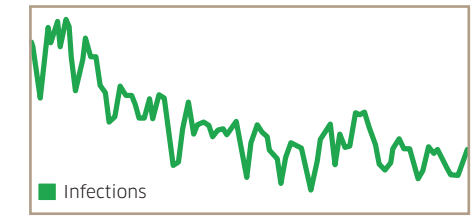
RANK	NAME	THREAT LEVEL	%	LAST QUARTER
1	Win32.Adware.iBryte	Moderate	16.95	New
2	Win32.Adware.Wajam	Moderate	9.88	1
3	Win32.AdWare.AddLyrics.T	Moderate	9.55	10
4	Win32.Adware.Wysotot	Moderate	5.74	7
5	Win32.Hijacker.StartPage.KS	Moderate	3.81	4
6	Win32.Trackware.Binder	Moderate	3.45	3
7	Win32.AdWare.Eorezo	Moderate	3.22	New
8	Win32.Bot.ZeroAccess2	High	3.17	2
9	Win32.Adware.Megasearch	Moderate	2.81	New
10	Android.Trojan.Coogos.A!tr	High	2.43	14
11	Win32.Adware.MediaFinder	Moderate	2.33	16
12	Android.Adware.Uapush.A	Moderate	1.88	9
13	Win32.BankingTrojan.Carberp	High	1.8	25
14	Win32.Adware.MarketScore	Moderate	1.78	8
15	Win32.Adware.Eorezo	Moderate	1.42	30
16	Win32.Adware.InstallMonetizer	Moderate	1.05	New
17	Win32.Backdoor.PcClient	High	1.02	New
18	Win32.BankingTrojan.Zeus	High	0.95	13
19	Win32.Downloader.Karagany.H	High	0.91	New
20	Win32.Adware.DealPly	Moderate	0.91	New

Five of the seven new entries in the top 20 list are in the adware category. These are moderate-threat-level malware that monitors web browsing and steals personal information to support targeted advertising through pop-up ads and browser redirection. In the first half of 2014, the malware infection rate doubled from 9 percent to 18 percent. Most of this increase was due to adware infections, with iBryte, Wajam and AddLyrics leading the pack.

TOP THREAT – WIN32.ADWARE.IBRYTE

iBryte is adware that installs toolbars and displays pop-up advertisements on the infected computer. It exhibits rootkit capabilities to hook deep into the operating system, making it difficult to remove. It is also a browser hijacker that interferes with the user's browsing experience. Often bundled with custom software installers, this malware appeared in late 2013 and has been in the number one spot, in terms of number of infections, for most of 2014.

FIGURE 9. IBRYTE SUMMARY



Name: Win32Adware.iBryte
ID: 2018026
Signature State: Active
Type: Adware
Class: Spyware
Level: Moderate

MAP: WIN32.ADWARE.IBRYTE

TOP 20 HIGH-THREAT-LEVEL INFECTIONS

Table 3 shows the top 20 high-threat-level malware that leads to identity theft, cybercrime or other online attacks. The top three are discussed in more detail in the next section.

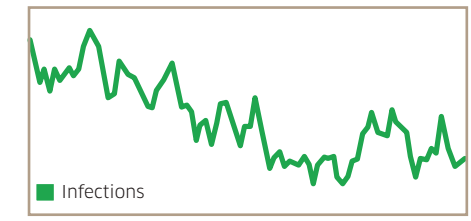
TABLE 3. TOP 20 HIGH-THREAT-LEVEL INFECTIONS

RANK	NAME	% OF TOTAL	LAST QUARTER
1	Win32.Bot.ZeroAccess2	11.13	1
2	Android.Trojan.Coogos.A!tr	8.54	6
3	Win32.BankingTrojan.Carberp	6.33	14
4	Win32.Backdoor.PcClient	3.58	New
5	Win32.BankingTrojan.Zeus	3.34	5
6	Win32.Downloader.Karagany.H	3.19	New
7	Win32.Trojan.Silentbanker.A	2.38	New
8	Win32.Trojan.Bunitu.B	2.07	8
9	Win32.BankingTrojan.ZBot	1.81	7
10	Win32.Trojan.Malagent	1.68	New
11	Win32.Worm.Mimail.E@mm	1.68	10
12	Android.MobileSpyware.Ackposts	1.60	New
13	MAC.Bot.Flashback.K/I	1.31	9
14	Win32.PasswordStealer.Lolyda.B	1.30	11
15	Android.Trojan.Sms.Send.B	1.17	New
16	Indep.Exploit.Heartbleed	1.14	New
17	Win32.ScareWare.Crypwall	1.11	New
18	Win32.ScareWare.Somoto.AMN	1.09	12
19	Win32.Downloader.Banload.AUN	1.09	New
20	Linux.Worm.TheMoon	1.01	New

TOP HIGH-THREAT-LEVEL INFECTIONS

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, it can be quite significant for the user. Due to the P2P nature of this infection the C&C servers are everywhere, with heavy concentrations of infection in the United States, Europe and Asia.

FIGURE 10. ZEROACCESS SUMMARY

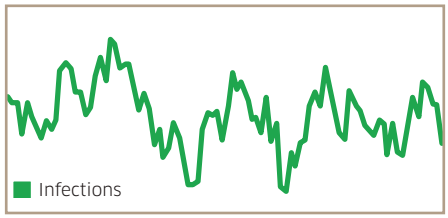


Name: Win32.Bot.ZeroAccess2
ID: 512061170
Signature State: Active
Type: Bot
Class: Cybercrime
Level: High

MAP: WIN32.BOT.ZEROACCESS2

Carberp is a banking Trojan, like Zeus and Spyeye, that steals banking credentials, passwords and credit card information and uploads the information to a remote C&C server. Carberp was first seen in June 2010. This was shut down in March 2012, but a new version was released in December 2012.

FIGURE 11. CARBERP SUMMARY



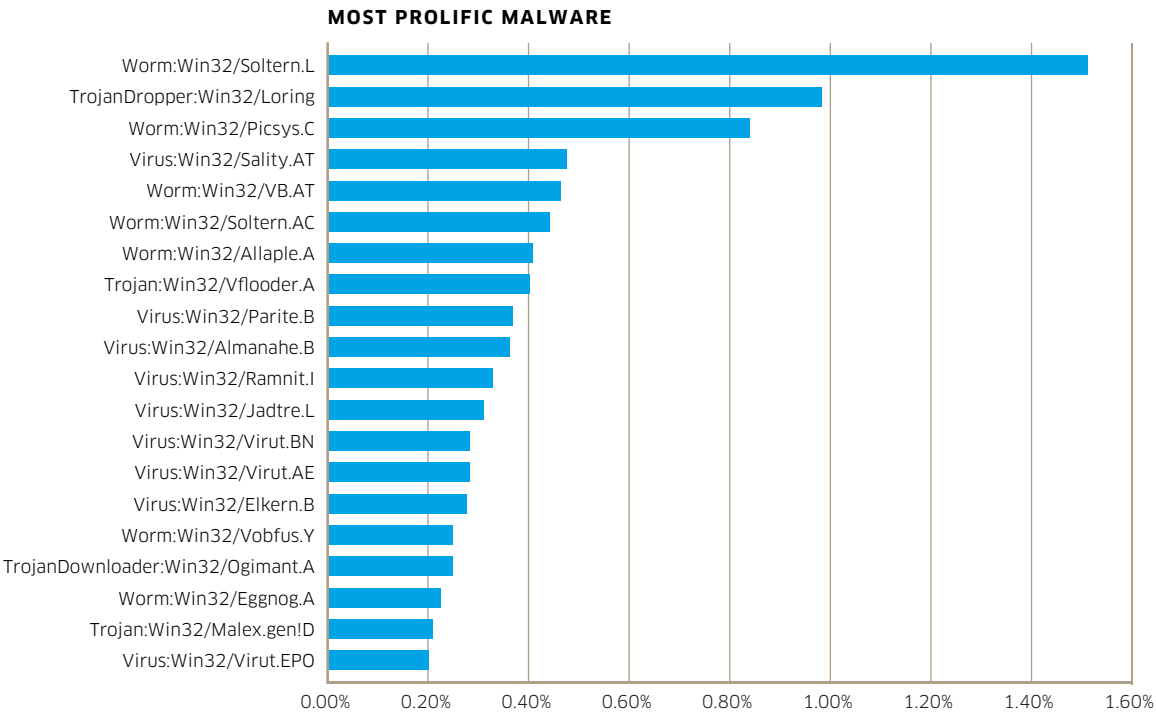
Name: Win32.BankingTrojan.Carberp
ID: 513031180
Signature State: Active
Type: Trojan
Class: Identity theft
Level: High

MAP: WIN32.BANKINGTROJAN.CARBERP

TOP 25 MOST PROLIFIC THREATS

Figure 12 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.

FIGURE 12. MOST PROLIFIC MALWARE



MALWARE IN THE NEWS

HEARTBLEED

The biggest story of 2014 so far has, of course, been Heartbleed, which could affect any server or client running OpenSSL versions 1.0.1 through 1.0.1f. It allowed the attacker to use OpenSSL's heartbeat mechanism to retrieve up to 64 K of the memory contents from the victim's computer. The attacker could not control which memory was returned. However, it was memory that was recently used by OpenSSL and could contain sensitive items, such as session keys, passwords and encryption keys.

Heartbleed is at number 16 on our top 20 high-level threats for 2014 so far.

ANDROID FAKE ID EXPLOIT

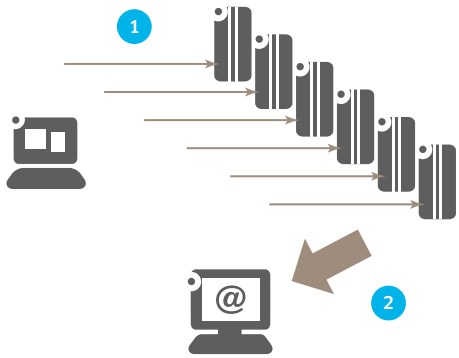
Last year, it was the MasterKey vulnerability that allowed a Trojanized app to be injected into a legitimate application and assume its identity and any system privileges. This year, we have the "Fake ID" exploit. It uses a flaw in certificate verification that allows a malicious application to pretend to be an application that has been given special privileges, such as Google Wallet.

NTP DDOS

The year started off with a series of Network Time Protocol (NTP)-based distributed denial of service (DDOS) amplification attacks leveraging ISP infrastructure. The attack worked as follows.

1. As shown in Figure 13, the attacker sends spoofed NTP MON_LIST requests to NTP servers. Each request is a 60-byte User Datagram Protocol (UDP) packet. The spoofed requests look like they were sent from the victim.
2. The NTP servers send the responses to the victim with about 50 K of data for each request, flooding the victim with Gigabytes of traffic (800 times amplification).

FIGURE 13. NTP-BASED DDOS AMPLIFICATION ATTACK



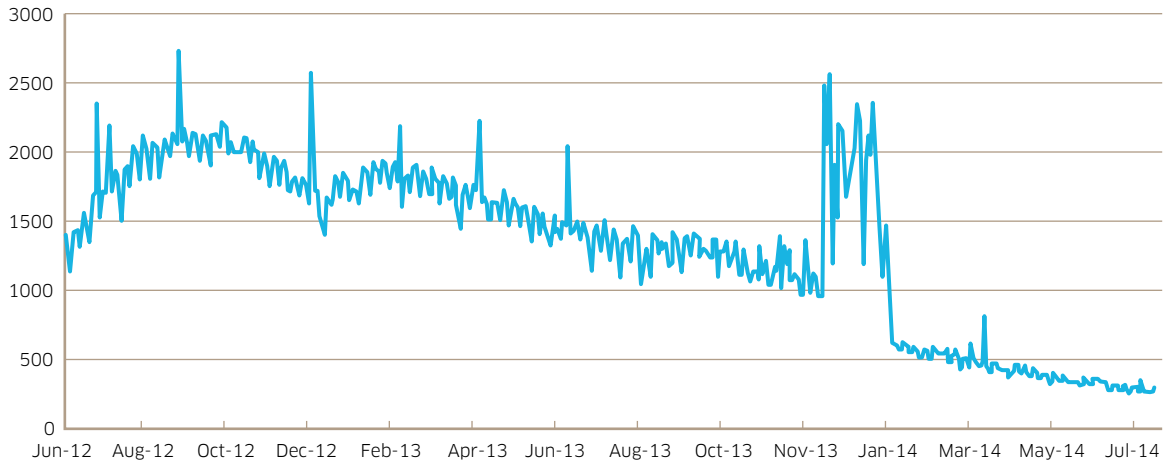
There are actually two victims of this attack. The main victims are, of course, the ultimate recipients of the UDP traffic. They are bombarded with UDP traffic from NTP servers all over the Internet. However the service providers whose NTP servers are used in the attack also suffer collateral damage due to a huge load increase on their NTP servers and significant increases in the amount of UDP traffic on their network infrastructure. In one instance we observed, the amount of UPD traffic was more than double its usual level.

The fix was to disable the MON_LIST feature, which is not required for normal NTP operation. However, in many cases, this required a software upgrade to the NTP servers.

ZEROACCESS

One surprising story of 2014 is the amazing resilience of the ZeroAccess botnet. The efforts from both Symantec and Microsoft to take it down have made a major impact to the botnet, as shown in Figure 14. However, it is still alive and kicking, albeit with a reduced presence. Separate instances of the botnet perform ad-click fraud (34 percent) and Bitcoin mining (66 percent). Observations on samples in the lab have failed to detect any ad-click fraud activity, so it appears that Microsoft's takedown of that infrastructure in December 2013 was successful. The Bitcoin-mining function may still be active. It could be that the remaining bots are simply a residue from the original botnet that are still alive, due to the simplicity and robustness of its P2P C&C protocol. Regardless, this botnet has been on our radar now for over two years and continues to be one of the most common infections on the Internet.

FIGURE 14. DAILY INFECTION RATE FOR ZEROACCESS



CONCLUSION

On the fixed residential side, the malware infection rate grew significantly in the first half of 2014, ending up at an all-time high of 18 percent. This was mostly due to moderate-threat-level adware infections, but high-threat-level infections also had a modest increase. Currently, 7 percent of homes monitored by a Kindsight security solution are infected with a high-threat-level variety of malware such as a bot, rootkit or banking Trojan.

On the mobile front, infection levels have increased 17 percent in the first half of the year. This is nearly double what was seen in 2013, with the average infection rate for Q2 at 0.65 percent. Extrapolating from this gives us about 15 M infected mobile devices worldwide. About 60 percent of the infected mobile devices are Android phones, with the remaining 40 percent being mostly Windows computers that are tethered to the mobile network. Less that 1 percent of the infections are from other devices, such as iPhones, BlackBerrys and Windows Phones. The number of Android malware samples in our database increased 83 percent in the first half of 2014.

In terms of malware trends, mobile spyware that tracks the victim's calls, text messages and location is certainly on the rise, with this type of malware representing four out of five of the new items on the mobile malware top 20 list. On the residential side, we have seen a significant increase in adware with five out of seven of the newcomers being adware.

TERMINOLOGY AND DEFINITIONS

This section defines some of the terminology used in this 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 are controlled remotely via the Internet by cyber-criminals. Botnets are used for sending spam e-mail, 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 or 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 people 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 packaged as malware and distributed through a botnet that is controlled by cyber-criminals who make money from the ad-click fraud.
Bitcoin mining	Bitcoins 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 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 computer. This includes:

- Malware C&C communications
- Backdoor connections
- Attempts to infect others, such as exploits
- Excessive e-mail
- Denial of Service (DoS) and hacking activity

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

- Monitoring information sources from major security vendors and maintaining a database of currently active threats
- Collecting malware samples (>10,000 per day), classifying and correlating them against the threat database
- Executing samples matching the top threats in a sandbox environment and comparing them against our current signature set
- Conducting a detailed analysis of the malware's behavior and building 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.

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

MKT2014087076EN (September)

Alcatel·Lucent