NOKIA

Nokia Threat Intelligence Report – H1 2016

Table of contents

NOKIA

Introduction

This report examines general trends and statistics for malware infections in devices connected through mobile and fixed networks in the first half of 2016. The data in this report has been aggregated across the networks where the Nokia NetGuard Endpoint Security solution is deployed. This network-based malware infection detection solution enables Nokia customers to monitor their fixed and mobile networks for evidence of malware infections in subscribers' endpoint devices, including mobile phones, laptops, notepads and the new generation of Internet of Things (IoT) devices. This solution is deployed in major fixed and mobile networks around the world, monitoring network traffic from more than 100 million devices.

The system examines network traffic for malware command-and-control traffic, exploit attempts, hacking activity and Distributed Denial of Service (DDOS) events. This enables the system to accurately determine the infection levels and malware profiles of these networks.

2016 first half highlights

Mobile network

- The smartphone infection rate averaged 0.49 percent in the first half of 2016. This is an increase of 96 percent from the 0.25 percent experienced in the second half of 2015.
- The infection rate rose steadily in the early months of 2016, reaching a new high of 1.06 percent of devices in April.
- Smartphone infections accounted for 78 percent of the infections detected in the mobile network. Twenty two percent are related to Windows/PC systems connected using dongles or tethered through phones.
- In April 2016, 0.82 percent of smartphone devices exhibited signs of malware infection. These malware infections included ransomware, Spyphone apps, SMS Trojans, personal information theft and aggressive adware.

Increase in smartphone malware infections	Smartphones account for seventy eight percent of mobile infections	Mobile infections peaked in April at
96%	78%	1.06%

- Android continues to be the main mobile platform targeted, but iOS-based malware was also targeted, particularly in the form of Spyphone applications.
- In 2016, DNS DDOS amplification attack activity continues to leverage devices in the mobile network, particularly mobile Wi-Fi hot spots that respond to recursive DNS requests from the internet.

Fixed residential networks

- The overall monthly infection rate in residential fixed broadband networks averaged 12 percent in the first half of 2016. This is up from 11 percent in late 2015. The increase is mostly due to moderate threat level adware infections.
- High-level threats such as a bots, rootkits, keyloggers and banking trojans remain steady at around 6 percent.

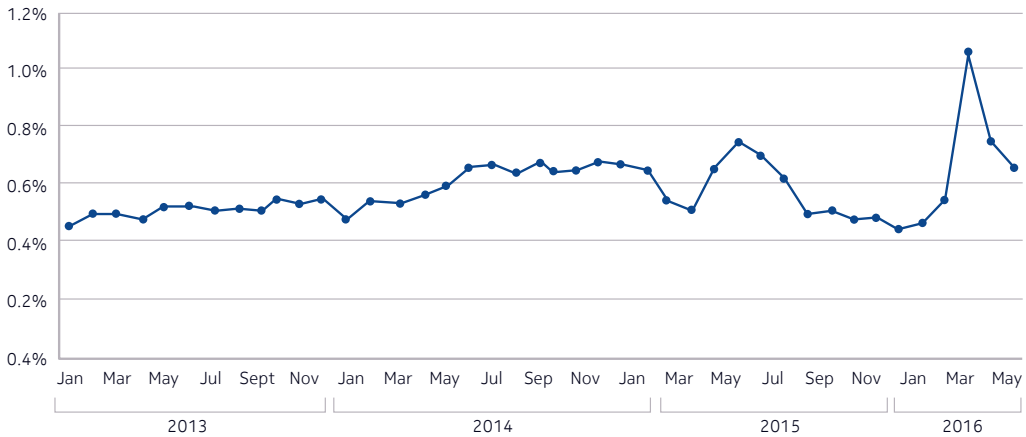
Malware in mobile networks

The average monthly infection rate among smartphones increased to 0.49 percent in the first half of 2016. This is a 98 percent increase from the 0.25 percent in the second half of 2015. The average monthly infection rate for all mobile devices, including smartphones, Windows PCs and other devices increased to 0.66 percent.

Mobile infection rate

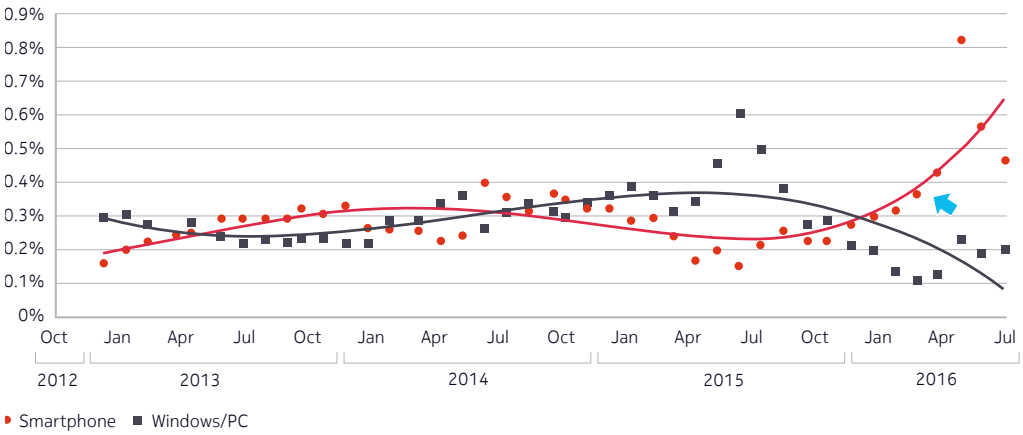
Figure 1 shows the percentage of infected devices observed monthly since December 2012. This data has been averaged from mobile deployments in Europe, North America, Asia Pacific and the Middle East.

Figure 1. Monthly infection rate on mobile networks since January 2013



After years of steady growth, the monthly infection rate has varied considerably since 2015. In 2016, it rose steeply to a new high of 1.06 percent in April, before returning to more normal levels. The sharp increase in April was due to a significant increase in smartphone infections involving the Kasandra, SMSTracker and UaPush Android trojans. These trends become clear when we look at the infection rates by device type as is shown in Figure 2.

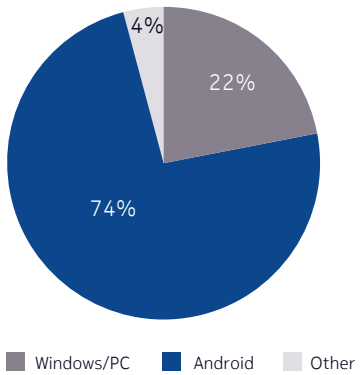
Figure 2. Monthly mobile infection rate by device type



One can clearly see a significant increase in smartphone infection in 2016 (pointed to by the arrow). In April, 0.82 percent of smartphone devices exhibited some form of malware infection. This represented 78 percent of the total infections observed for that month. To put that in perspective, close to one out of every 120 smartphones observed had a malware infection some time during the month of April.

Among smartphones, Android devices are the most commonly targeted by malware. Figure 3 provides a breakdown of infections by device type in 2016. Seventy-four percent were Android devices, 22 percent Windows/PCs and 4 percent iPhone and others.

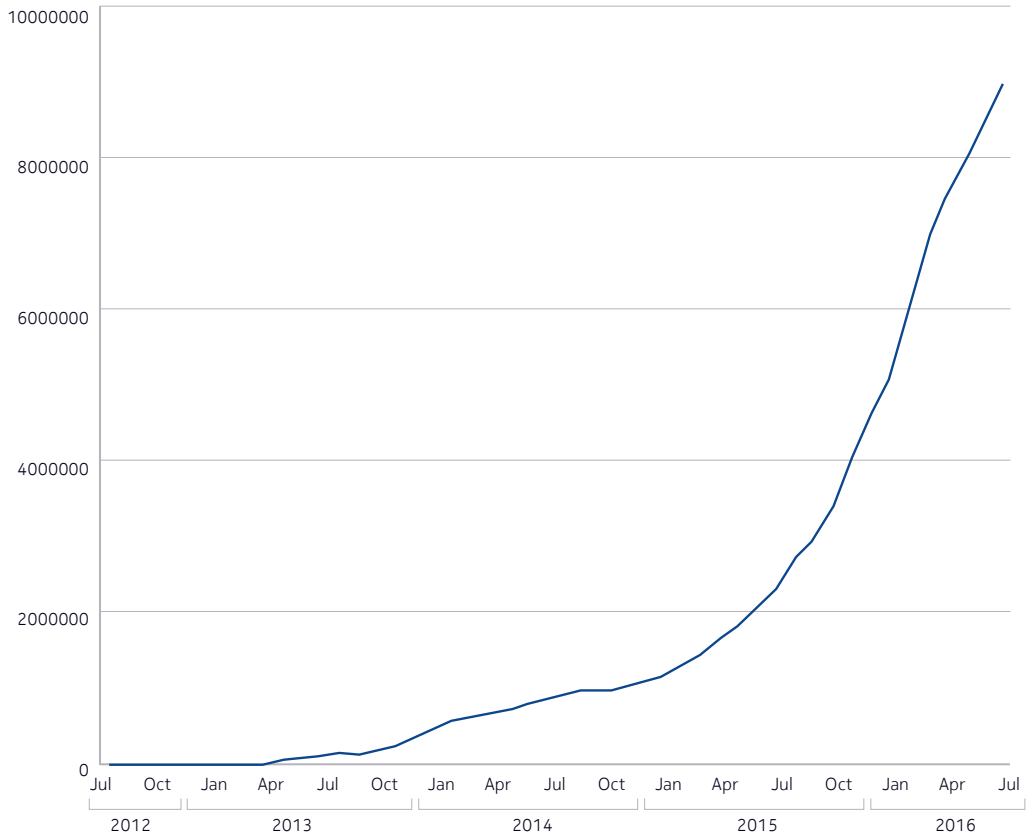
Figure 3. Infections per threat type



Android malware samples continue growth in 2016

An indicator of Android malware growth is the increase in the number of samples in our malware database. Figure 4 tracks the numbers since July 2012.

Figure 4. Mobile malware samples since July 2012



The number of Android malware samples in our malware data base increased by 75 percent in the first half of 2016.

NOKIA

Top smartphone malware

Table 1 shows the top 20 smartphone malware detected in the first half of 2016 in networks where Nokia NetGuard Endpoint Security solutions are deployed.

Table 1. Top 20 smartphone malware

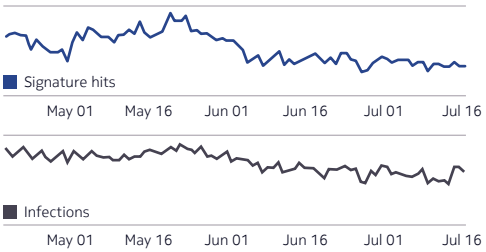
Rank	Name	Threat level	%	Previous position
1	Android.Adware.Uapush.A	Moderate	19.2	1
2	Android.MobileSpyware.Kasandra.B	High	15.23	2
3	Android.Trojan.SmsTracker	High	12.88	3
4	Android.Trackware.AndrClicker.D	Moderate	11.98	5
5	Android.BankingTrojan.Marcher.A	High	8.64	New
6	Android.Downloader.HiddenApp.HZ	High	3	New
7	Android.Trojan.Xiny.19.origin	High	2.94	New
8	Indep.MobileSpyware.mSpy	High	2.74	New
9	Android.Trojan.HiddenApp.XXS	High	2.2	New
10	iOS.InfoStealer.XcodeGhost	High	2.07	4
11	Android.Trojan.Rootnik.i	High	1.61	New
12	Android.Trojan.Axent.BS	High	1.16	New
13	Android.MobileSpyware.SpyAgnt.B	High	1.14	8
14	Android.Spyware.Ztorg.C	High	0.93	30
15	Android.Downloader.Gappusin.A	High	0.79	6
16	Android.Trojan.Gingermaster	High	0.65	New
17	Android.Backdoor.Levida.a	High	0.6	7
18	Android.Trojan.Qysly.Q	High	0.57	New
19	Android.Trojan.SMSreg.gc	High	0.55	New
20	Android.MobileSpyware.CellSpy.B	High	0.5	10

The three top entries (UaPush, Kasandra and SmsTracker) have been around since last year. In the first half of 2016, we noticed a significant increase in their activity, which was responsible for the April jump in the overall infection rate. This dropped back to previous levels in June. IOS XcodeGhost malware activity declined in 2016, but it is still in number 10 position. Also significant is the fact that ten of the top twenty malware varieties are new.

Top three mobile threats

The top three mobile threats observed in Netguard Endpoint Security deployments are described below:

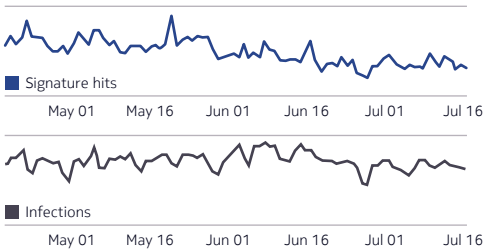
Uapush.A is an Android adware Trojan with a moderate threat level; it also sends Short Message Service (SMS) messages and steals personal information from the compromised device. The malware has its web-based C&C site located in China. Activity has been decreasing steadily in the past month.



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

MAP: ANDROID.ADWARE.UAPUSH.A

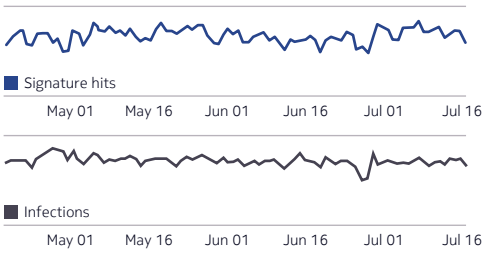
Kasandra.B is a high threat level Android remote access Trojan. It is packaged to look like Kaspersky's Mobile Security App, but is actually a Trojan that gives the attacker unrestricted access to sensitive details such as SMS messages, contact lists, call logs, browser history (including banking credentials), and GPS location data stored in Android devices. It stores all the data in an "adaptive multi-rate file on the SD card" to later upload it to a remote command-and-control (C&C) server. It is also known as SandroRAT.



Name: Android.MobileSpyware.Kasandra.B
Signature State: Active
Type: MobileSpyware
Class: Cybercrime
Level: High

MAP: ANDROID.MOBILESPYWARE.KASANDRA.B

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), text messages, voice calls, GPS locations and browser history. It is also known as Android.Monitor.Gizmo.A.



Name: Android.MobileSpyware.SMSTracker
Signature State: Active
Type: MobileSpyware
Class: Identity Theft
Level: High

MAP: ANDROID.TROJAN.SMSTRACKER

Mobile malware becoming more sophisticated

This year has certainly seen the introduction of mobile malware that is considerably more sophisticated than what's been there before. A common theme is the attempt to root the phone in order to provide complete control and establish a permanent presence on the device. Here are some examples:

HummingBad

This malware is a step up from the traditional trojanized Android app. It is an eco-system of malware components installed using a drive by download. It establishes a permanent foothold by rooting the device and makes money through ad-click fraud and by installing additional malicious apps. According to recent reports, the malware is built and operated by a Yingmob, a Chinese mobile ad-server company that is also responsible for the iOS Yispecter malware (see below).

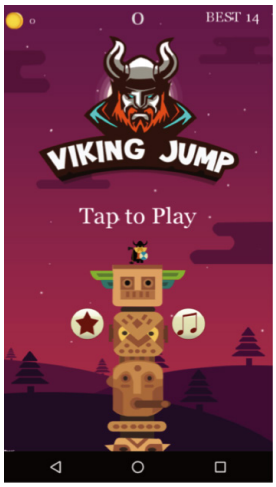
The malware first attempts to root the device, using the RightCore rooting components. If this works, it continues its app download activity, silently in the background, with no knowledge of the phone's owner. If it fails to root the device, it uses social engineering to coerce the phone's owner into giving it system permissions and downloading additional apps. The main danger of malware like this is that it can download and install malicious apps from anywhere, completely bypassing the safeguards provide by only downloading from trusted sites.

The malware also uses the “ptrace” system call to place hooks into other apps, such as the “Google Play” app. This is the first time Android malware in the wild has been seen using such sophisticated techniques to inject code into system applications. In the case of the “Google Play” app, it has enabled the malware to intercept and control the buy/install functions of “Google Play” and link them to ad-clicks that earned money for the malware operators. All in all, a nasty piece of work.

Viking Horde

This malware family gets its name from the Viking Jump game that was distributed through Google Play. Infected apps include:

- Viking Jump
- Wifi Plus
- Memory Booster
- Parrot Copter



The main purpose of the malware is to turn the phone into a transparent web proxy that can be used as part of an Ad-Click Fraud Botnet. The phone receives instruction from a command-and-control server to click on advertisements. This is similar in function to the “NotCompatible” Bot reported on last year.

This malware attempts to root the phone in order to establish a persistent hold on the device. If root is achieved, the malware installs various components in the root directory so they are hard to uninstall. It also sets up a watchdog service that reinstalls the malware, if it is removed. The watchdog can also install a fresh copy of the malware provided as an update from the C&C server.

Figure 5. Viking Horde Commands & Control (C&C)

Stream Content

```
00000000  04 00 ff 03                                        ....
    00000000  05 00 00 00 ff                                   .....
00000004  3c 00 00 00 02 03 00 32  36 39 35 63 32 64 66 31 <......2 695c2df1
00000014  63 62 62 36 38 39 32 fb  17 01 05 01 00 4e 4f 5f cbb6892. .....NO_
00000024  53 49 4d 00 00 00 00 00  00 00 00 00 00 00 00 00 SIM..... ........
00000034  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....
00000040  05 00 00 00 00                                     .....
    00000005  05 00 00 00 07                                   .....
00000045  05 00 00 00 00                                     .....
    0000000A  05 00 00 00 07                                   .....
0000004A  05 00 00 00 00                                     .....
    0000000F  05 00 00 00 07                                   .....
0000004F  05 00 00 00 00                                     .....
    00000014  05 00 00 00 07                                   .....
00000054  05 00 00 00 00                                     .....
    00000019  05 00 00 00 07                                   .....
00000059  05 00 00 00 00                                     .....
    0000001E  05 00 00 00 07                                   .....
0000005E  05 00 00 00 00                                     .....
    00000023  05 00 00 00 07                                   .....
00000063  05 00 00 00 00                                     .....
    00000028  05 00 00 00 07                                   .....
00000068  05 00 00 00 00                                     .....
    0000002D  05 00 00 00 07                                   .....
0000006D  05 00 00 00 00                                     .....
    00000032  05 00 00 00 07                                   .....
00000072  05 00 00 00 00                                     .....
    00000037  05 00 00 00 07                                   .....
00000077  05 00 00 00 00                                     .....
    0000003C  05 00 00 00 07                                   .....
0000007C  05 00 00 00 00                                     .....
```

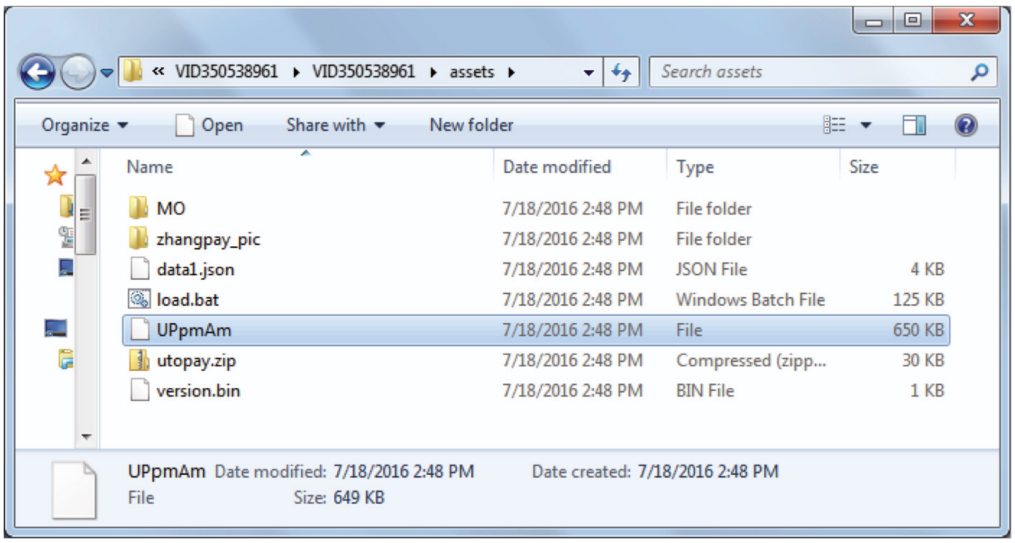
Figure 5 shows the VikingHorde C&C traffic. It uses port 443, but it is not actually using Secure Socket Layer (SSL). Communication begins with a handshake and exchange of information with the C&C server. The infected device and the C&C server then exchange keep-alive packets waiting for work.

GhostPush/Shedun

This family of Android malware is distributed in apps providing pornographic videos supported by direct payment and pop up ads. The malware component attempts to root the phone and, if successful, downloads additional malicious apps to the phone. Avira analyzed a sample in September 2015 and reported that components of this malware were being distributed in the "assets" directory as additional Android Package (APK) files. This not only makes static analysis of the code problematic, but it also bypasses various heuristics that are used on Google Play and other app stores to determine if an app contains malware.

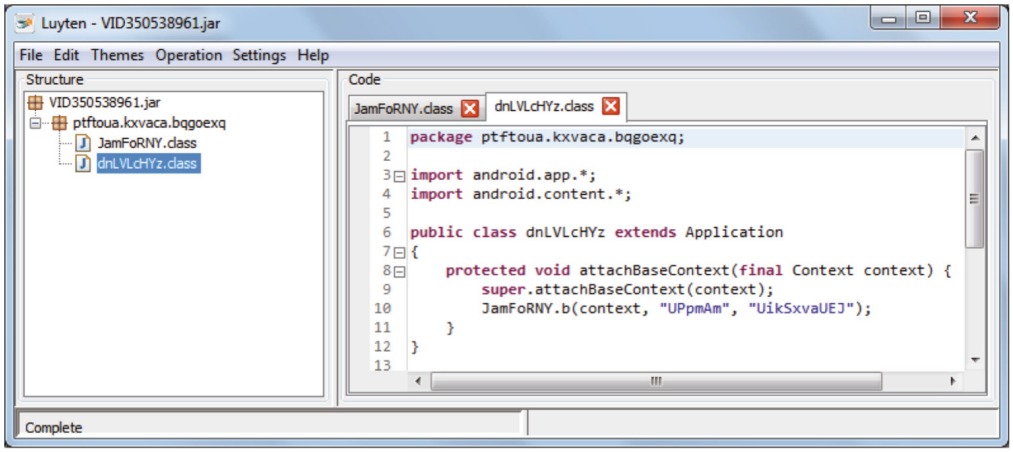
In a recent sample, it was discovered that this had gone one step further and that the entire application is distributed as an encrypted binary file in the "assets" directory.

Figure 6. Encrypted application in assets directory



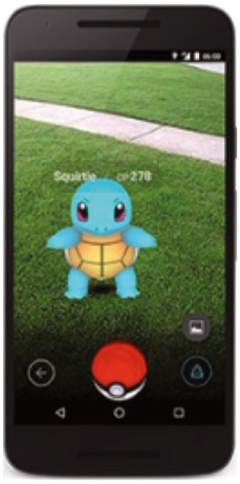
When the main application is viewed at the Java level, we see only a small stub that decrypts and unpacks the main component.

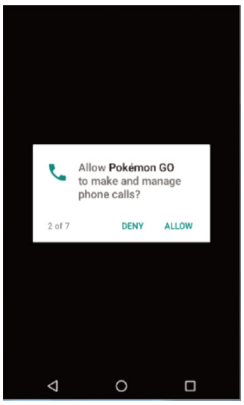
Figure 7. Function call to unpack the encrypted app



The encrypted app is contained in a binary asset called “UPpmAm,” which is converted to a JAR file and then passed to the Android class loader.

Pokémon GO





Pokémon Go is a highly popular game that has taken the world by storm since it was launched in early July. Because it was initially released in only a few countries (US, Australia, New Zealand), a number of gaming web sites provided instructions allowing people in other countries to download the game from un-trusted third-party web sites and side load it onto their Android phones.

This provided an unprecedented opportunity for hackers, and it was only a matter of a few hours before the Nokia Threat Intelligence Lab found copies of the game that had been injected with malware and made available for download from third-party sites.

One sample of Pokémon Go was infected with a remote access Trojan called “DroidJack”. This allows the attacker to track the phone’s location, record calls, take pictures and steal information and files from the phone. To the user, it is identical to the Pokémon Go game except that the first time you run it, it asks for permission to:

- Access your contacts
- Manage and make phone calls
- Take pictures and record video
- Access the device’s location
- Access photos, media. and files
- Record audio
- Send and view SMS messages

Most mobile anti-virus products detect this and prevent installation. It's also easy for the user to distinguish it from the uninfected game, when the malware asks for all those permissions.

Injecting the malware into the game is quite simple. The hacker gets a legitimate copy of the game. They open the game package (APK file) using "apktool" and a standard part of an Android developer's toolkit. This gives them access to the game's manifest, byte code, resources and assets. They drop in the malware code, adjust the manifest to include the malware components and make a minor hack to the game's byte code to run the malware when the game starts up. They then use "apktool" to rebuild the app, sign it with a bogus digital certificate, and distribute it to as many third-party app stores as they can. The whole process takes a matter of a few minutes. DroidJack, which is available to hackers for US$250, provides a complete graphical user interface to automatically inject the malware into legitimate games and applications, and provides an interactive command-and-control site for the malware.

Figure 8. Part of Pokémon Go manifest file showing "DroidJack" injection.

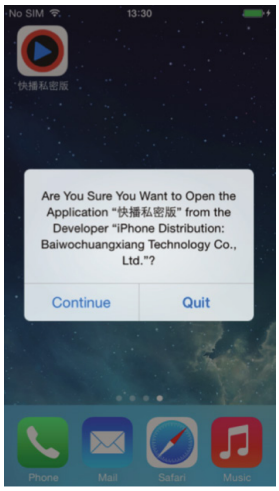
```
<meta-data android:name="com.upsight.gcm" android:value="com.nianticlabs.pokemongo.GCM_SENDER_ID"/>
<meta-data android:name="com.upsight.user_attribute.player_level" android:value="0"/>
<meta-data android:name="com.upsight.user_attribute.player_xp" android:value="0"/>
<meta-data android:name="com.upsight.user_attribute.player_avatar" android:value="0"/>
<meta-data android:name="com.upsight.user_attribute.pokemon_count" android:value="0"/>
<meta-data android:name="com.upsight.user_attribute.item_count" android:value="0"/>
<meta-data android:name="com.upsight.user_attribute.pokecoin" android:value="0"/>
<service android:enabled="true" android:name="net.droidjack.server.Controller"/>
<service android:enabled="true" android:name="net.droidjack.server.GPSLocation"/>
<service android:enabled="true" android:name="net.droidjack.server.Toaster"/>
<receiver android:name="net.droidjack.server.Connector">
    <intent-filter>
        <action android:name="android.net.conn.CONNECTIVITY_CHANGE"/>
        <action android:name="android.intent.action.BOOT_COMPLETED"/>
    </intent-filter>
</receiver>
```

For the consumer, the following rules will keep them safe.

1. Don't download games or any apps from un-trusted third-party sites.
2. Install anti-virus software on your phone.
3. Don't give games or apps permissions that they obviously don't need.

Aside from the obvious threat of side loading an infected copy of the game, the media has also noted that people can get so absorbed in the game they might inadvertently step off the curb into traffic.

YiSpecter (iOS)



This malware was discovered in 2015, but was back in the news this year because it apparently comes from the same group that created HummingBad. Its main claim to fame is that it was the first iOS malware capable of exploiting the apple sandboxing prevention mechanism on non-jail-broken iPhones. It did this by exploiting vulnerabilities in a private iOS API. This allowed the malware to install additional apps, uninstall existing ones and conceal its presence from the user.

Normally Apple's app approval process would have rejected any app that used a private API, but in this case the malware was distributed using an "Enterprise Developer" certificate, which allows iPhone apps to be distributed from private sources other than the official app store. In this case the user is asked to click "Continue" to proceed. Most users will click continue to run the app.

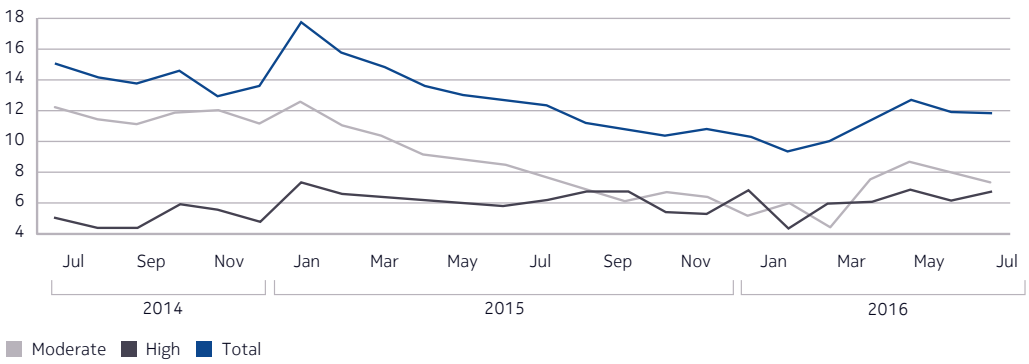
Apple fixed the issue with the private API in the IOS 8.4 version and has "improved" enterprise certificate security in iOS 9 by making it more complicated for the user to press "Continue".

Malware in fixed residential networks

Figure 9 shows residential infection rates since July 2014. These are reported on a monthly/per-residence basis, averaged across fixed network deployments of Nokia's NetGuard Endpoint Security. Although residential rates did drop throughout 2015, they have been on the increase again in the first half of 2016. Most of the fluctuation is due to moderate threat level "adware", which can vary considerably from one adware campaign to the next.

The total infection rate increased to a high of 12.7 percent in April and then dropped a little to end the first half of the year at 11.77 percent. The infection rate for high threat level malware such as bots, ransomware, and banking Trojans has remained fairly constant at around 6 percent of residences each month.

Figure 9. Monthly residential infection rate



In 2016 so far, on average each month, 11.17 percent of residences had some sort of malware infection. Of these 6.04 percent had high-threat-level infections and 6.95 percent had moderate infections. (Note that the subtotals don't add up to 11.17 percent because some residences can have moderate and high-threat-level infections).

Top 20 residential network infections

Table 2 shows the top home network infections detected by Nokia's NetGuard Endpoint Security solutions. The results are aggregated and the order is based on the number of infections detected over the six-month period of this report.

Table 2. Top 20 home network infections

Rank	Name	Threat Level	%	Previous
1	Win32.ScareWare.Winwebsec	High	14.09	4
2	Win32.Adware.MarketScore	Moderate	10.08	2
3	Win32.Adware.PullUpdate	Moderate	7.61	1
4	Win32.Adware.BrowseFox.AF	Moderate	6.37	New
5	Win32.Hijacker.Diplugem	Moderate	5.17	3
6	Win32.Adware.BrowseFox.G	Moderate	3.82	10
7	Win32.Adware.iBryte	Moderate	3.12	6
8	Android.Trackware.AndrClicker.D	Moderate	2.54	New
9	Win32.RansomWare.CryptoWall4	High	2.27	New
10	Android.MobileSpyware.Kasandra.B	High	2.08	17
11	Win32.Trackware.Binder	Moderate	1.98	13
12	Win32.Adware.ShopperPro.AR	Moderate	1.98	5
13	Win32.Downloader.Obvod.K	High	1.53	12
14	Win32.Hijacker.StartPage.KS	Moderate	1.43	18
15	Win32.Adware.Wysotot	Moderate	1.41	9
16	Win32.Trojan.Poweliks.A	High	1.24	7
17	Android.Adware.Uapush.A	Moderate	1.14	34
18	Win32.HackerTool.TektonIt	High	1.13	35
19	Win32.Bot.ZeroAccess2	High	0.97	16
20	Indep.Bot.DNSAmplification	High	0.84	New

In 2015, moderate-threat-level adware continued to dominate. Of the top 20 threats in the first half of 2016, 12 are moderate-threat-level adware and browser hijackers. Of the high-threat-level malware, ransomware, and spyware tend to dominate.

NOKIA

Top 20 high-level infections

Table 3 shows the top 20 high-threat-level malware that leads to identity theft, cybercrime, or other online attacks.

Table 3. Top 20 high-threat-level infections

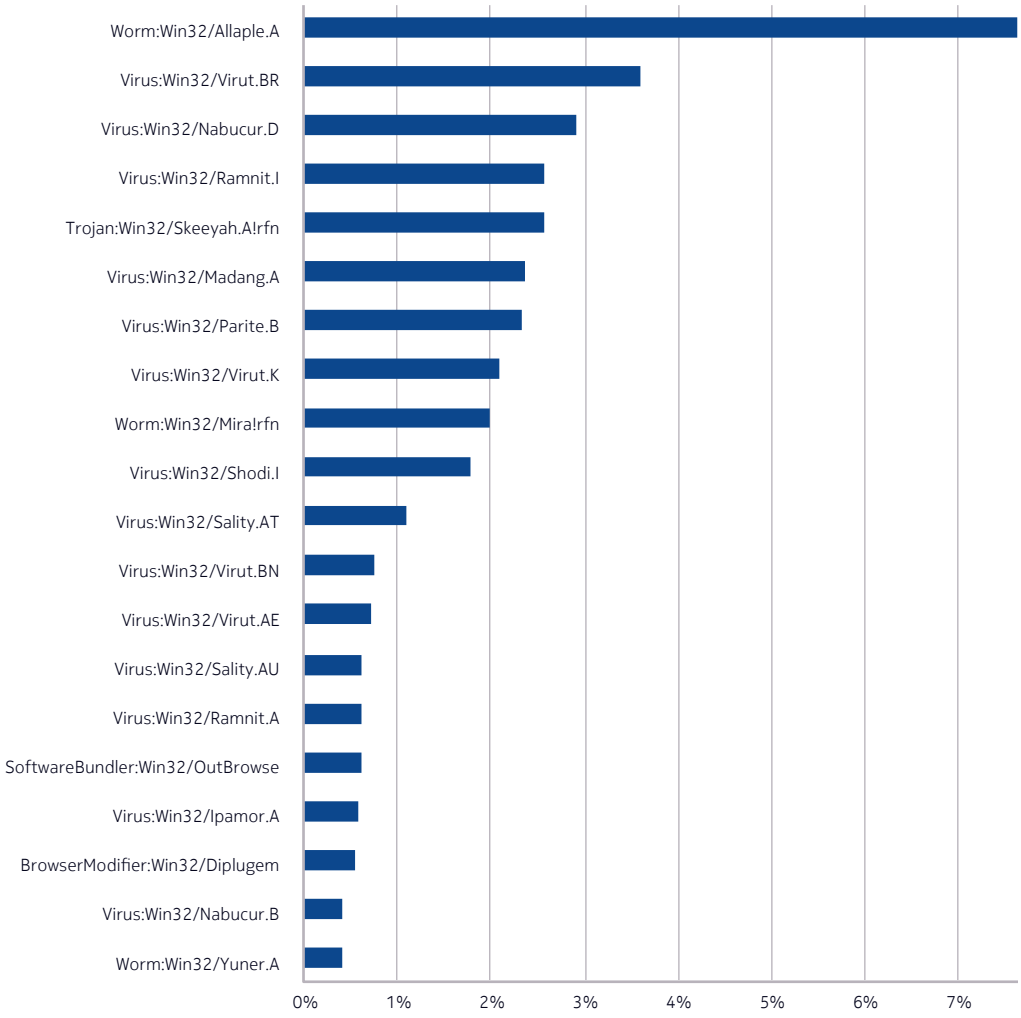
Rank	Name	%	Previous
1	Win32.ScareWare.Winwebsec	32	1
2	Win32.RansomWare.CryptoWall4	5.15	New
3	Android.MobileSpyware.Kasandra.B	4.73	5
4	Win32.Downloader.Obvod.K	3.47	3
5	Win32.Trojan.Poweliks.A	2.83	2
6	Win32.HackerTool.TektonIt	2.57	16
7	Win32.Bot.ZeroAccess2	2.2	4
8	Indep.Bot.DNSAmplification	1.91	11
9	Win32.Worm.Koobface.gen.B	1.9	12
10	Win32.Backdoor.Ammyy.z	1.74	New
11	Win32.Downloader.DownloadAssistant.A	1.67	15
12	Android.Trojan.Xiny.19.origin	1.63	New
13	Win32.Bot.Alureon	1.49	23
14	Android.Trojan.SmsTracker	1.41	56
15	Win32.Trojan.Bunitu.B	1.36	7
16	Win32.Trojan.Malagent	1.34	10
17	Win32.Trojan.Poweliks	1.19	New
18	Win32.Trojan.Usinec.A	1.03	New
19	Win32.Downloader.Ramnit.J	0.9	8
20	Win32.Downloader.Waledac.C	0.89	18

The top 20 list contains the usual suspects from previous reports with bots, downloaders, banking Trojans, and password stealers.

Top 25 most prolific threats

Figure 10 shows the top 20 most prolific malware found on the internet. The order is based on the number of distinct samples 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 10. Most prolific malware

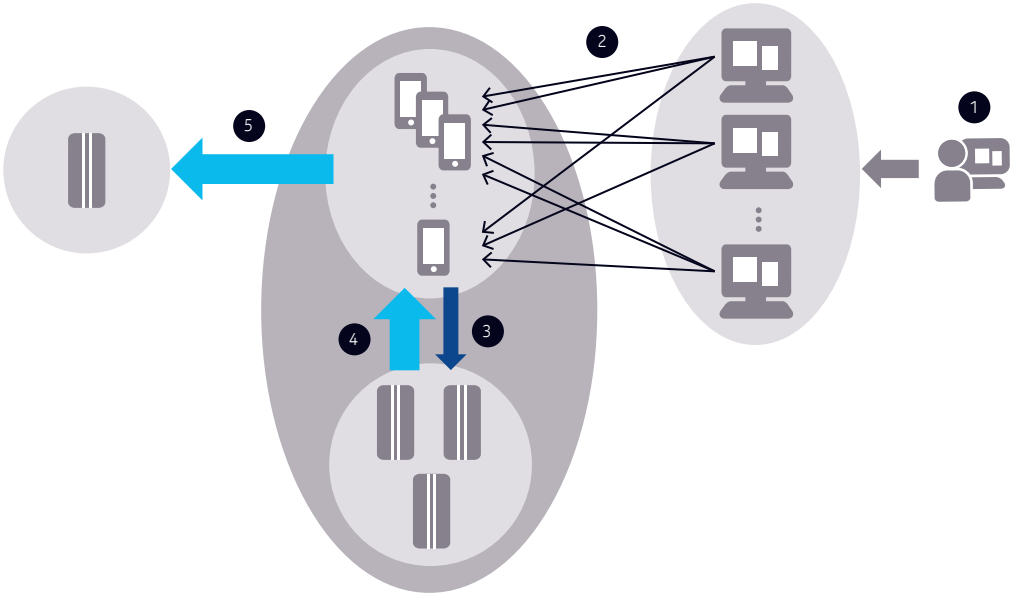


Other trends

DNS DDOS in mobile networks

This year, there have been a lot of DNS DDOS amplification attacks that leverage mobile network devices to reflect and amplify the attack. While the impact of this type of attack has been common in fixed broadband networks, mobile operators are not always aware of the impact on the mobile side.

The DNS DDOS amplification attack works as follows:



1. Attacker tells internet-based botnet to launch attack.
2. Bots send spoofed DNS request to mobile devices.
3. Mobile devices forward DNS requests to the carrier's DNS servers for resolution.
4. DNS servers respond with amplified response traffic.
5. Mobile devices flood the victim server with this response traffic.

The victim of the attack (5) can be an individual device, an entire enterprise, or a carrier subnet.

The key to the success of the attack is that the mobile devices in step 2 are willing to act as recursive DNS servers and handle the DNS lookup. Most mobile devices (e.g., phones) will not do this, but often mobile Wi-Fi hotspots will, and can be leveraged in this type of attack. The attacker will pre-scan the network in advance looking for such devices.

The impact of the attack on the carrier is as follows:

1. The reflector devices are flooded with hundreds of thousands of bogus DNS requests during an attack. These are designed to maximize the amount of information returned and often ask for information about an entire level 2 domain.
2. These, in turn, flood the carrier's DNS servers with bogus requests. In one case, more than 1 million bogus DNS requests per day were sent to the carrier's DNS server.

3. There is a large increase in UDP/DNS traffic during the attack. Sustained attacks can last for days at 2,500 DNS requests/second.

Figures 11 and 12 show detection results from DNS DDOS attacks in two mobile carriers — one from Asia and the other from North America, respectively. As is clear from Figures 11 and 12, these DDOS attacks are coordinated internet-wide events.

Figure 11. Carrier in Asia

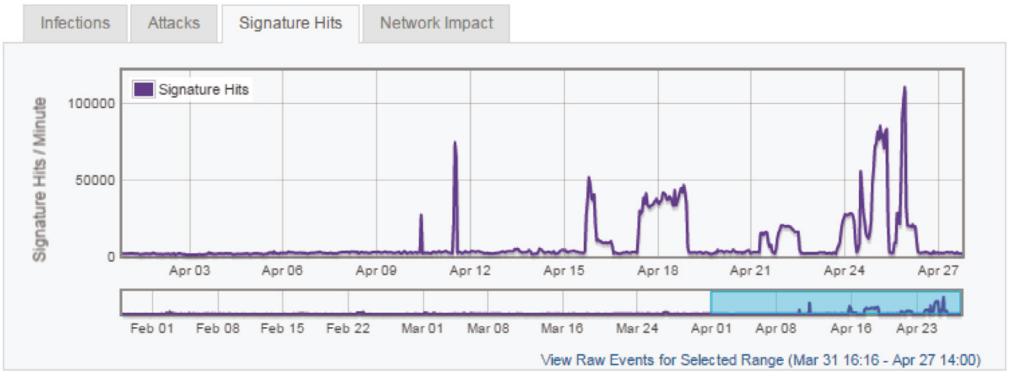
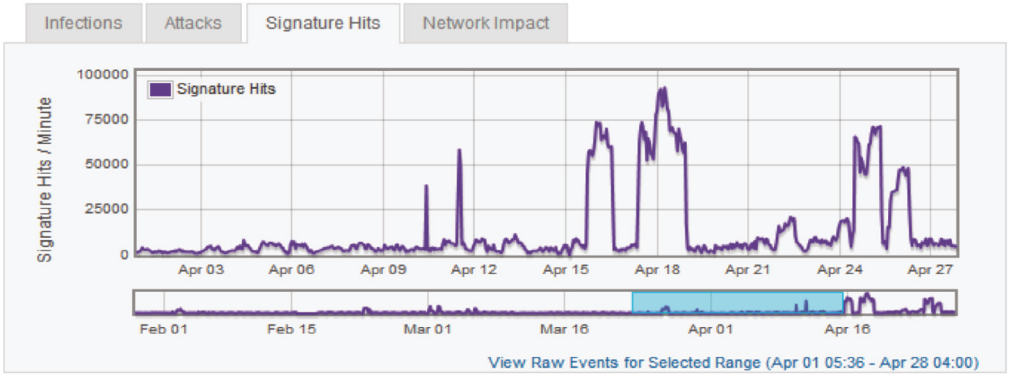


Figure 12. Carrier in North America



IoT ransomware

As discussed in the last report, ransomware was no longer only a problem for laptops and PCs, but had spread into the mobile space. It now seems to have moved into the IoT realm.

Many IoT devices are based on the Android operating system and can be impacted by malware designed to run on the Android platform. Researchers at Trend Micro found that the Flocker screen locker ransomware is capable of locking an Android-based smart TV.

NOKIA

Conclusion

The number of smartphone infections increased by 96 percent in 2016. The average monthly percentage of smartphones infected went from 0.25 percent to 0.49 percent.

Smartphone infections accounted for 78 percent of the infections detected in the mobile network. Twenty two percent are related to Windows/PC systems connected using dongles or tethered through phones. In April 2016, 0.82 percent of smartphone devices exhibited signs of malware infection. Android continues to be the main mobile platform targeted, but iOS-based malware was also evident, particularly in the form of Spyphone applications.

The overall monthly infection rate in residential fixed broadband networks averaged 12 percent in the first half of 2016. This is up from 11 percent in 2015. The increase is mostly due to moderate-threat-level adware infections. High-level threats such as a bots, rootkits, keyloggers and banking Trojans remain steady at around 6 percent.

In 2016, DNS DDOS amplification attack activity is continuing to leverage devices in the mobile network, particularly mobile Wi-Fi hot spots that respond to recursive DNS requests from the internet.

Mobile malware is definitely becoming more sophisticated, particularly in the Android space. Many examples were encountered where the malware rooted the device in order to make it difficult to detect and uninstall, as well as leverage additional privileges and access.

About the Nokia Threat Intelligence Lab

The Nokia Threat Intelligence Lab focuses on the behavior of malware network communications to develop detection rules that identify malware infections based on command-and-control communication and other network behavior. This approach enables the detection of malware in the service provider's network and the detection rules developed form the foundation of Nokia's network-based malware detection product suite.

NOKIA

To accurately detect that a user is infected, our detection rule set looks for network behavior that provides unequivocal evidence of infection coming from the user's device. This behavior includes:

- Malware command-and-control (C&C) communications
- Backdoor connections
- Attempts to infect others (for example, exploits)
- Excessive email
- Denial of Service (DoS) and hacking activity

Four main activities 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 (>100,000/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 a new signature, if a sample fails to trigger a signature.

For more information on Nokia's NetGuard Endpoint Security solution, please visit:

https://networks.nokia.com/solutions/security

https://networks.nokia.com/solutions/nokia-security-center

Or email: securitycenter@nokia.com

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: PR1608021618EN (August)