NOKIA

Nokia Threat Intelligence Report – 2017

Table of contents

NOKIA

Main findings

These main findings are discussed in detail in this report.

- Ransomware had moved to a much larger scale in 2017. Even though security patches were available, WannaCry and NotPetya spread like wildfire through enterprise networks. Network security will have to invest in new tools to ensure that all network devices are securely configured and patched. Nokia's recently announced Security Management Center is designed to fulfil this purpose.
- Despite the excellent efforts of Google to secure the Android app eco-system with Google Play Protect, Android remains the main target for mobile malware with 68% of the occurrences. We attribute this to the prevalence of side-loading apps from third party app stores and other sources. The genie is out of the bottle. In China for example, third party app stores account for 96% of the app market.
- Some incidents this year illustrated that a misbehaving app could cause significant performance issues in mobile networks, to the point that it looks like a Distributed Denial of Service (DDoS) attack is taking place. Network operators must be able to detect this type of activity and quickly take action to resolve the problem.
- Mobile adware is becoming more and more aggressive. However, as much of it is associated with ad-funded apps from reputable app stores, we cannot classify it as malware. We have seen many examples where personal information such as phone numbers, e-mail addresses and contact lists are taken from the device. Consumers should carefully read the license agreements, and be aware of the personal information they are exposing.
- The WannaCry ransomware incident caused havoc in enterprise networks, but did not have a significant impact on mobile and fixed residential networks. This can be attributed to the fact that in those cases devices are not exposed to the internet due to Network Address Translation (NAT). The recent exploits of shorter range network technologies has created a situation where it will be possible to spread malware directly from device to device via Bluetooth or Wi-Fi. Social media apps also provide a significant attack surface.

NOKIA

Introduction

This report examines general trends and statistics for malware infections in devices connected through mobile and fixed networks in the first three quarters of 2017. The data in this report has been aggregated across 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, personal computers, 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.

2017 highlights

So far 2017 has been the year of the ransomware worms. In May, WannaCry combined ransomware technology with the ability to spread like a worm and wreaked havoc on corporate networks around the globe. In June, NotPetya/Goldeneye, used the same exploits in a targeted attack on the Ukrainian government, utilities, and corporations. The ransomware was initially spread through an update to an accounting software package, and a number of companies outside Ukraine suffered considerable collateral damage. Maersk, the shipping giant, reported a loss of $US200 to 300 million in its Q2 financial report, which was directly attributable to the malware attack. These two ransomware events are covered in detail later in this report.

In September, Armis Labs announced eight zero day vulnerabilities in the Bluetooth protocol that could potentially impact billions of Bluetooth-enabled devices. Depending on the device, these vulnerabilities could result in remote code execution, man-in-the-middle attacks, and information leakage in Android, Windows, and Linux-based devices.

Mobile networks

Mobile device infection rate in 2017:	Smartphones account for seventy-two percent of mobile infections:	Average monthly Android infection rate in 2017:	Share of high level threats such as bots and ransomware:
0.68%	72%	0.94%	50%

- The average monthly infection rate in mobile networks was 0.68 percent.
- Smartphone infections accounted for 72 percent of infections detected in the mobile network.
- The average monthly Android infection rate in 2017 was 0.94 percent
- 50 percent of the threats were high level, such as bots and ransomware

- Windows/PC systems connected to the mobile network using dongles or tethered through phones accounted for 28 percent of infections observed.
- Android continues to be the main mobile platform targeted, but iOS-based devices were also targeted, particularly in the form of Spyphone applications.
- Mobile networks were not impacted significantly by the spread of WannaCry and NotPetya due to the lack of target systems and the extensive use of carrier-grade NAT.
- An accidental DDoS incident in September 2017 demonstrated that mobile network performance can be significantly impacted by misbehaving applications that generate excessive network traffic.

Fixed residential networks

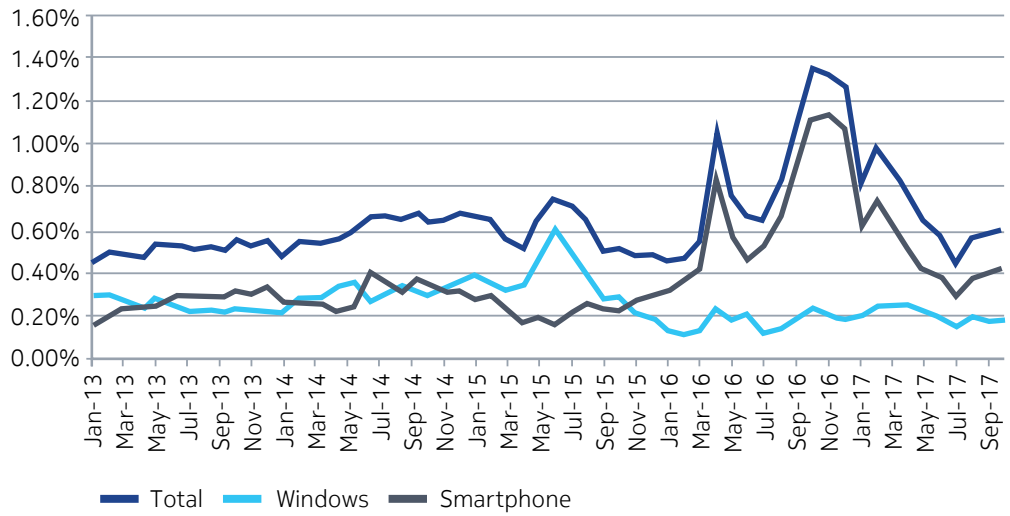
- The overall monthly infection rate in residential fixed broadband networks averaged 6.20 percent in 2017. This is down from 11.30 percent in the same period last year.
- Steady reduction in infection levels from year to year, shows that cybercrime is moving away from the Windows/PC platform to smartphones and IOT devices.
- High-level threats such as bots, rootkits, keyloggers and banking Trojans were responsible for half of the malware infections.
- There was no major impact in residential networks from WannaCry due to residential NAT.

Malware in mobile networks

Mobile infection rate

Figure 1 shows the percentage of infected devices observed monthly since January 2013. 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



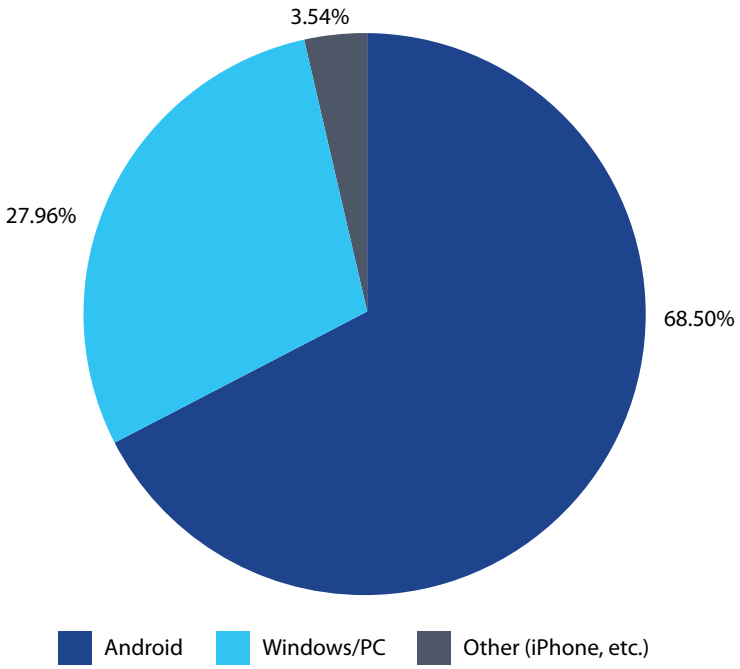
The chart shows a significant increase in mobile malware infections in the second half of 2016. Most of this growth was attributed to smartphone adware. It has become common practice to fund free apps through targeted advertising, so in early in 2017 we re-evaluated the adware that we were flagging as malicious. We decided that aggressive adware apps distributed from reputable app stores would no longer be considered malicious. Aggressive adware exclusively from third-party app stores would continue to be considered malicious if it made itself difficult to uninstall, aggressively displayed ads when the host application was not in use, shared personal information with third parties for targeted advertising purposes, or used misleading techniques to generate click-through results.

The impact of this new adware criteria can be seen in the malware infection numbers for 2017. The infection rate dropped back to pre-2016 rates in the first half of the year but has been rising again in Q3. The average infection rate for 2017 is 0.68 percent.

Infections by device

Among smartphones, Android devices are the most commonly targeted by malware. Figure 2 provides a breakdown of infections by device type in 2017. Android devices were responsible for 68.50 percent, Windows/PCs for 27.96 percent, with 3.54 percent coming from iPhones and other mobile devices.

Figure 2. Device breakdown 2017



Why is Android the main target? In the smartphone sector, the vast majority of malware is currently distributed as Trojanized applications. The user is tricked by phishing, advertising, or other social engineering into downloading and installing the application. The main reason that the Android platform is targeted, is the fact that, once side-loading is enabled, Android applications can be downloaded from just about anywhere.

Despite the very successful efforts by Google to ensure that the Play Store is malware free, Android users can continue to install apps by clicking on links in text messages and e-mail. In addition, in many regions third-party app stores have become the norm. For example, in China, Google Play is in 10th spot with less than 4% of the market share.

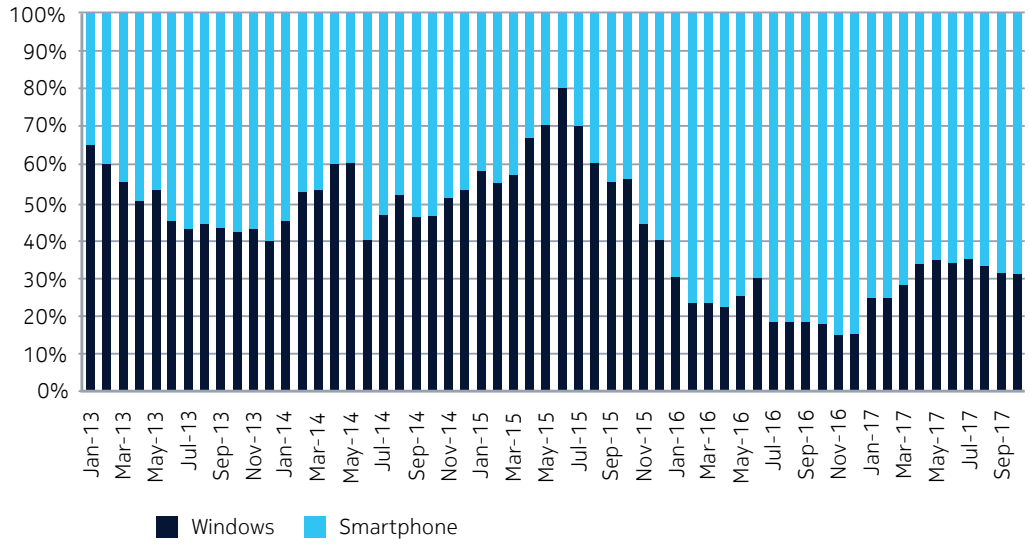
Figure 3. Top app stores in China*

IMAGE	RANK	APPSTORE	APPSTORE IN CHINESE	COVERAGE	CHANGE
	1	MyApp (Tencent)	腾讯应用宝	25.5%	-
	2	360 Mobile Assistant	360手机助手	14.8%	-
	3	Xiaomi App Store	小米应用商店	11.5%	-
	4	Baidu Mobile Assistant	百度手机助手	11.5%	-
	5	Xiaomi Game Center	小米游戏中心	10.3%	-
	6	Huawei App Market	华为应用市场	10.2%	-
	7	OPPO App Store	OPPO软件商店	7.2%	-
	8	Sogou Mobile Assistant	搜狗手机助手	4.4%	-
	9	PP Mobile Assistant	PP助手	3.6%	1 ▲
	10	Google Play Store	谷歌应用商店	3.6%	1 ▼

Many people are surprised to find that Windows/PCs are responsible for a large portion of the malware infections detected when analyzing mobile network traffic. These Windows/PCs are connected to the mobile network using USB dongles and mobile Wi-Fi devices or simply tethered through smartphones. They are responsible for 28 percent of the malware infections observed. This is because these devices are still a popular target for professional cybercriminals who have a huge investment in the Windows malware ecosystem. However, as the smartphone becomes the more preferred platform for accessing the internet, cybercrime is clearly moving in that direction. This is illustrated by the bar chart in Figure 3.

* https://newzoo.com/insights/rankings/top-10-android-app-stores-china/

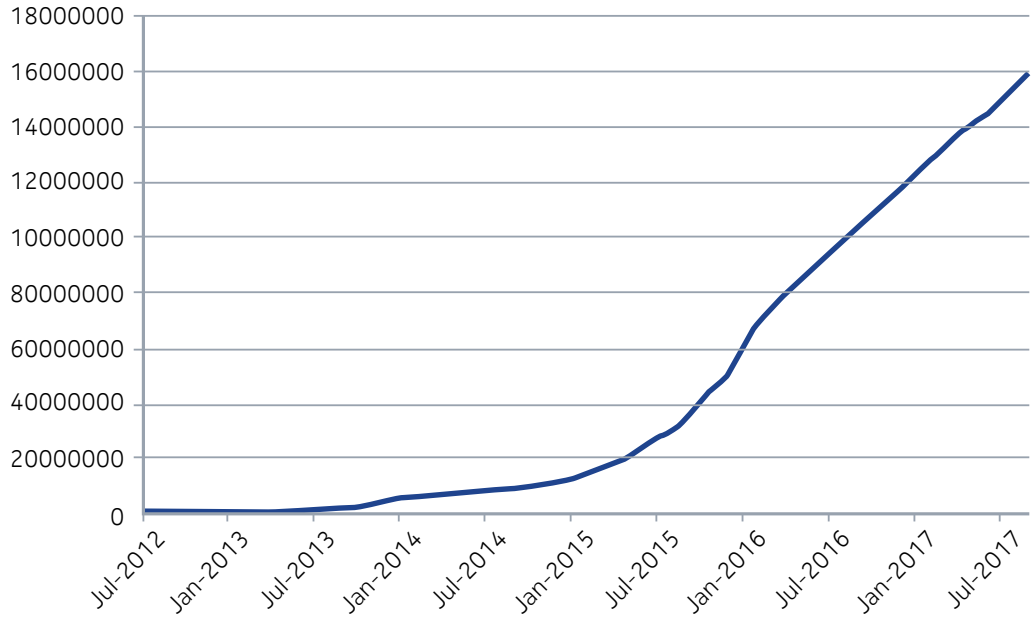
Figure 4. Comparison of Windows vs. smartphone infections over time



Android malware samples continue to grow in 2017

We now have close to sixteen-million Android malware samples in the Nokia Threat Intelligence malware database. The number of samples increased by 53 percent in the past year.

Figure 5. Mobile malware samples from July 2012 to September 2017



NOKIA

Top smartphone malware

Table 1 shows the top 20 smartphone malware detected in 2017 in networks where Nokia NetGuard Endpoint Security solutions are deployed.

Table 1. Top 20 smartphone malware

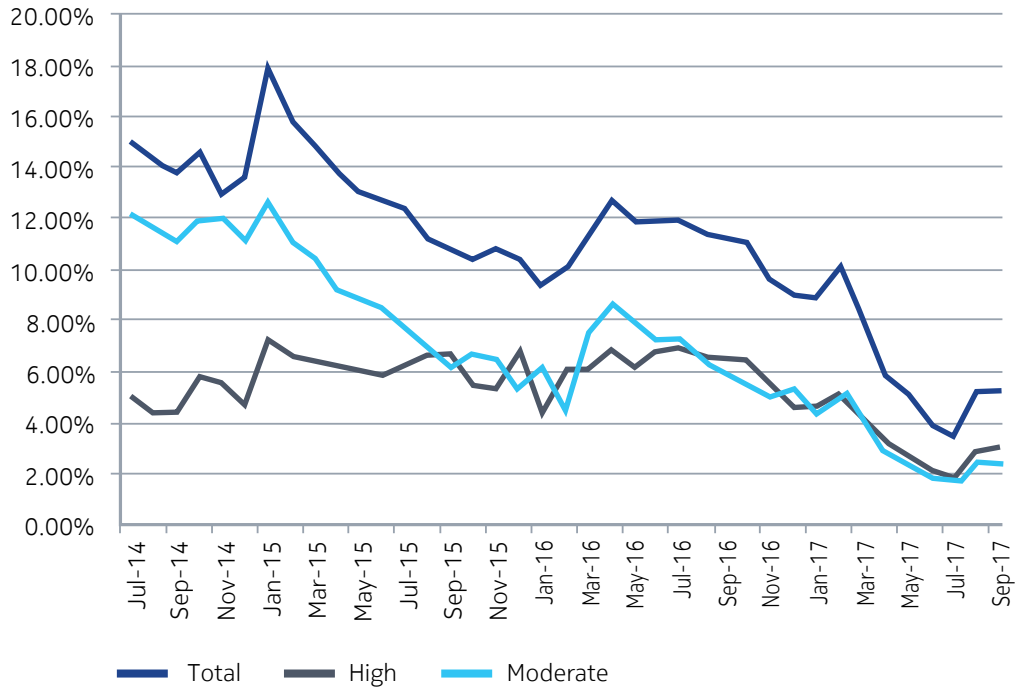
Name	Threat	%	Previous
Android.Adware.Uapush.A	Moderate	14.59	5
Android.RansomWare.Jisut.BT	High	9.93	34
Android.Trojan.Axent.EH	High	4.89	New
Android.BankingTrojan.Marcher.A	High	4.6	6
Android.Trojan.Sivu.C	High	3.96	16
Android.Trojan.HiddenApp	High	3.57	60
Android.Trojan.Clicker.HA	High	3.36	New
Android.Trackware.AndrClicker.D	Moderate	3.06	New
Android.Backdoor.Godless	High	2.82	17
Android.Trojan.Rootnik.i	High	2.6	New
Android.Trojan.Xiny.19.origin	High	2.54	14
Indep.MobileSpyware.mSpy	High	2.42	74
Android.InfoStealer.Adups	High	2.2	84
Android.MobileSpyware.SmsTracker	High	2.12	11
Android.Trojan.Xgen.FH	High	2.11	New
Android.Trojan.Rootnik.q	High	2.11	New
Android.Trojan.Qysly.Q	High	2.02	12
Android.BankingTrojan.Acecard.m	High	1.93	13
Android.Backdoor.Xgen.CD	High	1.73	New
Android.Trojan.Leech.d	High	1.47	43

Malware in fixed residential networks

Figure 5 shows residential infection rates since July 2014. These are reported on a monthly, per-residence basis, and then averaged across fixed network deployments of Nokia NetGuard Endpoint Security. Residential rates have been dropping consistently since 2015. There was an upward trend in the first half of 2016 due to a resurgence in moderate threat level adware activity. This, however, dropped off in 2017 and reached an all-time low of 3.35 percent in July 2017. Since then it has increased to 5.25 percent in September.

The average monthly residential infection rate for 2017 was 6.20 percent. About 53 percent of malware are high-threat-level bots, banking Trojans, downloaders and ransomware. The rest are moderate threat level adware and browser hijackers.

Figure 6. Monthly residential infection rate



Top 20 residential network infections

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

Table 2. Top 20 home network infections

Name	Threat	%	Previous
Win32.Adware.RelevantKnowledge	Moderate	13.56	New
Win32.ScareWare.Winwebsec	High	8.33	1
Win32.Adware.PullUpdate	Moderate	5.37	6
Win32.Bot.LatentBot	High	4.48	New
Android.Trojan.HiddenApp	High	3.23	2
Win32.Hijacker.Diplugem	Moderate	3.21	9
Android.RansomWare.Jisut.BT	High	2.83	New
Win32.HackerTool.TektonIt	High	2.64	19
Win32.Adware.Mindspark	Moderate	2.62	14
Win32.Adware.BrowseFox.AF	Moderate	2.61	5
Win32.Adware.BrowseFox.G	Moderate	2.2	12
Win32.Downloader.Obvod.K	High	2.18	17
Win32.Trackware.Binder	Moderate	2.09	21

Name	Threat	%	Previous
Win32.RansomWare.CryptoWall4	High	1.72	6
Win32.Downloader.InstallCore	High	1.41	61
Win32.Trojan.Poweliks.A	High	1.37	27
Win32.RansomWare.Kovter	High	1.35	New
Win32.Adware.ShopperPro.AR	Moderate	1.22	21
Win32.Worm.Koobface.gen.B	High	1.17	25
Win32.Adware.SlimwareUtil	Moderate	1.15	New

Of the top 20 malware infections detected in fixed residential networks in 2017, the majority still focus on the traditional Windows/PC platform; however 6 percent of the infections detected involved the Android platform.

Top 20 high-level infections

Table 3 shows the top 20 high-threat-level malware across both mobile and fixed networks. High-threat-level infections are associated with identity theft, financial loss, and other cybercriminal activity.

Table 3. Top 20 high-threat-level infections

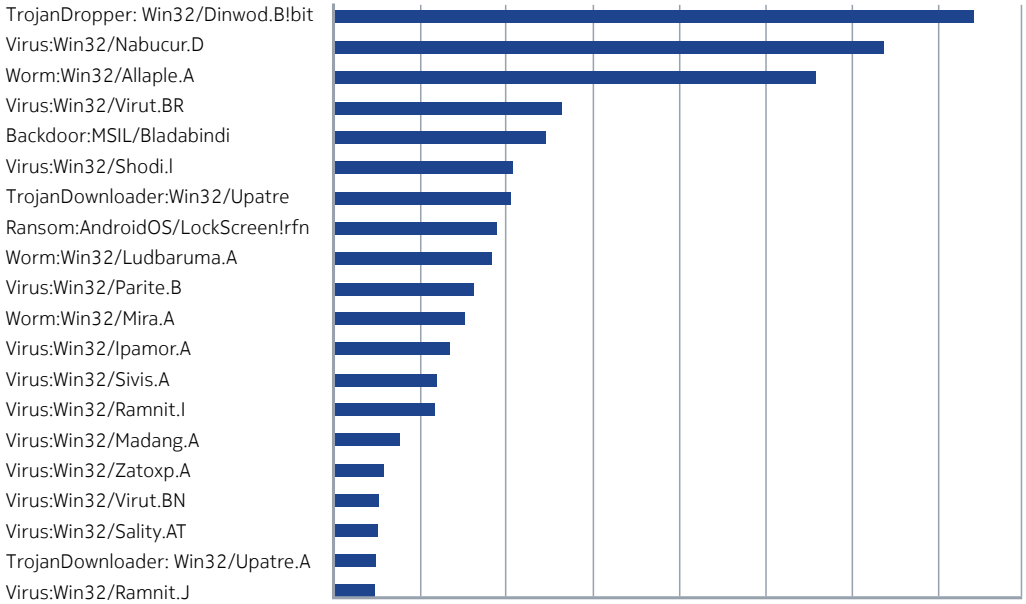
Name	%	Previous
Win32.ScareWare.Winwebsec	13.97	1
Win32.Bot.LatentBot	7.51	New
Android.Trojan.HiddenApp	5.41	2
Android.RansomWare.Jisut.BT	4.75	New
Win32.HackerTool.TektonIt	4.42	7
Win32.Downloader.Obvod.K	3.65	6
Win32.RansomWare.CryptoWall4	2.89	3
Win32.Downloader.InstallCore	2.37	41
Win32.Trojan.Poweliks.A	2.3	13
Win32.RansomWare.Kovter	2.27	New
Win32.Worm.Koobface.gen.B	1.97	11
Android.Trojan.Axent.EH	1.76	New
Win32.Backdoor.Ammyy.z	1.63	14
Win32.Bot.ZeroAccess2	1.63	12
Android.Trojan.Xiny.19.origin	1.38	9
Android.InfoStealer.Adups	1.32	New
Win32.Downloader.Waledac.C	1.31	20
Android.Trojan.Sivu.C	1.06	19
Android.Bot.DressCode	0.96	27
Win32.Bot.Redirector.Paco	0.83	18

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

Top 25 most prolific threats

Figure 6 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 7. Most prolific malware



Security incidents in 2017

WannaCry

On May 12th the WannaCry ransomware was responsible for one of the biggest ransomware attacks of all time. The main difference between WannaCry and previous ransomware was the fact that WannaCry exploited the EternalBlue Windows SMB vulnerability (CVE-2017-0144). This enabled WannaCry to spread directly from one Windows/PC to another through the network, without user intervention. It quickly spread through corporate networks, infecting a large number of un-patched Windows servers and laptops, hitting hospitals in Britain, as well as the Spanish telecom giant Telefonica while also spreading in other countries' organizations and businesses, including Russian banks, FedEx, Deutsche Bahn and European car makers. In sum, WannaCry infected more than 230,000 computers in 150 countries. The ransomware:

- Encrypted data on the computer and demanded a Bitcoin ransom.
- Targeted Microsoft Windows computers.
- Used standard phishing to get an initial foothold.

- Spread rapidly through corporate networks, using the EternalBlue exploit (CVE-2017-0144).
- Used its worm propagation ability to devastate corporate networks.
- Had less of an impact on residential and mobile users, primarily due to the widespread use on NAT.

The impact of WannaCry could have been much larger, had it not been for the discovery of a DNS "kill switch," that effectively shut down the malware and prevented it from spreading.

Figure 8. WannaCry infected more than 230,000 computers in 150 countries, and demanded ransom for encrypted data.

Impact on corporate IT networks

When the malware outbreak occurred, we saw significant activity in corporate networks where NetGuard Endpoint Security is deployed. As soon as an infected host was introduced to the network, the malware spread rapidly due to:

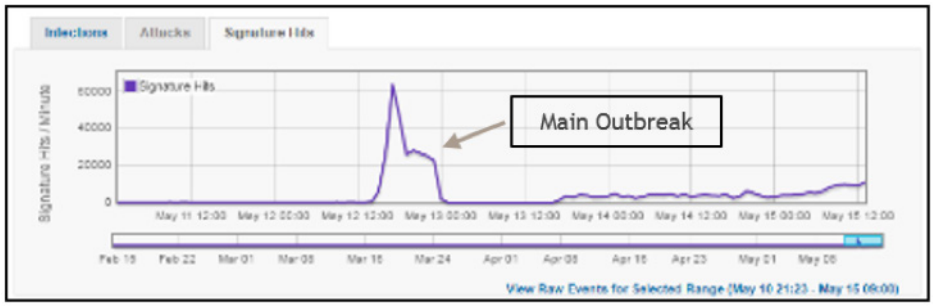
- The extensive use of the Microsoft SMB protocol in these types of networks
- A large population of susceptible devices
- The fact that WannaCry aggressively targeted local subnets made spreading very efficient

- The lack of any internal network segmentation blocking the SMB protocol
- The fact that many servers and laptops had not been patched for the CVE-2017-0144 vulnerability

Microsoft were aware of the vulnerability and on March 14th (two months before the attack), they issued security bulletin MS17-010 and announced that patches were available.

The chart bellows shown one example.

Figure 9. The malware outbreak caused a peak in activities in corporate networks.



The chart shows an initial infection event on the Friday, some quiet time over the weekend and then residual activity the next week, as people reintroduced infected laptops to the corporate network.

Impact on fixed residential and mobile networks

NES deployments in both fixed and mobile networks saw very little activity from WannaCry. The malware did try to spread to randomly selected internet addresses, but due to the widespread uses on NAT, it was very unlikely that the attacker would find a vulnerable system to infect.

In the fixed residential network, devices in the home are usually not visible from the internet. Only the residential gateway is visible from the internet and NAT protects the devices behind the gateway. Since the IP address is not accessible from the internet, it is not possible to launch the SMB attack.

In mobile networks, most of the devices are smartphones and are not vulnerable to the attack. Also, carrier-grade NAT is used for a large percentage of mobile devices, making them invisible from the internet. Even when NAT is not used, vulnerable Windows computers would likely be deployed behind a mobile hotspot or Mifi that would use local NAT and provide protection.

One caution to carriers is that, as they move to IPv6 and NAT is no longer required, they should consider the security protection that NAT has been providing and ensure that similar protection is available in the IPv6 networks. Firewalls can be used at the network borders to prevent unsolicited connection from the public internet. Many carriers already block the SMB protocol at the border of their network.

GoldenEye/NotPetya

On June 27th there was a new ransomware campaign, similar to the WannaCry incident of May 12th. The ransomware in this case is a variant of the GoldenEye-Petya family that has been modified to spread directly through the network, using the same worm-like exploitation as WannaCry.

Figure 10. GoldenEye/NotPetya demanded ransom, but the real motivation was to cause mayhem by rendering computers and servers unusable.

The attack was highly targeted at Ukraine. Ukraine's government, national bank and the biggest power companies were reported to have been attacked as were airlines and metro services in the country. The attack also spread outside the Ukraine and there were immediate reports that Maersk, Merck, DLA Piper, WPP and the Russian oil company Rosnoft had been attacked. Microsoft reported that computers in 65 countries were impacted.

Initial infection was delivered as a software update to Ukrainian accounting software MeDoc. The cybercriminals responsible had to hack into MeDoc and infect the software update with the malware. Once a computer was infected, it then spread rapidly through targeted networks using the same EternalBlue/DoublePulsar worm as WannaCry. It is hard to believe that, despite the huge publicity associated with WannaCry and the fact that patches had been available for months, that there were still so many vulnerable hosts.

The infection impacted Windows-based servers, desktops, and laptops. Once a device was compromised, the files were encrypted and a US$300 ransom was demanded. In this case, malware also encrypted the devices boot sector and then shut it down, rendering it unbootable.

So, it looks like the ransomware was just a smokescreen. The real motivation was to cause destruction and mayhem by rendering computers and servers unusable. The ransomware aspects of this attack were used to disable the computers. The attackers were not seriously expecting to make any profit from the ransom itself.

Maersk, the shipping giant, reported a loss of US$200 to300 million, directly attributable to the malware attack in its Q2 financial report.

WireX Android DDoS bot

This Android DDoS botnet, that was reported to have involved over 150K devices, targeted content delivery networks. On August 29th, Akamai, Google, and several security vendors announced that it had been taken down. The bot was distributed in Trojanized apps that had been downloaded from Google Play. As part of the takedown, more than 300 apps were removed from Google Play.

BlueBorne Bluetooth vulnerability

On September 12th, Armis Labs announced eight zero day vulnerabilities in the Bluetooth protocol that could potentially impact billions of Bluetooth-enabled devices. Depending on the device, these vulnerabilities could result in remote code execution, man-in-the-middle attacks, and information leakage. Their web site provides demonstrations of how vulnerabilities could be used to compromise Android, Windows, and Linux-based devices. The vulnerabilities include:

- Linux kernel RCE vulnerability - CVE-2017-1000251
- Linux Bluetooth stack (BlueZ) information Leak vulnerability - CVE-2017-1000250
- Android information leak vulnerability - CVE-2017-0785
- Android RCE vulnerability #1 - CVE-2017-0781
- Android RCE vulnerability #2 - CVE-2017-0782
- The Bluetooth Pineapple in Android - Logical Flaw CVE-2017-0783
- The Bluetooth Pineapple in Windows - Logical Flaw CVE-2017-8628
- Apple Low Energy Audio Protocol RCE vulnerability - CVE-2017-14315

Affected devices

According to Armis, Bluetooth-enabled devices running Android, Linux, Windows, and the pre-version 10 of iOS operating systems are impacted by at least one of the disclosed vulnerabilities. This covers a significant portion of connected devices globally. The security researchers who uncovered BlueBorne estimate that 5.3 billion devices with Bluetooth capabilities could be affected. However, certain conditions must exist before these vulnerabilities can be exploited:

- Bluetooth must be enabled.
- The attacker must be within the Bluetooth-enabled device's range (e.g., typically within 10 meters).
- The attack will vary per mobile platform (i.e., operating system), so having a single exploit that can target all devices is unlikely.

NOKIA

What does BlueBorne do?

The exploits used by Armis are proof-of-concept (POC) exploits that have been demonstrated in a lab environment. Even though the POC exploits have not been released, the exploits' technical details have been disclosed in a technical white paper, so attackers can now build exploits based on that information.

The Android demonstration showed an attacker taking remote control of an Android phone and activating the camera without the owner's knowledge. The Windows demonstration showed a man-in-the-middle attack where the Windows user was redirected to a fake website and entered his e-mail, user id and password, which were stolen by the attacker. The Linux demonstration showed an exploit used to eavesdrop on a Linux RCE smartwatch. The attacker then rebooted the device.

Armis did not demonstrate a worm that could spread from one device to another, but due to remote code execution, it might also be possible. However, as the Stagefright vulnerabilities proved, it is often very difficult in practice to come up with an exploit that will work across a wide range of software implementations. It is theoretically possible to build a worm that can spread to a large variety of Bluetooth devices, but it is highly unlikely.

What has been done?

Armis shared the details of the vulnerabilities and exploits with Google, Microsoft, Apple, Samsung and Linux in April 2017. The following security updates were provided prior to the disclosure on 12 September 2017.

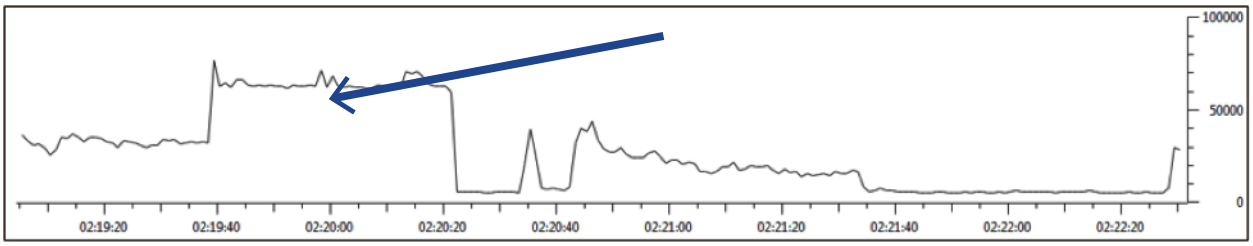
- Google addressed CVE-2017-0781, CVE-2017-0782, CVE-2017-0783, and CVE-2017-0785 through its Android Security Bulletin for September.
- Microsoft made updates on 11 July 2017, and released one for CVE-2017-8628 as part of its September patch on 12 September 2017.
- Apple has no vulnerability in its current versions. iOS 9.3.5 and AppleTV devices with version 7.2.2 (released in August and December 2016 respectively) and lower are affected, but those running iOS 10 are immune from CVE-2017-14315.
- Linux: Targeting updates for the disclosure on or about 12 September 2017.

Accidental DDoS

Distributed denial of service (DDoS) attacks are usually associated with cybercriminals, hackers, and botnets; however, in a recent case investigated by the Nokia Threat Intelligence Lab, it appears as if the DDoS was caused by malfunctioning software.

We noticed some unusual network activity in a mobile carrier's core network that had the characteristics of a DDoS attack. One instance is illustrated in the graph below.

Figure 11. Traffic flood caused by a software flaw



Between 2:19:40 and 2:20:20, we saw more than two-million packets sent from a single smartphone to a web server owned by the device manufacturer. This doubled the packet load on the network and caused some performance issues. All the packets were identical TCP packets— each 52 bytes long, with the ACK+URG flags set. There was no response from the server. This has all the hallmarks of a DDoS flooding attack. A single phone was generating an ACK flood of more than 50K packets/second.

There had been similar events in a number of mobile carriers. Detailed analysis concluded that this was not a deliberate DDoS attack, but that the traffic flood was due to a software flaw in a software upgrade. It is significant that a software flaw could cause a single smartphone to generate so much traffic.

KRACK Wi-Fi Vulnerabilities

In October 2017, a security researcher published information about several vulnerabilities in the WPA2 protocol that is used to secure Wi-Fi communications. The name "KRACK" comes from the technique used to describe the attack which is called a "Key Reinstallation AttaCK".

The attack is launched against the Wi-Fi client, and causes it to reuse cryptographic keys and parameters which allows the attacker to decrypt the communication. In most cases the attacker can only decrypt parts of the communication, but this is enough to steal sensitive information, such as access credentials and passwords. A software flaw in some Linux and Android implementations allows the attacker to decrypt the entire communication.

The main attack is against the four-way handshake of WPA2 that is used to set up the cryptographic keys and associated parameters that are used to encrypt the communications. The attack involves replaying the third message of this handshake in a way that tricks the client into reinstalling a previously used encryption key, and resetting the nounce value and packet counter. This opens the door to known plaintext attacks that can be used to decrypt communications.

Due to a software flaw in some Linux and Android implementations the attack can cause the Wi-Fi client to completely zero out the encryption key, making the entire communication visible. Android 6.0 devices are vulnerable to this level of attack.

The vulnerability allows the attacker to decrypt the supposedly secure communication between the victim and the Wi-Fi access point. This enables the attacker to steal sensitive information, and in some cases to modify the data and inject malicious content into the communications.

The researcher demonstrated an attack with inserting a rogue Wi-Fi access point between the victim and the normal access point that they were trying to connect to. Rogue access points can use several techniques to get access to unencrypted data, but in this case, it was acting as a man-in-the-middle between the victim and the real access point. In case of corporate Wi-Fi access, this could provide the rogue access point with access to the corporate network

Conclusion

The average monthly infection rate in mobile networks was 0.68 percent. Smartphone infections accounted for 72 percent of the infections detected in the mobile network. The overall monthly infection rate in residential fixed broadband networks averaged 6.20 percent in 2017. This is down from 11.30 percent in the same period in 2016. So, there is a clear trend that cybercriminals are changing their focus from the Windows/PC ecosystem to smartphones and IoT devices.

Android continues to be the main mobile platform targeted, but iOS-based devices were also targeted, particularly in the form of Spyphone applications. The main reason that Android is the most popular target is because currently, most mobile malware is distributed as Trojanized applications and the Android app ecosystem allows the user to download and install applications from untrusted sources.

The biggest security events of 2017 have been the WannaCry and NotPetya ransomware incidents. These spread like wildfire through corporate networks, using the EternalBlue SMB vulnerability. Corporate networks were extremely vulnerable due to the large number of vulnerable Windows servers, as well as PC and the wide-open internal network communication within these corporate networks. Devices on mobile and fixed broadband networks were not impacted significantly by the spread of WannaCry and NotPetya. This is due to the lack of target systems and the extensive use of NAT in those networks.

An incident in September illustrated that mobile network performance can be significantly impacted by misbehaving applications that generate excessive network traffic. Carriers will need to be able to detect these types of events quickly and quarantine the affected devices.

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 the Nokia network-based malware detection product suite.

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:

- Monitoring of information sources from major security vendors and maintaining a database of current and active threats
- Collecting malware samples (>200,000/day), and classifying and correlating them against the threat database
- Executing samples that match 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 a new signature, if a sample fails to trigger a signature.

Find out more about the Nokia Threat Intelligence Center, visit our Security solution page, or learn more about the Nokia NetGuard Endpoint Security solution

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

Product code: SR1710017387EN (November)