Bitdefender®

The Global Threat Landscape Report - 2017

Foreword

The past few months have spurred a dramatic reshaping of the threat landscape. Traditional threats such as generic Trojans, ransomware and spam bots have been massively complemented by data destructors. Powered by military-grade code allegedly leaked from the NSA, both WannaCry and GoldenEye wrought havoc throughout Q2 and Q3, shutting down businesses and causing unprecedented operating losses.

Novel lateral movement vectors have complemented zero-day exploits such as EternalBlue and EternalRomance to take over the enterprise space. Other significant trends in 2017 are the increased focus on freeware or open-source tools stitched together by custom-built code to weaponize them to support the attacker's agenda.

Our APT and targeted attack investigations in 2017 reveal free tools such as password recovery utilities from Nirsoft and legitimate encryption utilities such as DiskCryptor and so on, which makes detection and remediation increasingly difficult.

These targeted attacks are reshaping the corporate and government security landscape, and causing fallout in the consumer space, as commercial cyber-criminals rush to adopt leaked exploits and advanced lateral movement technologies into their own payloads.

Bitdefender is constantly monitoring its global network of more than 500 million sensors and honeypots for emerging threats or low-key cyber-attacks that try to fly under security products' radar. The aggregated data allows us to paint an accurate picture of what is happening in the industry and helps us develop new mitigations for the upcoming generation of cyber-threats.

This report is based exclusively on information collected via a wide range of security services within GravityZone: Security for Virtualized Environments, Security for Endpoints, Security for Mobile and Security for Exchange, consumer-oriented products such as Bitdefender Antivirus, Bitdefender Internet Security or Bitdefender Total Security, as well as from Bitdefender BOX, the innovative solution for protecting devices in the IoT space.

Key findings

Bitdefender telemetry shows ransomware is still the most frequently encountered threat. During 2017 alone, the number of new major ransomware families surpassed 160, with dozens or even hundreds of variations per family. The most prolific ransomware strain is Troldesh / Crysis, with hundreds of sub-variants seen to date. GlobeImposter, another extremely prolific ransomware family, competes head-to-head with Troldesh in the number of released sub-variants.

The commercial malware ecosystem is intensely focused on developing and planting ransomware. Our stats show that **one in six spam e-mail messages comes bundled with some form of ransomware** (link to drive-by download sites, attachments rigged with ransomware or even JavaScript/VBS downloaders for ransomware).

Another spectacular development in the 2017 threat landscape is **the re-emergence of Qbot** (also known as Brresmon or Emotet), a multi-purpose, network-aware worm with backdoor capabilities that has been around for years. It has larely re-emerged with a significant redesign of the command and control infrastructure and, more importantly, with a cloud-based polymorphic engine that allows it to take a virtually unlimited number of forms to avoid AV detection.

Ransomware specifically aimed at companies is now a thing. Since the re-emergence this March of the Troldesh ransomware family, companies have faced extremely targeted attacks that abuse the Remote Desktop Protocol to connect to infrastructure, then manually infect computers. Ransomware like Troldesh and GlobeImposter have lateral movement tools (such as Mimikatz) to infect the organization and log clean-up mechanisms to cover their tracks.

Crypto-currency miners have taken multiple shapes and approaches in 2017. Traditional illicit coin miners have rushed to adopt lateral movement tactics such as the EternalBlue and EternalRomance exploits, allegedly originating from the NSA, to infect computers in organizations and increase mining efforts. Representative of this category is the Monero miner Adylkuzz, which appeared in early May, roughly at the same time as WannaCry. Another notable development is attackers' move to integrate mining code in compromised web sites to reach a broader audience and increase the mining yield.

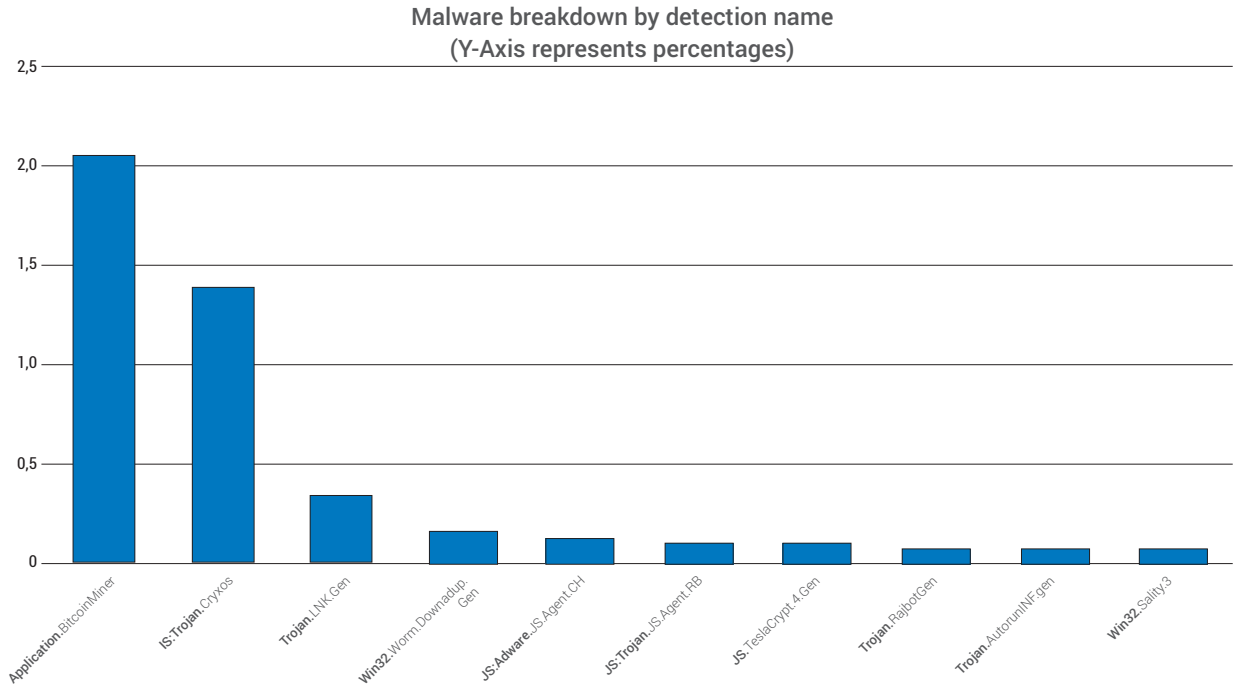
The Windows threat landscape at a glance

Bitdefender threat intelligence shows the United States is still the favorite destination for cyber-crime. The US ranks first in the number of malicious incidents detected throughout 2017 with 18.5 percent of incidents detected by the Bitdefender sensors.

Illicit Bitcoin miners dominate this year's top, accounting for more than 1.05 percent of all infections detected worldwide.

Application.BitdcoinMiner is representative of this category and consists of a legitimate miner configured to hijack mining efforts to various wallets. The application, along with its configuration file, is surreptitiously planted on victims' computers.

JS:Trojan.Cryxos is another interesting entry in the threat report for 2017. This detection deals with JavaScript code appended to hacked websites to display alarming popups. These Trojans are part of "call support" or "tech support" scams, where compromised websites also display a support number hosting cyber-criminals who offer "assistance" for a fee. Cumulatively, the Cryxos Trojan accounts for 1.39 percent of all malware reports.



Ranking third in the 2017 malware tops is an older threat dubbed Trojan.LNK. This detection deals with multiple families of malware that use maliciously modified shortcut files with a .LNK extension that are designed to trick users into mistakenly launching a malicious file.

Fourth place is taken by the Downadup worm, which is still active on unpatched computers. For almost 10 years, the Downadup worm has been a constant presence in the top threats since its emergence in 2008 , and it continues to spread and create scheduled tasks on infected computers.

Fifth and sixth places are taken by the JS:AdwareJS.Agent and JS:TrojanJS.Agent families, two very large categories of Trojans used for various purposes.

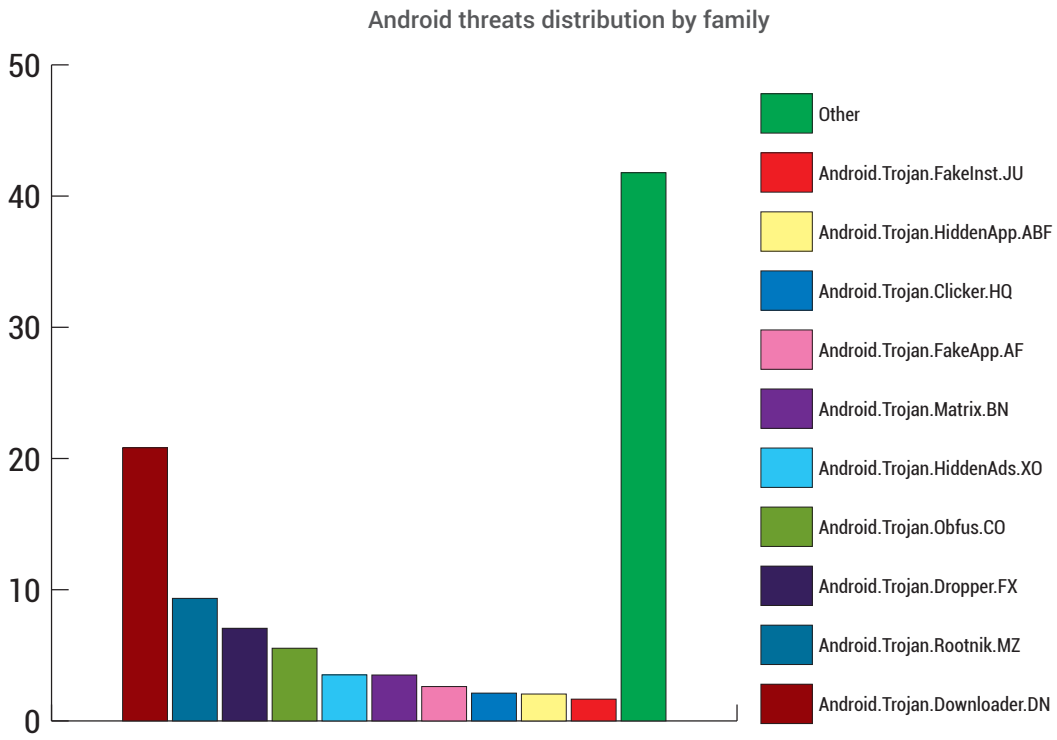
Ranking seventh, JS.TeslaCrypt4 is a generic downloader that brings the TeslaCrypt executable to the victim's computer. This threat comes bundled via e-mail and acts as a first-stage downloader that fetches and executes TeslaCrypt's current payload.

Trojan.Rajbot ranks eighth in the malware top 10 for 2017. This multi-functional piece of malware is written in Node.JS. It comes with its own JavaScript interpreter that allows it to execute outside of a browser and features a plug-and-play architecture that allows its reuse in various scenarios.

Ranking ninth in the top 10 malware threats for 2017, Trojan.AutorunInf is still active and associated to 0.7 percent of global malware reports. Even though its spreading mechanisms no longer work on modern operating systems, malicious Autorun files are still detected on removable media that have made contact with infected computers running Windows XP.

Win32.Sality ranks last in our list of most frequently encountered threats, with 0.06 percent of infections worldwide. This polymorphic file infector has been around for years. It infects executable files on local or removable storage media and joins the infected computer to a peer-to-peer network of compromised machines, where it awaits further instructions.

Android threats at a glance



Android. Trojan.Downloader.DN	**20,82%**
Android. Trojan.Rootnik.MZ	**9,34%**
Android. Trojan.Dropper.FX	**7,06%**
Android. Trojan.Obfus.CO	**5,54%**
Android. Trojan.HiddenAds.XO	**3,51%**
Android. Trojan.Matrix.BN	**3,50%**
Android. Trojan.FakeApp.AF	**2,62%**
Android. Trojan.Clicker.HQ	**2,12%**
Android. Trojan.HiddenApp.ABF	**2,05%**
Android. Trojan.FakeInst.JU	**1,66%**
Other	**41,78%**

One of the most prevalent Android malware families seems to be Android.Trojan.Downloader accounting for 20.82 percent of attacks. This family is known for tricking victims into downloading various types of fake applications, claiming to be legitimate Flash or Adobe updates. Usually distributed through compromised wesites or webpages containing adult content, this malware family is mosty used to spread malware with a wide range of capabilites.

The second-most-prevalent Android malware family is Android.Trojan.Rootnik (9.34 percent of attacks), which is known for using a wide range of commercial rooting tools to gain root access to infected devices. Its purpose is to steal information and download additional [4]

(malicious) apps to give attackers a permanent foothold and full control over the compromsied Android handset. With some samples of this malware family packing several rooting exploits, it's highly versatile and effective in the hands of cyber-criminals.

Another pervasive Android malware family is Android.Trojan.Dropper (7.06 percent) of attacks, meant to control the infected device and make it part of a botnet, amongst others. Some variants from this family have various abilities which include full Trojan-like capabilites, such as accessing and exfiltrating data or allowing remote access for cyber-criminals.

Another Android Trojan with data harvesting abilities is Android.Trojan.Obfus family (5.54 percent of attacks), which in some instances can also capture keyboard input or upload and download files to an attacker-controlled command and control (C&C) server. Not limited to only these "features," this particular malware family has samples that pack various malware functionalities.

Android adware is not uncommon either, and two families, Android.Trojan.HiddenAds (3.51 percent of attacks) and Android.Trojan.HiddenApp (2.05 percent) are notorious for displaying a plethora of ads once installed on victims' devices. Cyber-criminals often repackage legitimate applications with these aggressive adware families to get users to click as many ads as possible, generating reveue for the cybercriminal. While not malicious per se, these repackaged applications can significantly slow down a device's performance, display nag screens, and harm the overall user experience.

The Android.Trojan.Matrix malware family (3.50 percent of attacks) is a well-known Android malware family, normally meant to both root a users device to allow complete remote control and constantly prompt users to install additional malicious applications that have adware capablities or more malicious features. Usually distributed though fake applications presenting themselves as adult video streaming applications, the malware family generally targets older versions of Android.

Android.Trojan.FakeApp (2.62 percent of attacks) and Android.Trojan.FakeInst (1.66 percent of attacks) are two Android malware families usually distributed through tampered or fake popular Android apps. Their main purpose is to display ads, collect personal information from infected devices, and even send text messages to premium-rate numbers. Some variants of Android.Trojan.FakeInst are known to even pose as security solutions, usually prompting users to urgently install them to fix bogus security issues.

While arguably not as popular as the other Android malware families, the Android.Trojan.Clicker (2.12 percent of attacks) malware family is commonly used to redirect users to attacker-controlled websites to illegitimately boost traffic or prompt users with the installation of malicious apps. Some variants even let attackers turn infected devices into bots, and use them to perform Distributed Denial of Service (DDoS) attacks against particular victims.

What's next

As 2017 draws to an end, the Bitdefender threat analysis unit is already looking into the upcoming malware developments that will likely emerge in the year to come. Bitdefender experts predict an increase of zero-day exploits leaked from security agencies the world over, and massive changes to the way ransomware operates.

After years of focusing on individuals, malware authors will increasingly target enterprises and networks of computers. Lateral movement will become standard in most malware samples, either via password-grabbing utilities like Mimikatz, or by exploiting wormable vulnerabilities.

The number of malicious attachments in SPAM emails will increase, particularly those written in scripting languages such as PERL or Python. Fileless attacks will also increase sharply as Windows 10 adoption becomes universal, leveraging the platform's support for Powershell or Linux Bash.

The threat landscape will remain faithful to the malware that monetizes best: ransomware, banker Trojans and digital currency miners, but these threats will undergo major changes in the way they perform. We expect to see ransomware that leverages GPU power for encryption purposes to move faster and attempt to circumvent antimalware products.

Bitdefender experts also expect major changes in the PaaS (polymorphism as a service) market, a vertical that will consolidate throughout 2018. Advanced polymorphic engines running in the cloud are already used by cyber-criminals to flood the market with unique variants of known malware and the advantages they offer cyber-criminals are extraordinary. Licensing access to these custom engines will likely generate good business for these actors.

Such polymorphic engines will also be complemented by machine learning algorithms put to bad use. In 2018, we expect to see increased efforts on anti-machine-learning techniques that will advance in two major directions: creating and spreading samples that will make the security vendor create false positives or manipulating the payload until it becomes undetected.

In 2018, threat actors will also research vulnerabilities in components that reside below the operating systems, such as firmware. The WiFi and Bluetooth stacks will get increased attention as any potential vulnerabilities identified here offer a stealth backdoor by design that is very difficult to detect and mitigate.

Large IoT botnets will become the new normal in 2018. Source code for IoT bots is already available for free on the Internet, and cyber-crime groups interested in compromising IoT devices already have a solid platform to customize to their own needs. We predict this code will be improved in 2018 to allow lateral movement inside the compromised network for ransomware or spam-sending purposes.

Last but not least, we expect increased activity in the OS X space. For consumers, malware will likely focus on scareware tactics to force victims into paying for useless tools. Enterprises will likely see more targeted attacks, as well as malicious payloads used in advanced persistent threats.

About Bitdefender

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.

BD-Business-Nov.21.2017-Tk#:CREA-2186
Bitdefender-Business-2017-Whitepaper-threat_landscape-crea2186-en_EN