Bitdefender®

Encrypting Businesses – ransomware developers' favorite cash cow

Bitdefender shields from prolific threats against all OSs

Abstract

Ransomware, the most prolific cyber threat of the moment, gains foothold in organizations and companies via file-sharing networks, e-mail attachments, malicious links or compromised websites that allow direct downloads. The first quarter of 2016 saw 3,500% growth in the number of ransomware domains created, setting a new record.

According to a Bitdefender study carried in the United States last year, ransomware is mentioned second in the top CIO concerns for medium and large companies. According to the findings of that study, 13.7 percent of the interviewed companies perceive ransomware as a hard-to-tackle threat. The study also shows that ransomware and rootkits are perceived as particularly difficult to tackle by companies with limited experience in malware attacks.

Ransomware was seen as a major threat in the top predictions list in cyber security for 2016 by Bitdefender CTO Bogdan Dumitru. This March, Palo Alto Networks researchers revealed KeRanger ransomware targeted Mac users for the first time, realizing Bitdefender's predictions about ransomware's expansion to new operating systems in 2016.

"We've already seen ransomware for Linux, Windows and Android. Mac OS is just around the corner," he said in December 2015. "It targets both consumers and companies, and the 2016 versions not only will encrypt files and ask for ransom, but will also make all documents available on the internet if ransom is not paid. In an ironic twist, the victim will be able to recover encrypted files – when they are uploaded on the internet for public shaming."

"Ransomware has probably been the largest unresolvable threat to Internet users ever since 2014, and it will remain one of the most important drivers of cybercrime in 2016," Bitdefender noted. "While some operators will prefer the file encryption approach, some more innovative groups will focus on developing 'extortionware' (malware that blocks accounts on various online services or that expose data stored locally to everybody on the Internet). Throughout 2016, file-encrypting ransomware will most likely expand to Mac OS X as well."

Last year, reports show millions of users fell victim to CryptoWall version 3.0 (and many go unreported), adding over $350 million to cyber-criminals' bank accounts.

Top Countries Affected by PC Ransomware

PC and mobile threats have increased in both numbers and complexity for the past couple of years. However, some malware strands have proliferated more than others, mostly because cybercriminals have been using them for generating huge revenue streams from infected victims.

File-encrypting malware – known as ransomware – is a type of malware that has generated over hundreds of millions of dollar from extortion, the FBI even estimating that it could lead to more than 1 billion dollars in financial losses by the end of 2016.

Ransomware has not only become a growing threat for PCs, but also for Android-running devices. During the first half of 2016, the largest number of ransomware reports came from the United States, with 19.09 percent of the total number of ransomware reports, globally.

The United Kingdom came in second, with 11.89 percent, just only 2.26 percentage points above Germany (9.63 percent) that ranked third in our most affected countries targeted by ransomware.

However, in terms of some of the most prolific ransomware families, worth noting is that the largest number of ransomware incidents seem to involve delivery via JavaScript files. Either embedded in email attachments or distributed via malicious websites, it seems to be the most popular method used by cybercriminals when infecting victims. Some 44.98 percent of all ransomware reports account for JavaScript files being used to smuggle ransomware on victims' PCs.

One of the reasons for why we've seen JavaScripts ranking so high in our report could point to cybercriminals looking to avoid having their droppers being marked by security solutions and to obfuscate the domain names from where the ransomware downloader is being downloaded.
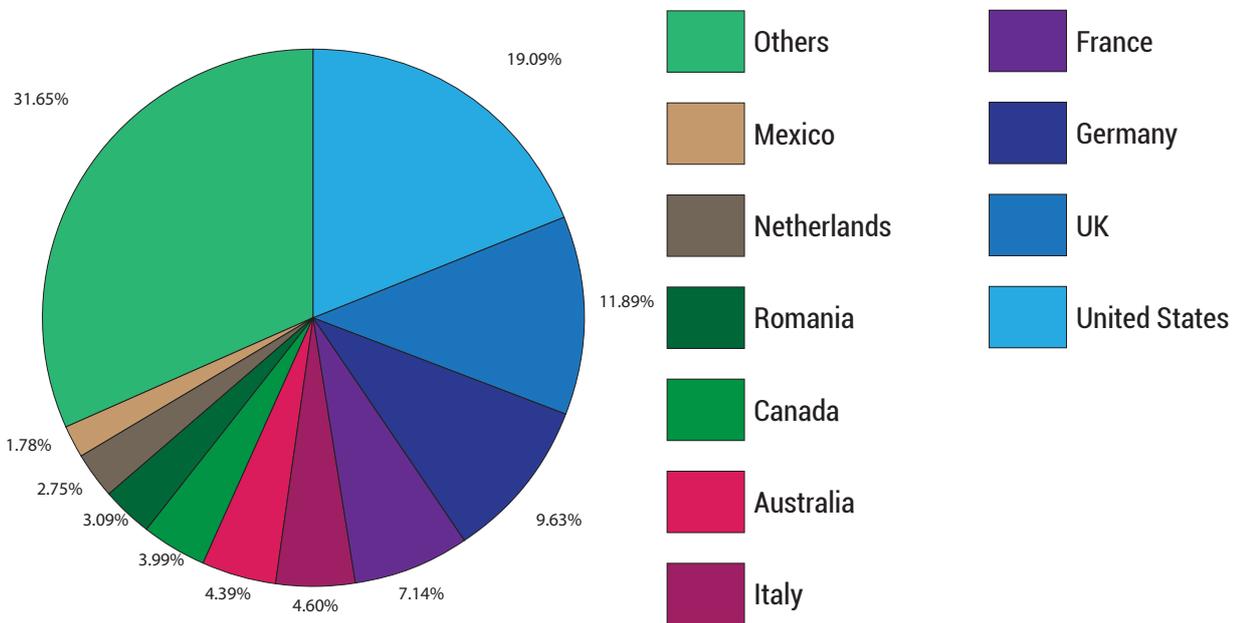
Top Countries Affected by PC Ransomware H1 2016*

Ranking second with 9.29 percent of all ransomware reports, the Teslacrypt ransomware family seems to have been a popular "weapon of choice" in terms of cybercriminal activities. CTBLocker and Cryptowall are also in the top 5 most prevalent ransomware families, scoring 8.67 percent respectively 7.05 percent of the total number of malware reports globally. Cryptowall and Bedep scored 4.34 percent and 2.72 percent, while Petya – that **Bitdefender Labs analyzed** a while back – got 1.80 percent of the total number of ransomware reports.
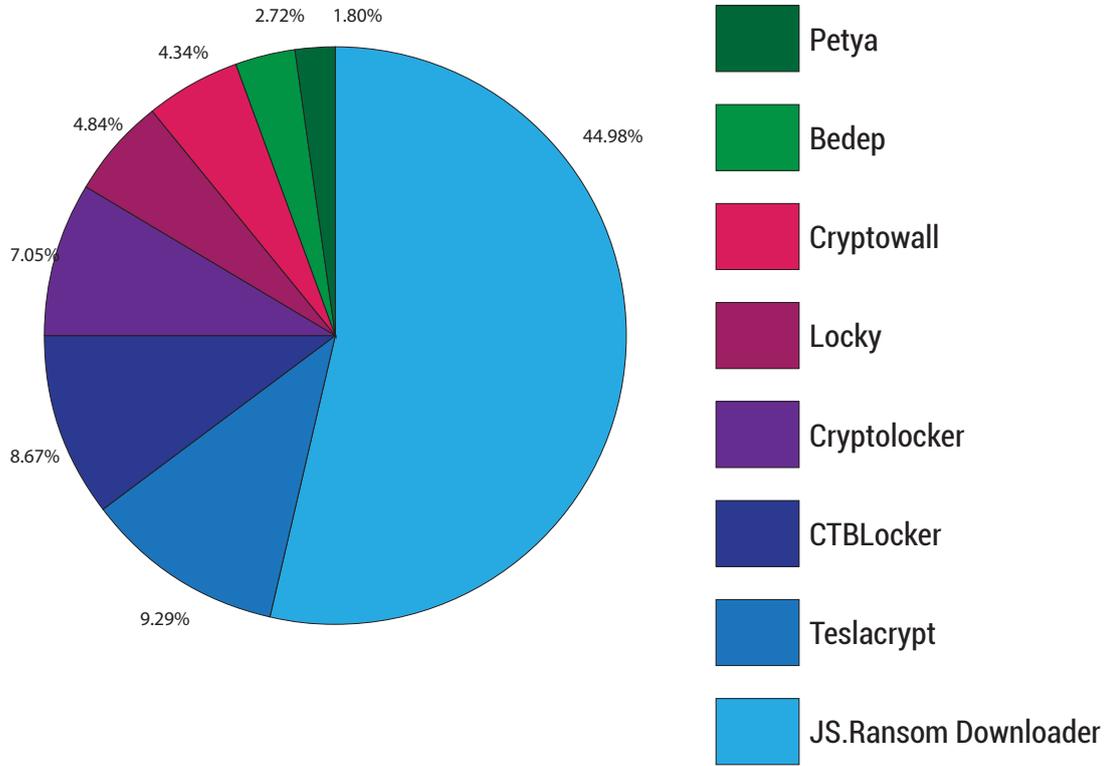
Top Global PC Ransomware Families*

When it comes to picking out some of the most popular ransomware families that have targeted specific countries, Teslacrypt, CTBLocker and Bedep are amongst the top three ransomware families that seem to be really popular with cybercriminals.

[4]

Top PC Ransomware Families H1 2016 in United States

Some 12.83 percent of the total ransomware reports in the United States accounts for Teslacypt reports, making – by far – the most significant threat. With 5.78 percent of reports, Cryptolocker is less than half the number of reports for Teslacrypt, with 5.78 percent of reports. Bedep is close behind with 3.99 percent of ransomware reports in the US, with the the top three ransomware families accounting for more than 20 percent (22.6 percent) of the total ransomware reports in the United States.
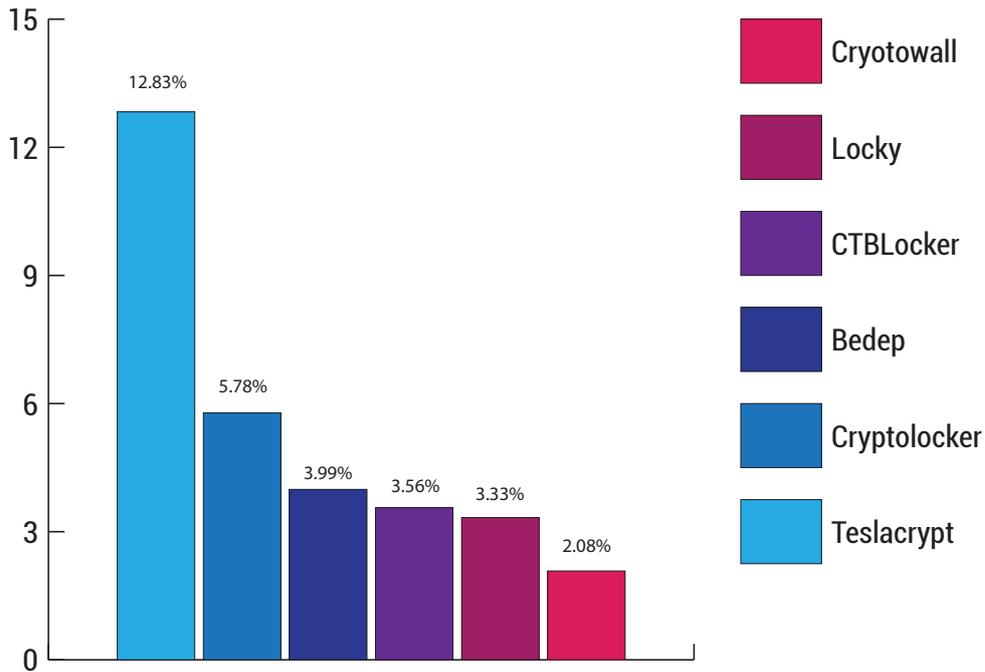
Top PC Ransomware Families US H1 2016*

Top PC Ransomware Families H1 2016 in United Kingdom

Unlike the United States where the Teslacrypt ranked first, in the UK Bedep is by far one of the most popular weapons of choice for cybercriminals. With some 34.71 percent of the total ransomware reports in the country, Bedep occurrences seem to account for 1 in 3 of all ransomware occurrences. Cryptowall ransomware reports clocked in second with 5.52 percent of all UK ransomware reports, followed closely by Teslacrypt with 4.87 percent.
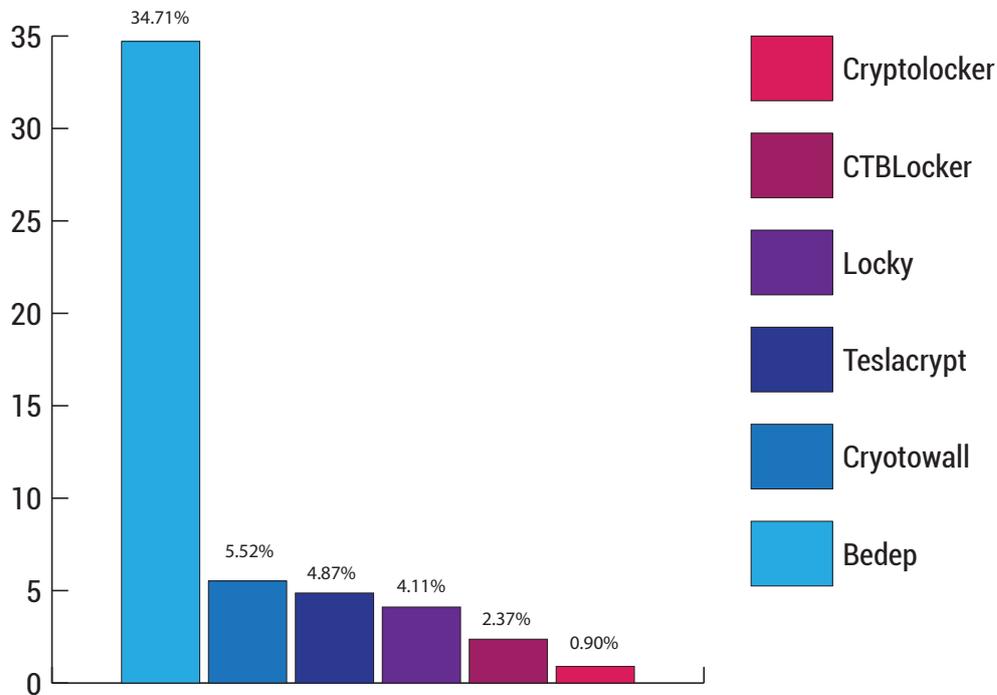
Top PC Ransomware Families UK H1 2016*

An interesting takeaway from these findings is that cybercriminals seem to have been targeting Brits with Bedep ransomware, which is interesting as security researchers **have found** it to be usually delivered via the Angler Exploit Kit. Consequently, drive-by attacks is usually the method through which Bedep usually ends up executing on victims' machines. Either via legitimate websites that have been used in the dissemination process or via fully malicious websites, Brits seem more prone to web-related attacks rather than infected email attachments – the usual culprit for ransomware dissemination.

Top PC Ransomware Families H1 2016 in Germany

Just like in the UK, the number one ransomware family far outranks the second most prolific family by far. CTBLocker got 22.80 percent of the total number of ransomware reports in Germany, with Teslacrypt ranking second with only 6.18 percent. The Cryptowall ransomware family ranked third with only 3.44 percent of ransomware reports.

Legend:
- Bedep
- Cryptolocker
- Locky
- Cryotowall
- Teslacrypt
- CTBLocker

Bar chart values:
- 22.80%
- 6.18%
- 3.44%
- 2.84%
- 2.53%
- 1.11%
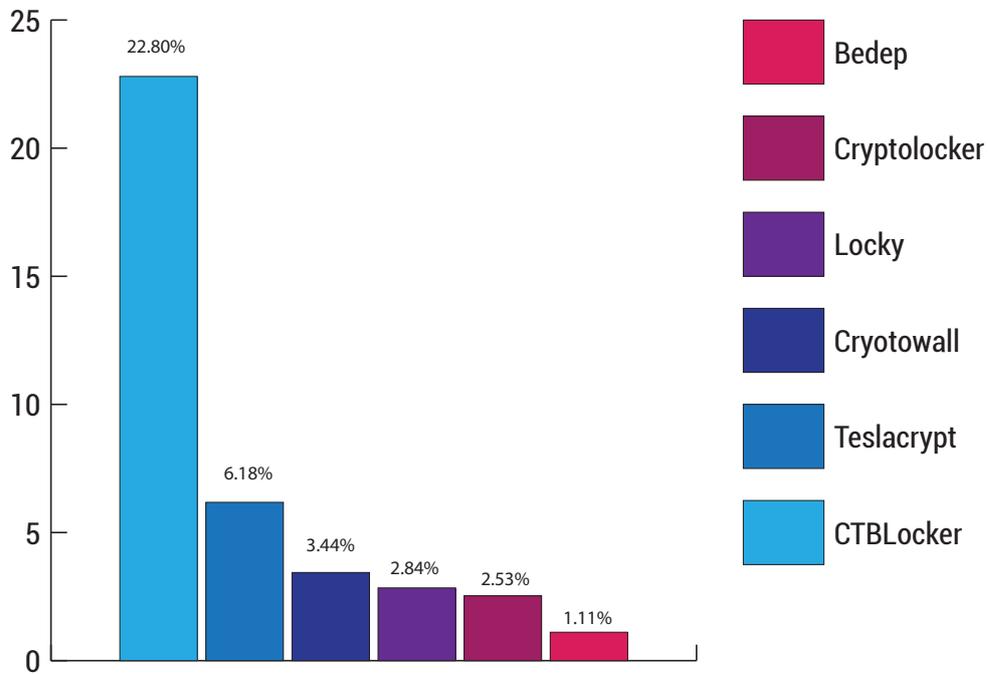
Top PC Ransomware Families Germany H1 2016*

Unlike the United Kingdom where most ransomware infections were delivered via drive-by downloads, the main infection vector for Germany in terms of delivering CTBLocker usually relates to infected email attackmen's and fake downloads. Encrypting files and renaming them with the .ctbl file extension is usually a good sign that infection with CTBLocker has occurred, that's unless it's clearly specified in the payment instructions.

Top PC Ransomware Families H1 2016 in France

A bit out of the ordinary when compared to the previously analyzed countries, the top three threats in France together account for 22.52 percent of the total number of ransomware infections. Teslacypt rankes first with 9.38 percent of total ransomware repots, Locky ranks second with 7.48 percent, and Cryptolocker ranked third with 5.66 percent.
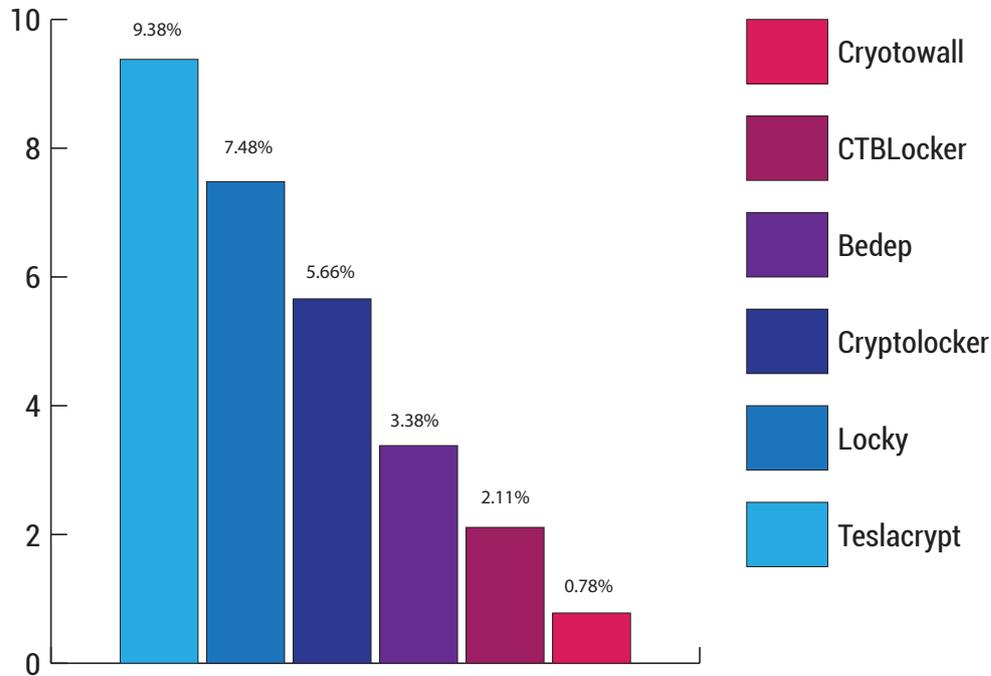
Top PC Ransomware Families France H1 2016*

Because the difference between the top three is marginal, it seems that cybercriminals have been using a wide array of techniques to infect victims. If other countries have been particularly targeted by specific ransomware infections, when it comes to France it seems they've been using all the tricks in the book to deliver ransomware.

Top PC Ransomware Families H1 2016 in Australia

As with France, the top three ransomware threats in Australia are pretty close to each other in terms of reports, with Teslacrypt ranking first with 9.22 percent of all ransomware reports in the country. Locky is close behind with 8.62 percent, and Cryptolocker ranked third with 5.76 percent or reports.
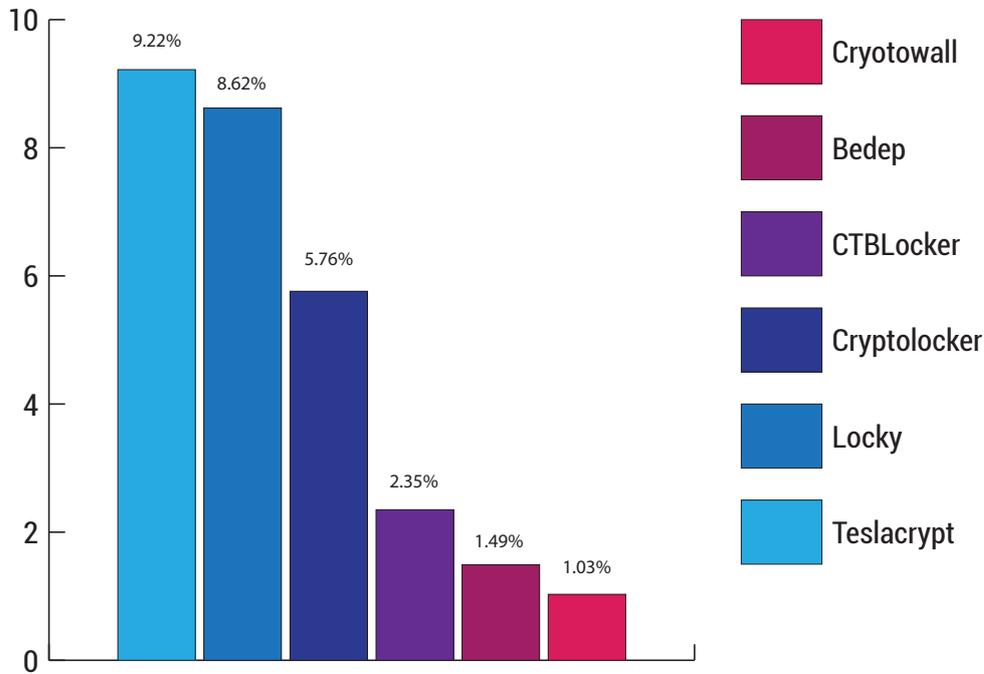
Top PC Ransomware Families Australia H1 2016*

With the top three ransomware threats accounting for 23.6 percent of all ransomware reports in Australia, chances are that around 1 in 4 ransomware infections was one of the three ransomware families previously mentioned.

Top PC Ransomware Families H1 2016 in Romania

Romania is probably one of the most atypical in terms of ransomware reports, as the percentages between the top three ransomware families is even tighter together. While Teslacrypt may hold the pole position with 10.97 percent of all ransomware reports in the country, Locky follows closely with 9.59 percent, and Cryptolocker comes in third with 8.52 percent.
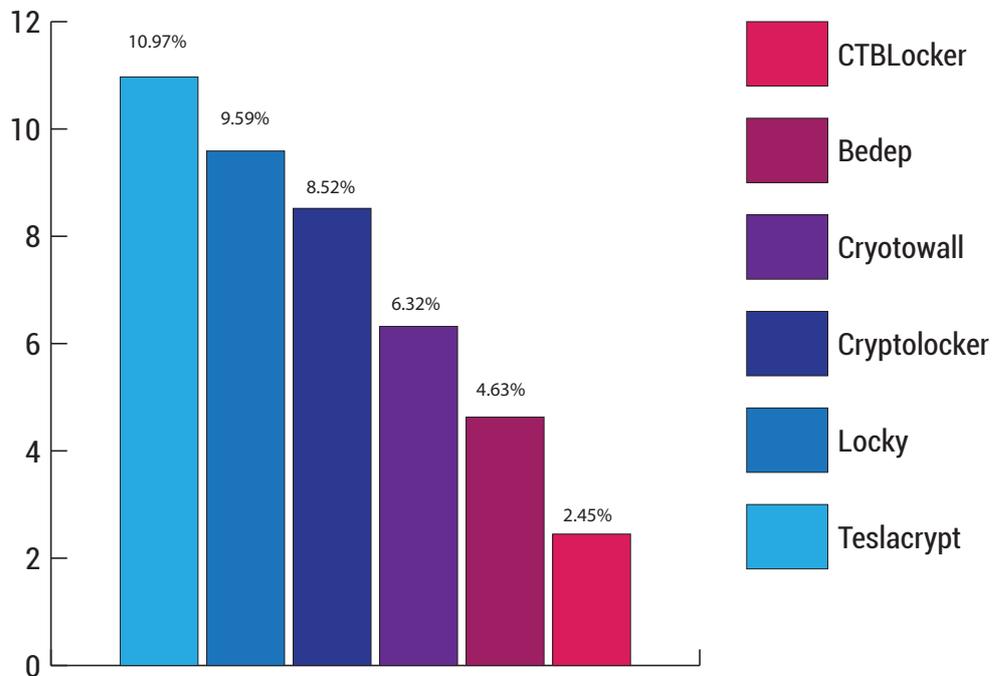
Top PC Ransomware Families Romania H1 2016*

These reports probably suggest that again cybercriminals have been deploying as many ransomware samples as possible, using diverse attack vectors, as to make sure they infect a large pool of victims with various online behavior. While some might have been infected via drive-by downloads, infected attachments and fake installers seem to have also been deployed for successful ransomware infection.

Android Ransomware

With Android dominating the mobile market share with a whopping 87.6 percent, **according** to IDC, malware developers have been focusing their attention towards developing threats that specifically target this operating system. Since PC ransomware has proven to be an excellent revenue source, it was only a matter of time until it would have been ported for the Android operating system.

While we've seen Android ransomware show up in **previous mobile threat landscape reports**, during this first half of 2016 this particular threat has gained significant traction in terms of both numbers and complexity. Some of the most affected countries in which the Android. SLocker ransomware family has been most reported include Germany, Australia, UK, and the United States.

Top Countries with Most Ransomware Reports

While the Android ransomware problem has been spotted across the world, affecting all countries regardless of their economic development, it does seem that Germany has taken the blunt of it. With 25.64 percent of all Android malware reports in Germany, more than 1 in 4 were related ransomware samples.
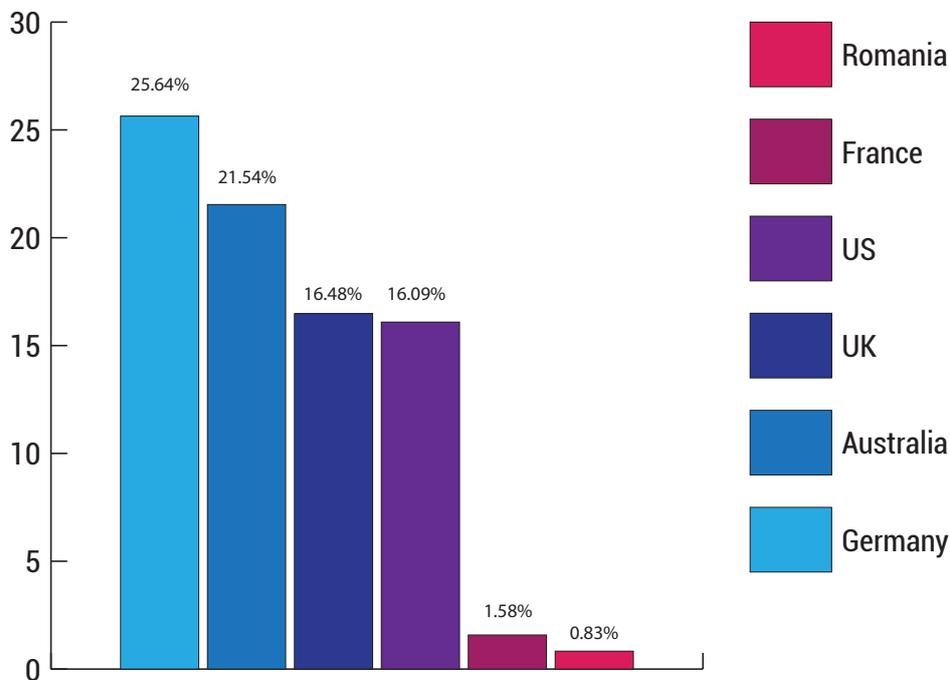
Android.Trojan.Slocker Ransomware Family Distribution per Country*

While Germany might seem to have the highest count of ransomware, Australia ranks second with just a couple of percentage points below, with Android ransomware scoring 21.54 percent of the total local number of malware reports. While the two countries might be on the opposite sides of the world, cybercriminals seem to have been focusing on them probably because of the high Android OS penetration as well as because respective users are more likely to pay to recover their data, rather than loose it.

The UK and the United States are both pretty close together in terms of ransomware reports, with the UK clocking 16.54 percent and the US 16.48 percent. However, while the percentages might look somewhat similar, there's probably a considerable difference in terms of the actual number infections between the two. That's probably because the reports are coming from two totally different user bases.

While France and Romania have been scoring 1.58 percent, respectively 0.83 percent in terms of local ransomware reports, this is probably a good thing, as it either means that users are far more aware of the security of their devices or they're simply not that of an appealing target for cybercriminals.

Android Ads, Fake Installers, and Hidden Apps Still Top Threats Globally

As seen in some of pour previous Android malware landscape reports, fake installers and applications riddled with adware remain a constant threat for mobile users. While cybercriminals have been focusing ransomware on more economically developed countries, Adware and fake installers seem to be mostly focused at countries where ransomware reports have been most scares.

To that end, Romania seems to have the largest number of reports in terms of adware, with the Android.Trojan.HiddenAds malware family ranking first – 22.52 percent – of all malware reports locally. By comparison, the same malware family only accounted for 14.76 percent of all malware reports in France, 13.66 percent in UK, 11.14 percent in Germany, 11.13 percent in the United States, and 9.50 percent in Australia. While malware developers might not be targeting Romania and France with ransomware, they do seem to be generating revenue from users installing applications injected with aggressive adware.
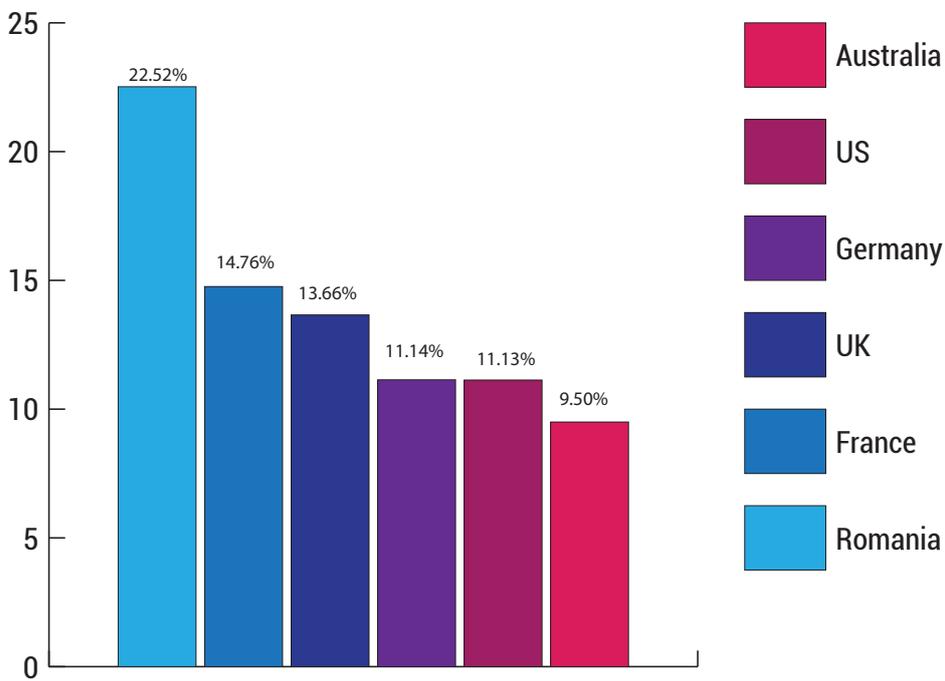
Android.Trojan.HiddenAds Malware Family Distribution per Country*

One of the consequences of installing applications riddled with aggressive adware is that users will constantly be prompted with popups, browser redirects and battery drainage cause by this constant activity. While they're not malicious per se, they do tend to irk uses and ruin the entire user experience on Android devices.

In regards to applications posing as popular apps as to trick users into installing them, the Android.FakeInst malware family has been mostly reported in U.S., with 4.87 percent of all local Android malware reports. The Australia, France, and Germany follow closely behind with 1.63 percent, 1 percent, respectively, 0.97 percent each, from their respective number of local malware reports.
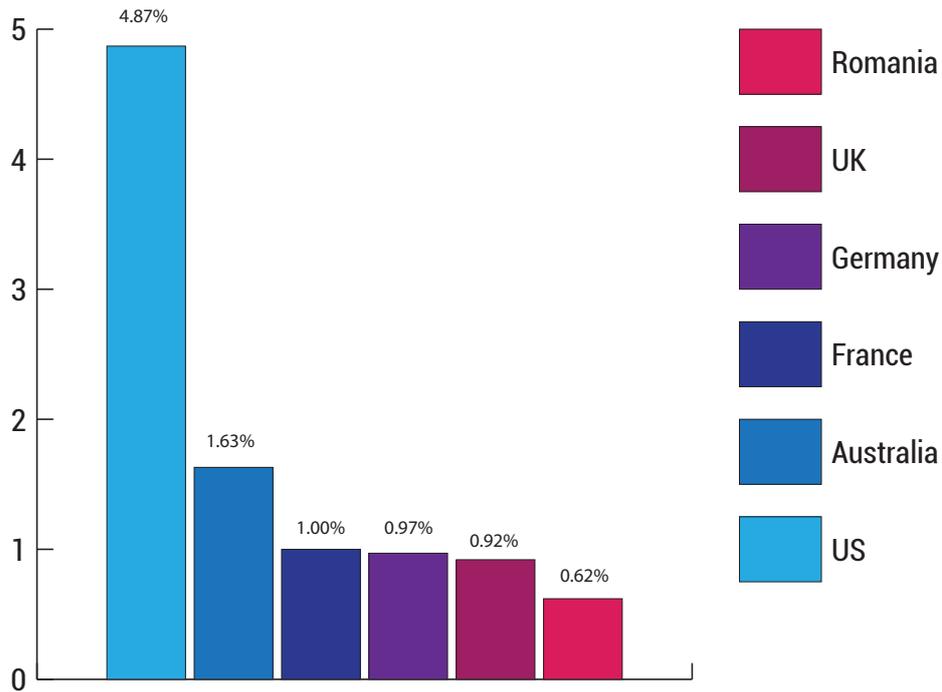
Android.Trojan.FakeInst Malware Family Distribution per Country*

Quite often, this type of malware family poses as mobile security software in order to trick unsuspecting users into downloading them. After performing fake system scans they usually scare victims into paying various amounts of money as to unlock the "full features" of the applications and clean up the Android device from all the (fake) malware. Of course, payment options rarely include traceable services, such as PayPal, and quite frequently involve the use of "MoneyPack" or other similar payment options.

Another type of Android malware family is known as Android.HiddenApp and its purpose is to both trick users into installing it and hide its presence – by changing its name into something like "System Manager" - once it's installed on the device. From there, it starts prompting users to install additional applications featuring aggressive ads or simply subscribes victims to premium rated numbers.
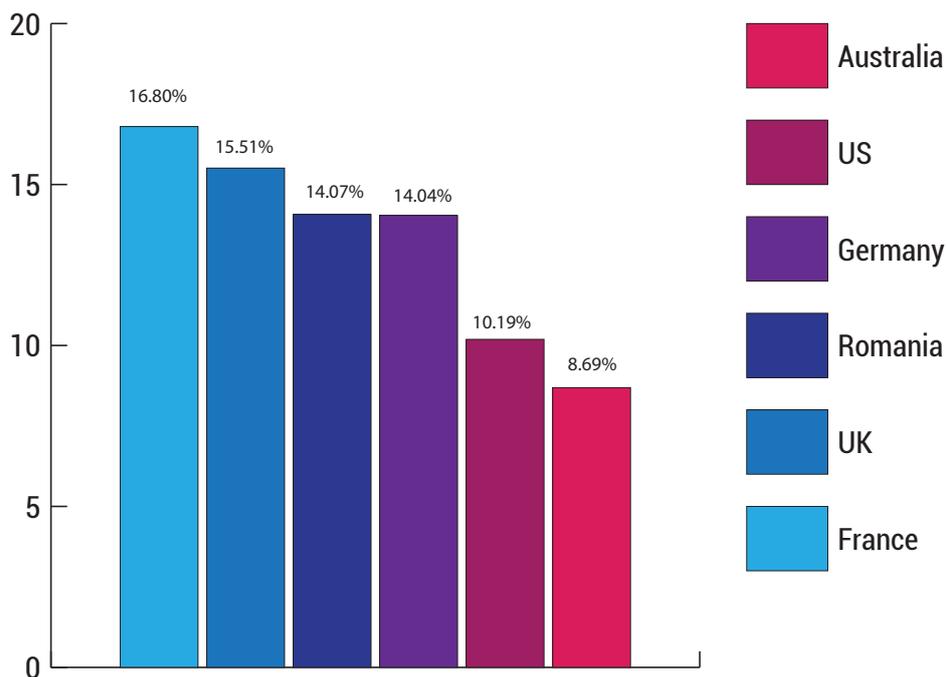
Android.Trojan.HiddenApp Malware Family Distribution per Country*

While most of these applications are usually downloaded and installed from third party marketplaces, there have been instances where they have been found in the **official** Google Play store.

The Android.HiddenApp family seems to have been mostly reported in France (16.80 percent), followed by UK (15.51 percent), Romania (14.07 percent), and Germany (14.04). That's probably not a coincidence considering that the Android.HiddenApp malware family seems to have been present in the same countries.

Patented Machine Learning in Ransomware Detection

With more than 7 issued patents for using machine learning algorithms in detecting malware and other online threats, the use of deep learning and anomaly based detection techniques play a vital role in proactively fighting new and unknown threats.

Ransomware has not only become a scourge for Windows-based operating systems, but it has also targeted Android mobile operating system for years. With financial losses estimated in the hundreds of millions, some estimating that it's could reach close to **one billion dollars** by the end of 2016, traditional security mechanism and technologies have fell short of completely protecting against it.

At Bitdefender we've been working on machine learning algorithms since 2009, constantly developing and training them to identify new and unknown threats. Artificial Intelligence and machine learning are essential to combat a threat landscape that is larger and more sophisticated than ever. Unlike other vendors, Bitdefender has years of experience in perfecting these technologies and the results clearly show this: better detection rates with fewer false positives.

Machine learning algorithms have the ability to significantly improve detection time for ransomware threats, as they're able to analyze large amounts of data significantly faster than any human would. If properly trained to accurately detect various types of ransomware behavior, machine learning algorithms can have a high detection rate even on new or unknown samples.

The merging of human ingenuity with machine learning speed and relentless data analysis, significantly reduces reaction time against new ransomware samples, offering protection even from previously unknown ransomware samples. However, it's not always just a single machine learning algorithm doing the detection. Detecting ransomware requires the use of several algorithms, each specialized in detecting specific ransomware families with individual behaviors. This significantly increases the chances of detecting similarly-looking ransomware while reduces the amount of false positives.

By training machine learning algorithms on large datasets of ransomware samples, they're able to quickly reveal indicators of compromise and help the security solution prevent new or unknown ransomware samples from encrypting files.

Multiple anti-ransomware defenses with Bitdefender Gravity Zone

Using advanced behavior-based technologies, Bitdefender detected 99% of unknown threats in independent trials run by reputed independent testing organization, AV-Comparatives.

Bitdefender Advanced Threat Control (ATC) permanently monitors running processes for signs of malicious behavior. A pioneering technology launched in 2008 as AVC (Active Virus Control), ATC has constantly been enhanced, keeping Bitdefender one step ahead of emerging threats.

Bitdefender also has two additional anti-ransomware defense layers – a blacklist of 2.8 million samples and rising, and a vaccine that can immunize devices against the encryption process.

This spring, Bitdefender was able to analyze the Petya ransomware and offer potential victims a tool that intercepts the encryption process and offers the decryption key, free of charge. Most importantly, the tool needs to be installed prior to being infected - not afterwards – in order to perform its function correctly.

Previously, Bitdefender anti-malware researchers have released a new vaccine tool which can protect against known and possible future versions of the afore-mentioned CTB-Locker, Locky and TeslaCrypt crypto ransomware families by exploiting flaws in their spreading methods. These are still some of the most prevalent types of ransomware to date, according to Bitdefender's internal intelligence.

Last November saw the emergence of an interesting piece of ransomware targeting vulnerable Linux web servers. Fortunately, a programming flaw allowed Bitdefender researchers to get hold of the decryption key and provide victims with a free recovery utility. Two

months later, the world's first piece of fully functional Mac OS X ransomware relied on a rewrite of the famous Linux.Encoder.

Useful steps to stop your business from being hit by ransomware[1]:

- Regularly back up data and verify the integrity of those backups. Backups are critical in ransomware incidents; if you are infected, backups may be the best way to recover your critical data.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might include securing backups in the cloud or physically storing them offline. It should be noted, some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real-time, also known as persistent synchronization.
- Scrutinize links contained in e-mails and do not open attachments included in unsolicited e-mails.
- Only download software – especially free software – from sites you know and trust. When possible, verify the integrity of the software through a digital signature prior to execution.
- Ensure application patches for the operating system, software, and firmware are up to date, including Adobe Flash, Java, Web browsers, etc.
- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Disable macro scripts from files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full Office Suite applications.
- Implement software restrictions or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.

Additional considerations for businesses include the following:

- Focus on awareness and training. Because end users are often targeted, employees should be made aware of the threat of ransomware, how it is delivered, and trained on information security principles and techniques.
- Patch all endpoint device operating systems, software, and firmware as vulnerabilities are discovered. This precaution can be made easier through a centralized patch management system.
- Manage the use of privileged accounts by implementing the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary; they should operate with standard user accounts at all other times.
- Configure access controls with least privilege in mind. If a user only needs to read specific files, he or she should not have write access to those files, directories, or shares.
- Use virtualized environments to execute operating system environments or specific programs.
- Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organizational units. For example, sensitive research or business data should not reside on the same server and/or network segment as an organization's e-mail environment.
- Require user interaction for end user applications communicating with Web sites uncategorized by the network proxy or firewall. Examples include requiring users to type in information or enter a password when the system communicates with an uncategorized Web site.
- Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.

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/.

*Source: Btidefender's internal intelligence
Authors: Liviu Arsene, Security Specialist; Răzvan Mureșan, Security Specialist.

---

1   "Ransomware victims in the US urged to report infections, FBI warns", Sep 19, 2016, citing FBI recommendations, "Ransomware victims urged to report infections to federal law enforcement", https://www.ic3.gov/media/2016/160915.aspx

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at
http://www.bitdefender.com/