COMODO

# Comodo Threat Research Labs

## Q1 2017 REPORT

# Table of Contents

# Executive Summary

## Overview

- Comodo Research Labs detected over 25 million malware incidents in Q1 2017
  *This is a staggering number, with serious ramifications for government, law enforcement, military, and intelligence personnel worldwide.*
- Comodo discovered malware in 223 top-level country code domains (ccTLD)
  *On planet Earth, wherever there is human civilization, there is malware. Comodo detected malicious code in almost every nation, province, state, city, and vertical.*
- The highest number of malware detections were in Russia, Taiwan, Hong Kong, Philippines, Indonesia, the U.S., Turkey, Poland, Brazil, and the UK
  *Malware is a highly flexible weapon, with certain families targeting rich nations due to a high return on investment and others targeting poorer nations due to outdated or unmanaged software.*

## Malware Detections

- 13M+ trojans in 223 countries
  *In most countries, trojans are the #1 malware threat. Trojans are a versatile weapon, offering the same rights and privileges as a local user, and can be used for myriad purposes, including the installation of ransomware.*
- 9M+ viruses in 183 countries
  *In 2017, self-replicating virus code seems to predominate in Asia, with Taiwan, Hong Kong, Russia, Philippines, Indonesia, Kazakhstan, Turkey, and India among our top ten most affected countries.*
- 4M+ computer worms in 187 countries
  *Autonomous, self-propagating worms afflicted countries at the lower socio-economic tier of nations. For countries with a minimum of 100 detected worms, Congo, Maldives, Somalia, Cape Verde, Macedonia, Philippines, Nigeria, Yemen, South Africa, and Gambia had the highest percentage of worms compared to overall malware detections.*

- 1M+ malware packers in 173 countries

  *Packers hide or obfuscate malicious software by compressing or "packing" executable code. The top three victim nations in this category were significantly richer nations: The United Kingdom, Japan, and the U.S. The number of unique malware families was smaller, with the tiny, versatile, and efficient "modified Ultimate Packer for Executables," or MUPX, topping the list in 167 countries.*

- 900K+ backdoors in 153 countries

  *Hidden ways to bypass normal user authentication were discovered more often targeting richer nations with Belgium, Spain, Bahrain, Singapore, Saudi Arabia, the U.S., Germany, and the United Kingdom having a high ratio of backdoors to overall malware detections. This suggests that attackers likely deploy higher-grade malware against more lucrative or better-defended targets, with a goal of achieving a higher return on investment.*

**Current Trends**

- 99K+ ransomware detections in 127 countries

  *Ransomware, as evidenced by the recent outbreak of Wannacry, is a rising threat, which may only get worse as the Internet of Things expands quickly around the world. In Q1 2017, over 25% of Comodo ransomware detections were found in either Russia or Iran. However, Poland and the U.S. saw a sharp rise toward the end of the quarter. In 2017, Comodo has detected 44 unique families of ransomware, but unless a solution to this new malware threat is found, that number may rise dramatically in the near future.*

- Technology is the most targeted vertical and the most complex data set

  *Comodo undertakes strategic malware analysis, in part by placing its clients into "verticals", or economic sectors, to analyze the scope, intent, and impact of cyberattacks upon them individually and for comparative purposes. Based on our Q1 data, it is clear that hackers place a premium on undermining the security of high technology, including telecommunications and online services, especially in the West.*

**Recommendations**

- Hire qualified cybersecurity personnel

  *Given the highly technical and quickly evolving nature of the cyber threat landscape, it is critical that enterprises hire, train, and retain qualified cybersecurity personnel. Many cyberattacks have unique aspects, and it is hard to predict where the attackers will strike next, or what the next attack will look like.*

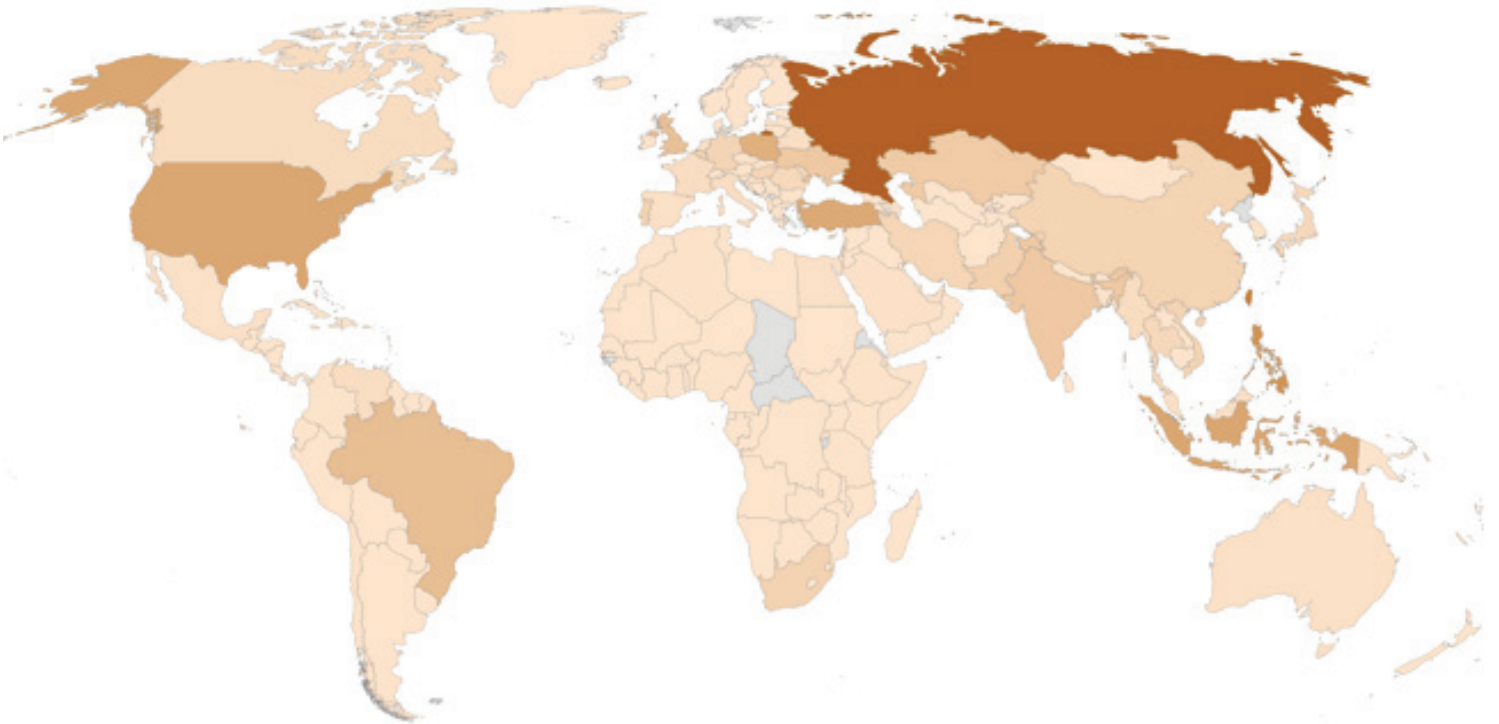
- Keep skills, software, and processes up to date

  *Attackers prey on vulnerable hardware and software. Therefore, system administration and security personnel must strive to keep their skills, equipment, and software as current as possible through proper configuration, hardening, minimization, and patching.*

## Malware Analysis

In Q1 2017, Comodo detected more than 25 million malware incidents within 223 country code top-level domains (ccTLD), spanning nearly the entire globe. These numbers show that malware is a global problem, with malicious code continually crossing international borders with little regard for national sovereignty or law enforcement jurisdiction. However, systematic malware analysis shows that certain types of malware tends to cluster within certain countries, verticals, and even enterprises. Understanding this strategic context can help security architects to design more logical and efficient cyber defenses.

The map below displays Comodo's malware detections on a traditional map. Countries are shaded based on the number of malware detections that Comodo security software discovered. The top ten countries affected by malware were Russia, Taiwan, Hong Kong, Philippines, Indonesia, the U.S., Turkey, Poland, Brazil, and the UK.



Clearly, malware is a worldwide phenomenon and can be found across the internet and throughout Planet Earth. The table below lists the top ten countries, including the overall number of malware detections within each country and their percentage of Comodo detections throughout the world for Q1 2017.

| | | | |
|---|---|---|---|
| 1 | Russia | 3,027,125 | 11.83% |
| 2 | Taiwan | 2,272,681 | 8.88% |
| 3 | Hong Kong | 1,977,522 | 7.73% |
| 4 | Philippines | 1,829,659 | 7.15% |
| 5 | Indonesia | 1,397,740 | 5.46% |
| 6 | USA | 1,392,776 | 5.44% |
| 7 | Turkey | 1,327,555 | 5.19% |
| 8 | Poland | 1,173,002 | 4.59% |
| 9 | Brazil | 867,196 | 3.39% |
| 10 | United Kingdom | 801,649 | 3.13% |

It is significant that Russia displays so prominently in our data, demonstrating that while Russia is alleged to have been the source of many celebrated international cyberattacks, from The Cuckoo's Egg to Moonlight Maze, Estonia, and the Democratic National Committee, it also suffers greatly from the presence of malicious code within its own national borders.

The other countries in the top five are all in Asia, which is also noteworthy. Taiwan, Hong Kong, Philippines, and Indonesia are geographically proximate, roughly circling the South China Sea. In our Q1 Report, we found a number of such correlations, indicating that malware sometimes clusters in regions that share geographic, linguistic, socio-economic, or technological commonalities.

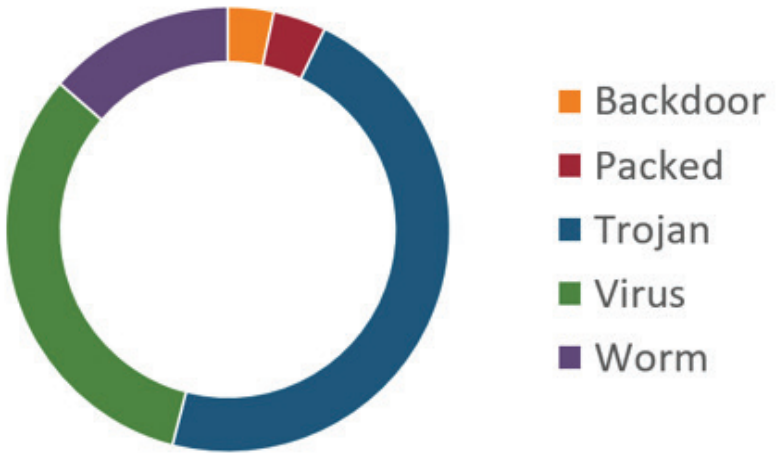
The graphic below shows the same malware data in another way, broken down by ratio and country code. Here, it is possible to see Comodo Q1 malware detections according to the rough proportion of the overall total that each nation experienced.


This view is helpful because it quickly allows many more countries to see where they fall within the larger malware ecosystem. The countries are designated by their country code top-level domain (ccTLD) names. Here, it is clear that every country in the world, from Brazil to Ukraine, Pakistan, South Africa and Iran, are confronting significant threats from malware.

Comodo security software searches the entire planet for dozens of malware types, subtypes, families, attacks, and campaigns. The five most common malware types that Comodo detected in Q1 2017 were:

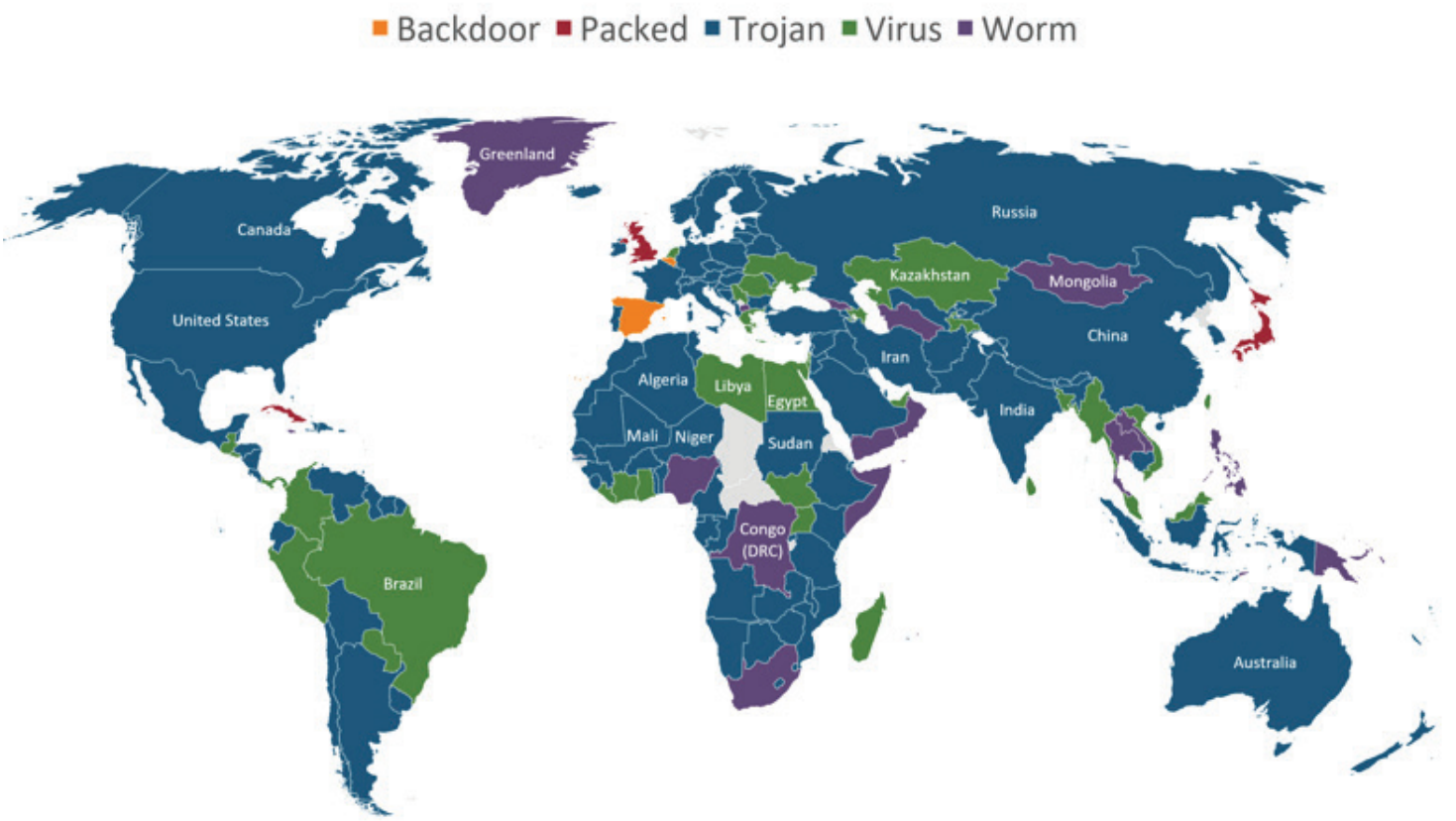
- Backdoor (993,282 incidents)
- Packed Malware (1,148,231 incidents)
- Trojan (13,947,885 incidents)
- Virus (9,633,478 incidents)
- Worm (4,059,958 incidents)

Within the top five malware types, in percentage terms, trojans accounted for 46.8%, viruses 32.3%, worms 13.6%, packed malware 3.9%, and backdoors 3.3%. The chart below displays this graphically.




As detailed below, an analysis of malware types, victims, and other aspects of cyberattacks can be used to profile regions, nations, and verticals in unique and illuminating ways, which can significantly help with both strategic and tactical cyber defense.

One of the best ways to perform large-scale malware analysis is with the aid of a traditional map. On the next page, this graphic depicts the most common malware type that Comodo detected in each country. Almost every country within the United Nations is represented within Comodo data, so this is truly a strategic dataset, with which it is possible not only to construct a malware profile for individual nations but to compare entire regions against one another. It is possible to see that geographic, linguistic, socio-economic, and technological commonalities help to determine threat profiles and the best strategies and tactics for managing enterprise cyber defense.




Even a quick glance shows that the most common malware threat in the world today is trojans. Malware trojans play a similar role to that of the celebrated wooden horse in Greek mythology. Essentially, these are computer programs that have hidden functionality. They offer remote attackers the same rights and privileges as a local user, and can be used for any type of cyberattack, including the installation and execution of ransomware.

However, a closer look shows that there are interesting regional anomalies that must be investigated. Look at South America, Africa, Southeast Europe, and Southeast Asia. Here, we can see that numerous countries on the lower end of the socio-economic spectrum are more susceptible to viruses and worms than they are to trojans. Upon reflection, this is probably due to the fact that these nations have higher numbers of older or unlicensed software, as well as enterprises without full-time computer security support staff. Countries which have recently experienced war, such as Somalia, Yemen, and Georgia, share the characteristic of having computer worms as the highest malware threat. Only with the benefit of a strategic malware set can we gain this eye-opening insight.

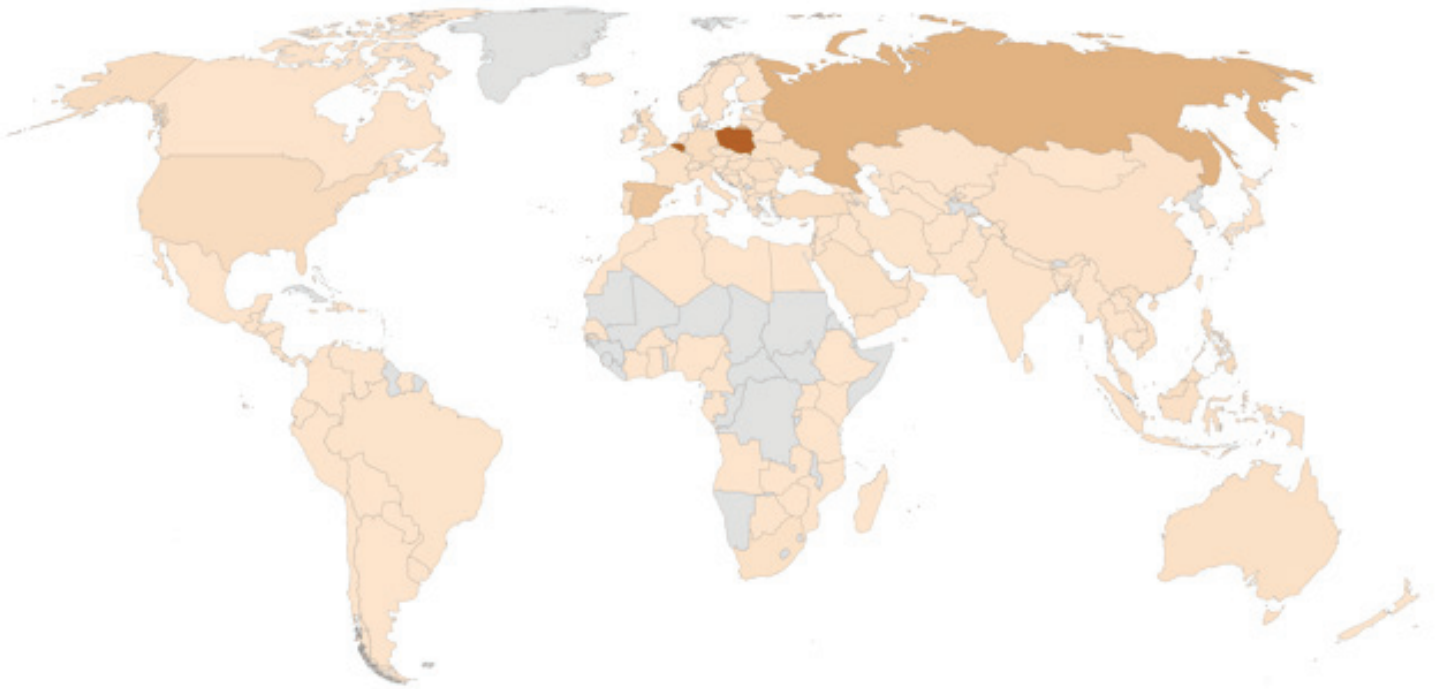
Other anomalies in the data were the unusually high number of packed malware in the United Kingdom and Japan, and the high number of backdoors discovered in Spain and Belgium. The only countries where packed malware or backdoors were the top malware type were rich nations in the northern hemisphere. The UK and Japan are shaded read while Spain and Belgium are shaded orange. It is likely that these malware types were more expensive to develop, and yield a higher return on investment.

One of the key takeaways from this map is that cyber defenders must conduct strategic as well as tactical Malware analysis. They need to understand the broader threat profile under which they are operating, in order to construct a logical and efficient cyber defense.

## 1 | Backdoor

A backdoor is a hidden way to bypass normal user authentication, often leveraged to gain covert, remote access to a computer system, cryptosystem, or algorithm. A backdoor can be an installed program (such as Back Orifice), or can be a modification to an existing, legitimate program. Backdoors are often built into software for administrative purposes, but hackers can install secret backdoors with the aid of malicious software such as a rootkit.

In Q1 2017, Comodo discovered 993,282 backdoors in 153 countries. Incredibly, over 50% of them were detected in two countries alone: Belgium and Poland. Also among the top ten most affected countries were Spain, Singapore, the U.S., Germany, and the United Kingdom. This pattern suggests that backdoors are a high-value hacker tool that is deployed against lucrative targets. Belgium and Poland are both leading members of both the European Union (EU) and the North Atlantic Treaty Organization (NATO), which may be another clue in efforts to attain attacker attribution.



The following table displays the top ten affected countries by the overall number of backdoor detections within each country and percentage of backdoor detections throughout the world for Q1 2017.

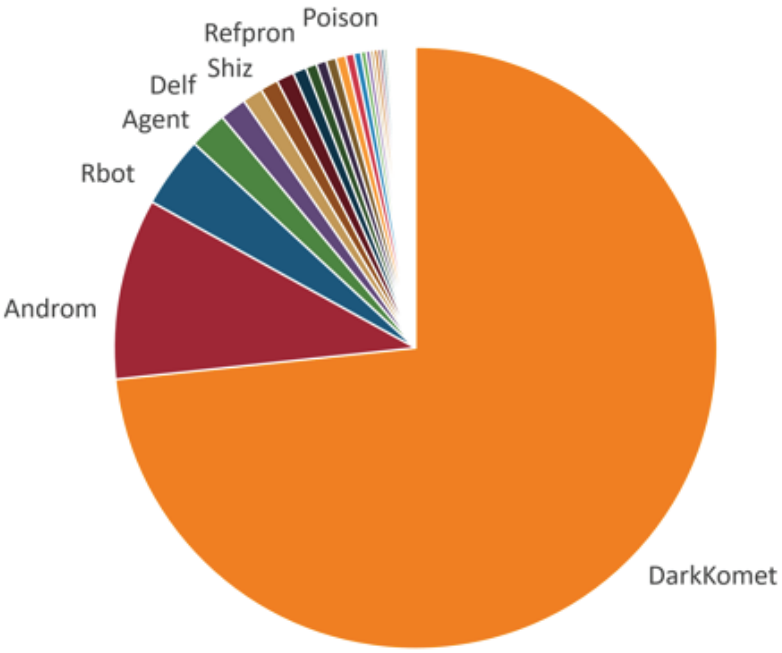
| | | | |
|---|---|---|---|
| 1 | Belgium | 227,188 | 28.64% |
| 2 | Poland | 224,766 | 28.33% |
| 3 | Russia | 84,333 | 10.63% |
| 4 | Spain | 53,380 | 6.73% |
| 5 | Singapore | 18,680 | 2.35% |
| 6 | USA | 15,014 | 1.89% |
| 7 | Turkey | 12,646 | 1.59% |
| 8 | Germany | 12,311 | 1.55% |
| 9 | United Kingdom | 12,143 | 1.53% |
| 10 | Philippines | 11,656 | 1.47% |

The graphic below shows the same malware data, broken down by ratio and country code. This type of graphic is helpful for other nations to see where they fall within the global malware ecosystem. The small blue square at the bottom right, showing three dots, depicts the rest of the 153 countries where Comodo discovered backdoors in Q1 2017.


Another interesting way to study datasets is to see which subgroups (in this case countries) have the highest ratio of backdoors within their overall detections. For countries with a minimum of 100 detected backdoors, Belgium, Spain, Poland, Bahrain, Lebanon, Cyprus, Jordan, Jamaica, Saudi Arabia, and Latvia had the highest percentage of backdoors compared to overall malware detections.

The fact that Belgium, especially as a small country, stands out so prominently in this data may be contrasted with worm detection in lower socio-economic tier countries. As headquarters to both the EU and NATO, these data suggest that attackers likely deploy higher-grade malware against more lucrative or better-defended targets, with a goal of achieving a higher return on investment.

In Q1 2017, Comodo detected 495 unique families of backdoors around the world. These are depicted in the pie chart below, where we see that one family in particular dominates the backdoor landscape. However, remember that in the white band there are actually hundreds of backdoor families, some of which may be highly professional programs that are causing great harm within certain networks. Thus, cyber defenders are forced to do an incredible amount of research simply to understand the full scope of even one malware type.

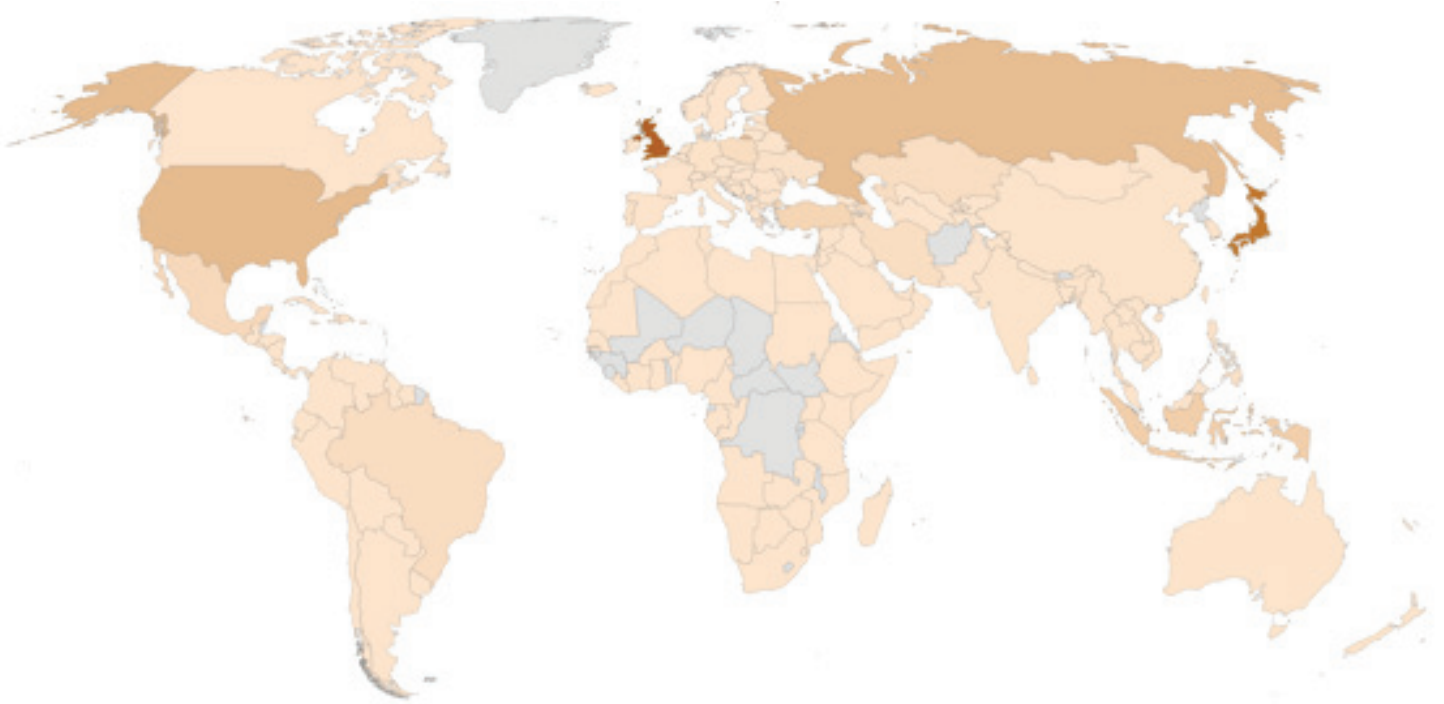



The most common backdoor was DarkKomet, or DarkComet, which was detected in 100 countries. DarkKomet is a Remote Administration Tool (RAT) that was created in 2008 and has been common since 2012. It allows remote attackers the ability to control a victim's computer via Graphical User Interface (GUI) and can be used for good or evil. It includes the capability to take screenshots, log keystrokes, crack passwords, and more.

## 2 | Packer

Have you ever heard of a malware packer? At Comodo, our technical analysts use this term to refer to any means that is used to hide or obfuscate malicious software by compressing or "packing" executable code, even in the form of scripts, and combining the compressed data with decompression code into another executable, or even a self-extracting archive. When the latter is executed, the decompression code recreates the original code from the compressed code and executes the malware. This method, which may also incorporate encryption, is a way to conceal malware from security software and to obfuscate an attack.

In Q1 2017, Comodo discovered 1,148,231 incidents of packed malware in 173 countries. And this dataset is surprising because the UK, Japan and the U.S. were home to over 60% of Comodo detections, with Russia in fourth place. What does this mean? Similar to backdoors, it is likely that packed malware is a higher value hacker toolset that is deployed against lucrative targets.



Nonetheless, the world map above shows that packed malware is a global phenomenon that must be taken seriously by network Security administrators wherever they are. As compared with backdoors, in Q1 2017, Comodo discovered more incidents of packed malware, and in more countries.

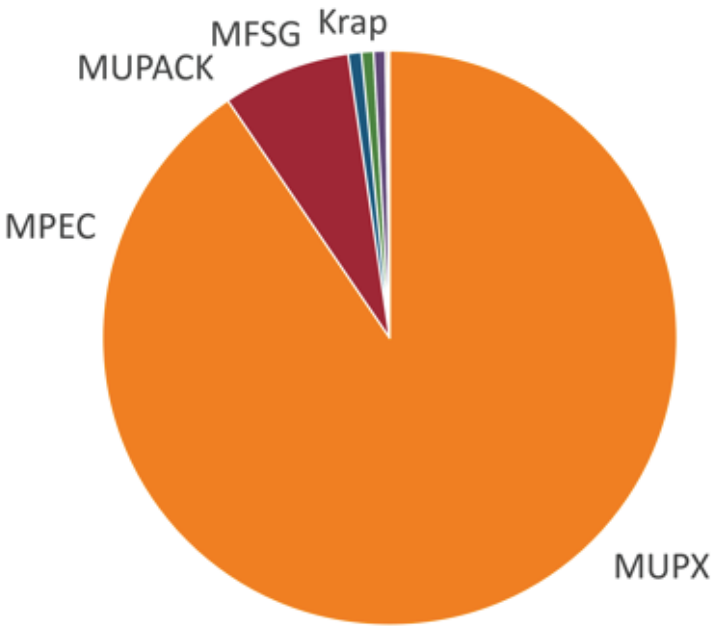
The following table displays the top ten affected countries by the overall number of packed malware detections within each country and percentage of packed malware detections throughout the world for Q1 2017.

| | | | |
|---|---|---|---|
| 1 | United Kingdom | 243,957 | 30.18% |
| 2 | Japan | 197,548 | 24.44% |
| 3 | USA | 75,194 | 9.30% |
| 4 | Russia | 71,796 | 8.88% |
| 5 | Indonesia | 40,802 | 5.05% |
| 6 | Turkey | 27,928 | 3.46% |
| 7 | Mexico | 21,135 | 2.61% |
| 8 | Brazil | 14,128 | 1.75% |
| 9 | Poland | 13,598 | 1.68% |
| 10 | Kazakhstan | 12,373 | 1.53% |

The graphic below shows the same malware data, broken down by ratio and country code. As you can see, the UK (signified by the “gb” code for Great Britain) should take the packed malware threat seriously. Furthermore, other nations may be able to learn from the UK’s infections before it is too late.


If we expand the scope of our analysis to the ratio of packed malware within overall detections, another group of interesting countries emerges. For countries with a minimum of 100 detected packers, Japan, United Kingdom, Paraguay, Mexico, Turkmenistan, Azerbaijan, Ecuador, Slovenia, Israel, and New Zealand had the highest percentage of packers compared to overall malware detections. In particular, Israel stands out, since that nation is well-known for its professional cyber defense; this fact strengthens our argument that packed malware can be used in malware campaigns against high-value targets.

Comodo detected 16 unique families of malware packers in Q1 2017. This fact is significant, in that the smaller number of overall families may allow network defenders to focus their training and resources on a less complex threat profile.

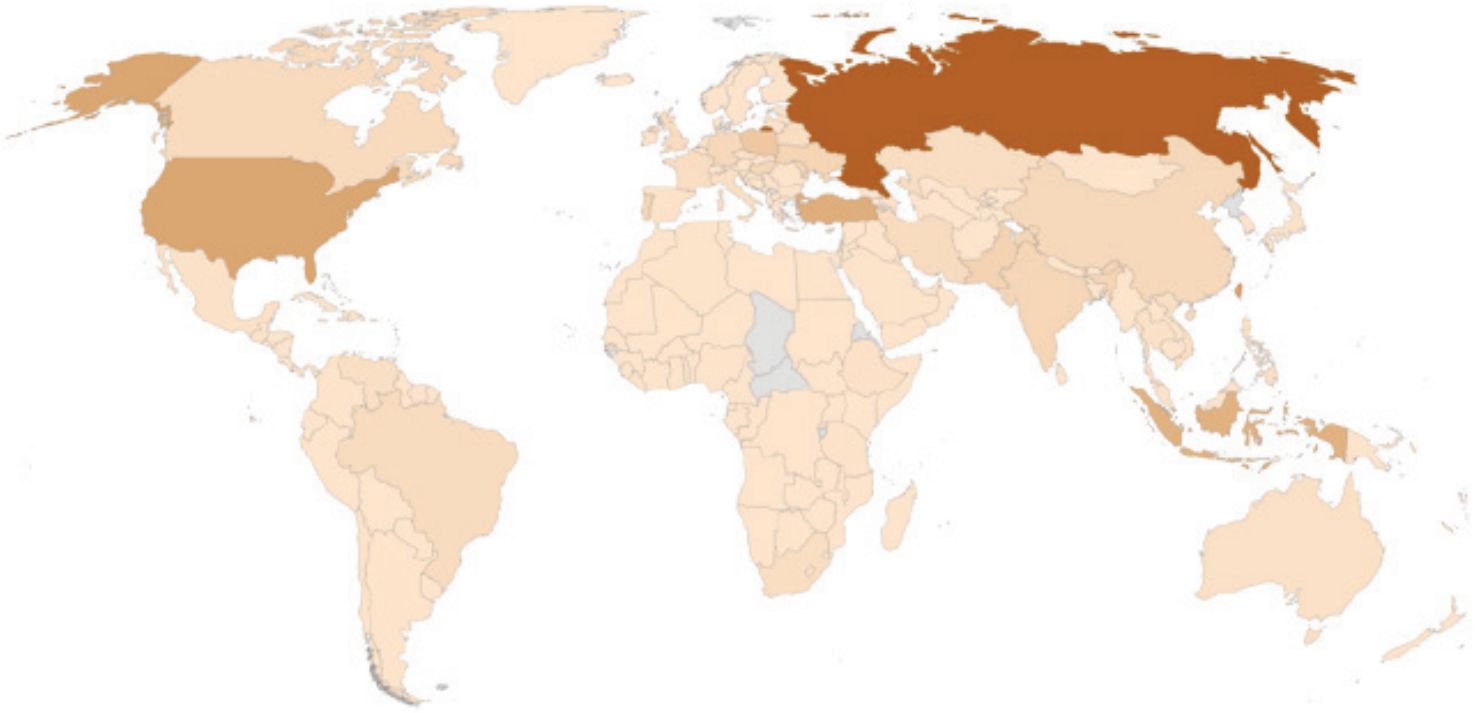



The most common type of packer, by far, was MUPX, which Comodo found within 167 country code domains. MUPX stands for “modified UPX,” which references free, open source software called UPX, or the “Ultimate Packer for Executables,” which is compatible with numerous file formats and different operating systems. UPX leverages an open source data compression algorithm, UCL, that is just a few hundred bytes of code in length. UCL is so efficient that it also does not require much or any additional memory allocation for decompression. Unmodified UPX packing is often detected by security software, which means that the software has likely been modified in some way by the attacker.

### 3 | Trojan

Borrowing its name from the famous wooden horse in Greek mythology, which was used to facilitate the invasion of Troy, a "trojan" computer code is any functionality, usually malicious, hidden within a seemingly useful or benign computer program. It is designed to exploit or damage the system on which it is run. As with a virus, attackers often use social engineering to trick users into downloading and installing these programs. Trojan horses are commonly delivered by email with messages that misrepresent the program's true purpose.

In Q1 2017, Comodo discovered 13,947,885 trojans within 223 country domains. Thus, in both depth and breadth, trojans are the most prevalent and complex malware type on planet Earth today. Basically, Comodo detected trojans in nearly every country where our security software is deployed. Due to predominance of trojans within the overall malware landscape, the top ten list here looks very similar to the top ten list of overall detections cited above.



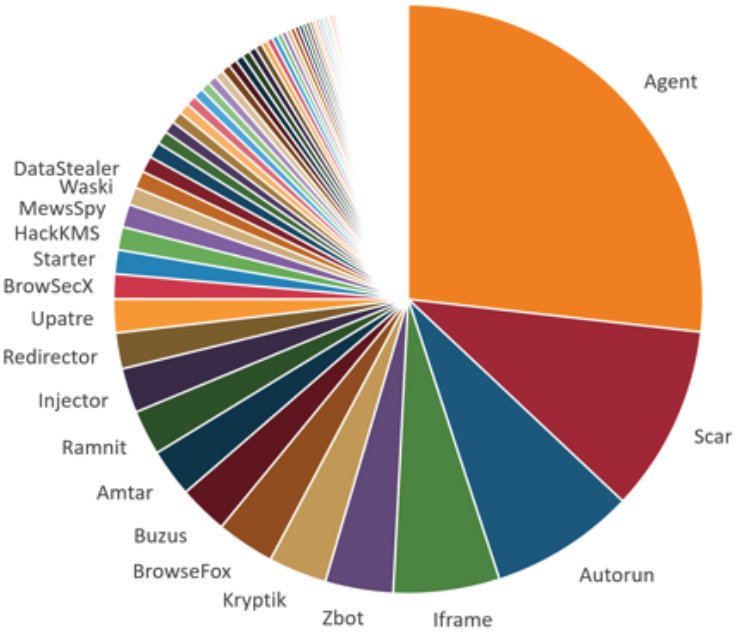
The following table displays the top ten affected countries by the overall number of trojan detections within each country and percentage of trojan detections throughout the world for Q1 2017. Again, we see that Russia has not only been home to many cybercriminals in the past, but has also suffered mightily from the negative impact of malware.

| | | | |
|---|---|---|---|
| 1 | Russia | 2,322,608 | 18.51% |
| 2 | Taiwan | 1,205,654 | 9.61% |
| 3 | USA | 1,068,493 | 8.52% |
| 4 | Turkey | 929,216 | 7.41% |
| 5 | Indonesia | 870,194 | 6.93% |
| 6 | Hong Kong | 708,086 | 5.64% |
| 7 | Poland | 503,712 | 4.01% |
| 8 | Singapore | 452,962 | 3.61% |
| 9 | Pakistan | 310,333 | 2.47% |
| 10 | Ukraine | 268,021 | 2.14% |

Placing the same data into a treemap, we see many other countries, from Portugal to India, Iran, Belarus, and Italy. The graphic below shows the same malware data, broken down by ratio and country code.


If we look solely by ratio, some very exotic countries enter the picture. For countries with a minimum of 100 detected trojans, Bermuda, Curacao, Belize, Tanzania, Europe, Guadeloupe, Zimbabwe, Northern Mariana Islands, Singapore, and Ireland had the highest percentage of trojans compared to overall malware detections. In part, from a strategic perspective, this list tells us that hackers may want to have a very diverse and geographically separated malware infrastructure within which they can operate and maintain some level of anonymity or at least plausible deniability from which to conduct attacks anywhere on the globe.

In short, trojans are a large and complex data set. In Q1 2017, Comodo detected 1,209 unique families of trojans, making this malware type our most diverse and difficult to analyze. From a cyber defense perspective, complexity is the enemy of security, which leaves cybersecurity personnel in the position of trying to defend against whole classes of malicious functionality, usually employed by unknown attackers for unknown purposes. Even the "Agent" malware family seen in the pie chart below refers to a multifaceted group of computer programs that in and of itself represents a challenging analytical problem for cyber defense researchers.



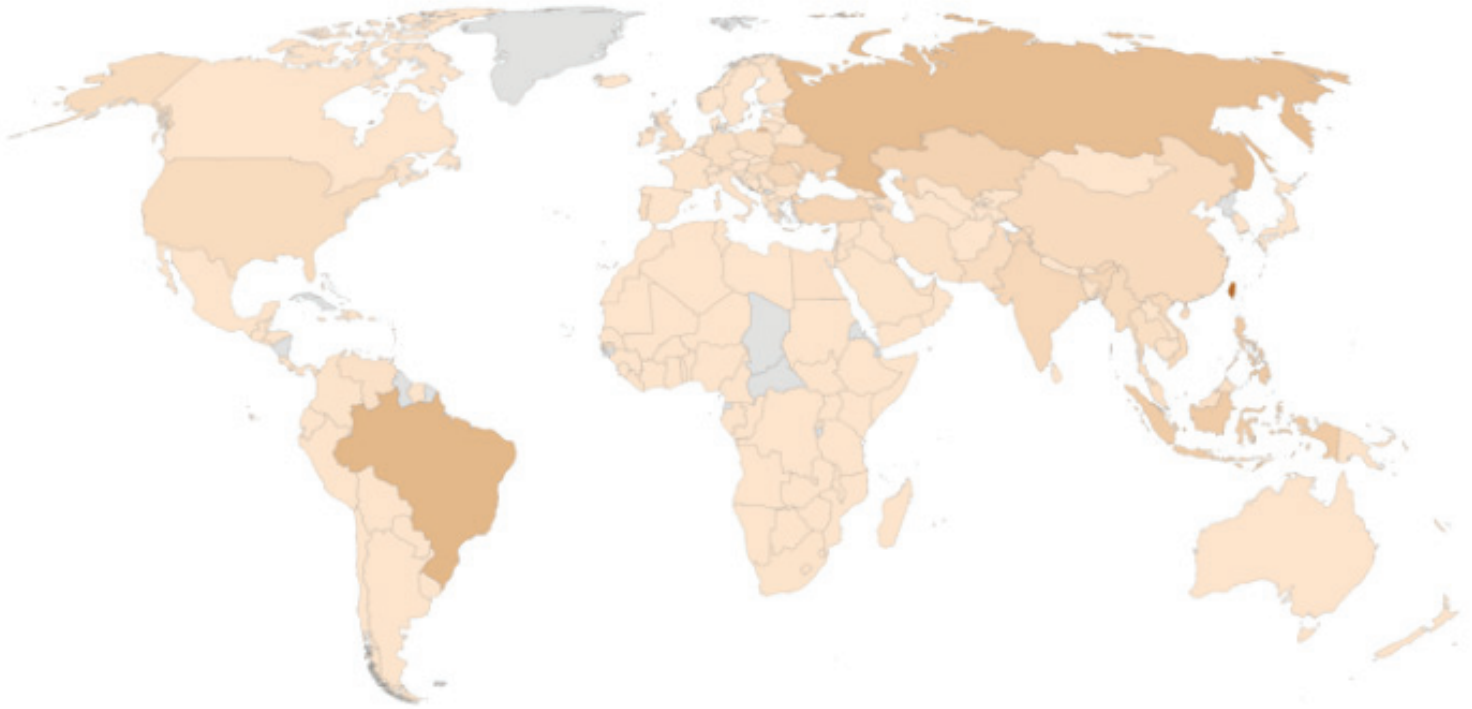

Agent, a generic trojan type that refers to a wide range of trojan-like malware, highlights the fact that trojans are a vexing problem for cyber defenders given their high number and similarity of functionality. Scar, in the number two spot, is a cybercrime trojan created for financial theft, which redirects web browsers from legitimate websites to another IP address under an attacker's control where an imitation logon screen can capture victim credentials.

For cyber defenders, some of the best advice we can give is to be aware of the basic functionality of software trojans, so that you can identify new, unknown variants as they are created and propagate across the internet.

### 4 | Virus

A computer virus is self-replicating code that “infects” another computer program, and can corrupt it in malicious ways to facilitate data theft, spam dissemination, data destruction, and more. Like human viruses, a computer virus attempts to spread from computer to computer by attaching itself to a host program. A virus usually cannot be transferred to another computer unless a user moves the infected file or performs some action, such as opening an attachment or clicking on a hyperlink. When the host file is executed, the virus code also runs, infecting the new host. A virus can damage hardware, software, or data.

In Q1 2017, Comodo detected 9,633,478 viruses in 183 country domains. This is the second largest malware type the Comodo discovered and analyzed. But the victim list looks quite a bit different. Taiwan, Hong Kong, and Brazil accounted for nearly 50% of detections. Another thing we notice within the top ten affected countries, looking past Taiwan and Hong Kong, is that viruses are prevalent in a lower socio-economic tier of nations. Unlike backdoors and packed malware, viruses appear to primarily affect countries that may run older and perhaps unpatched versions of software.



The following table displays the top ten affected countries by the overall number of virus detections within each country and percentage of virus detections throughout the world for Q1 2017.

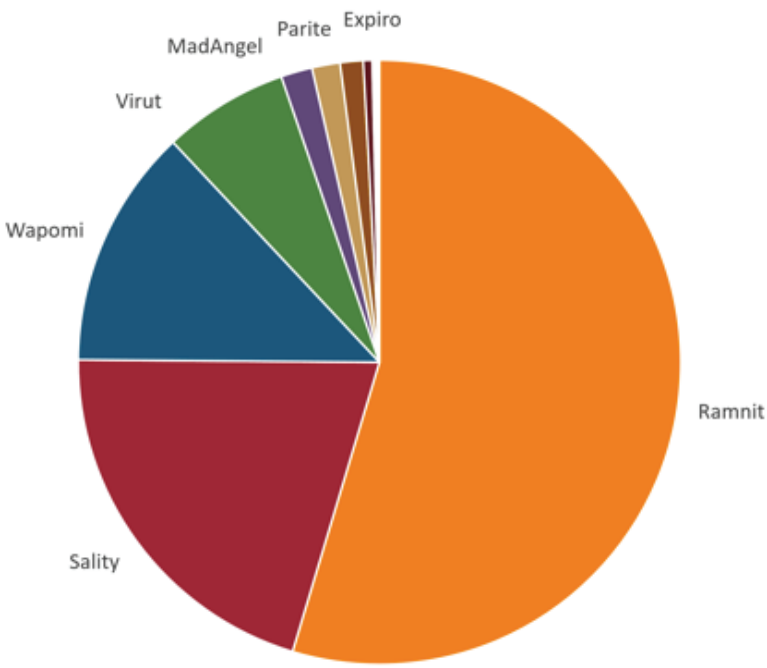
| | | | |
|---|---|---|---|
| 1 | Taiwan | 2,054,962 | 23.80% |
| 2 | Hong Kong | 1,263,589 | 14.64% |
| 3 | Brazil | 690,940 | 8.00% |
| 4 | Russia | 599,008 | 6.94% |
| 5 | Philippines | 409,000 | 4.74% |
| 6 | Indonesia | 386,442 | 4.48% |
| 7 | Ukraine | 291,782 | 3.38% |
| 8 | Kazakhstan | 273,161 | 3.16% |
| 9 | Turkey | 225,973 | 2.62% |
| 10 | India | 212,018 | 2.46% |

The graphic below shows the same malware data, broken down by ratio and country code. We can see that Taiwan really stands out in this dataset. Further down the list we see Romania, Vietnam, Pakistan, China, and Iran.


Looking at all countries by ratio further strengthens this argument. For countries with a minimum of 100 detected viruses, Myanmar, El Salvador, Malta, Madagascar, Brazil, Romania, Bangladesh, Peru, Taiwan, and Ghana had the highest percentage of viruses compared to overall malware detections. By and large, these are relatively poor nations, which may struggle to keep up with best practices in computer security, including the latest patches from commercial vendors.

Fortunately for cyber defenders, Comodo detected only 112 unique families of viruses. Compared with trojans, this relatively small number may allow network security personnel to focus on a less complex dataset, which may simplify the task before them.

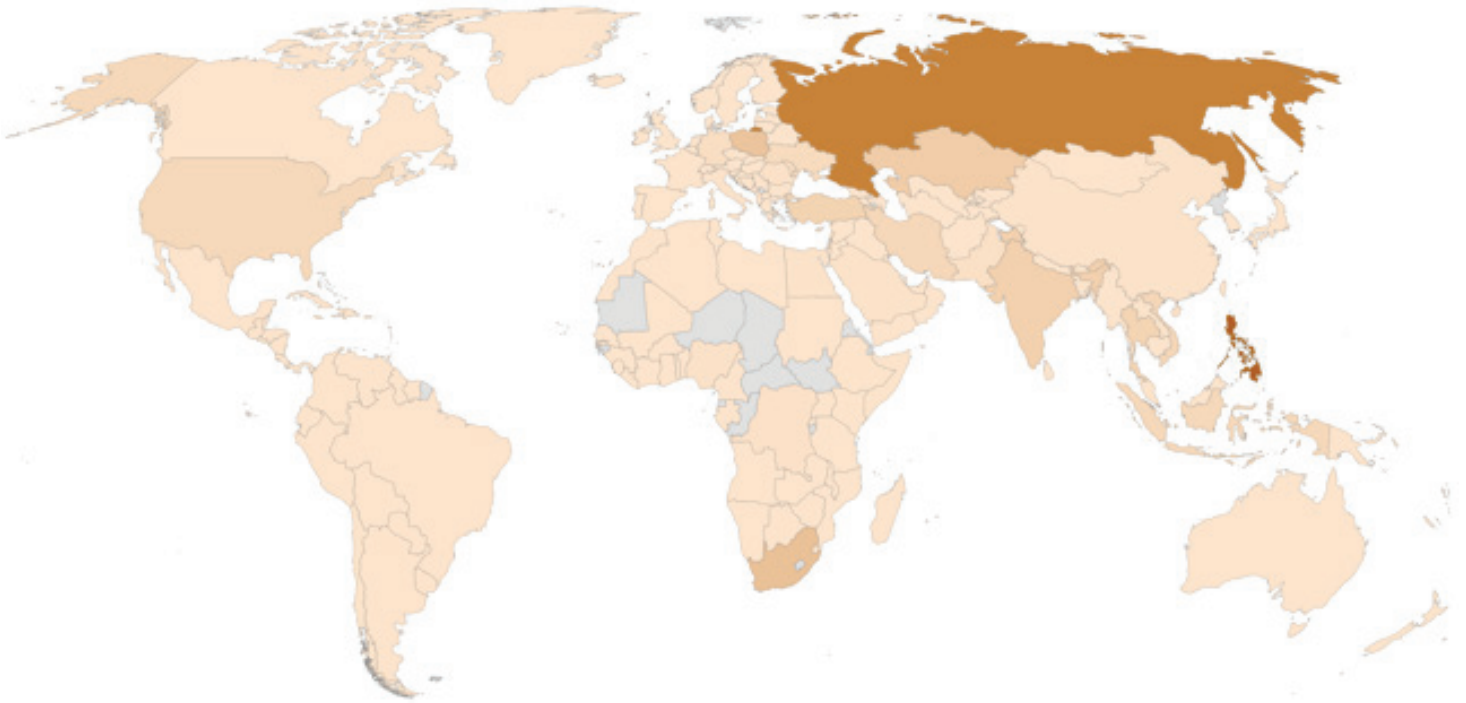
The most common type of virus was Ramnit, which Comodo detected within 130 country code domains. Ramnit can spread via removable devices such as a USB flash drive, infected files on public download servers, malicious advertisements, dodgy applications, or links distributed through social media. It is designed to steal sensitive information, such as passwords or bank credentials.



### 5 | Worm

A computer worm is like a virus, but typically travels the internet autonomously, exploiting vulnerabilities in network defenses as it spreads across the internet. Thus, a worm is normally self-propagating, automatically distributing itself from one computer to another through network connections. A worm is usually designed to deliver a malicious payload to the victimized computer. However, even worms without a payload can consume enormous bandwidth, diminish network or local system resources, and possibly cause a denial-of-service.

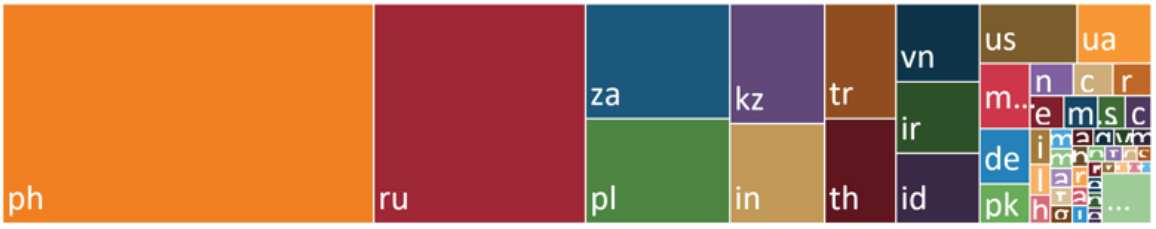
In Q1 2017, Comodo detected 4,059,958 computer worms within 187 country code domains. The Philippines stands out as home to over one-quarter of the worms detected. System administrators in that country should take note. But if we look further into the top ten list, we can see that a pattern emerges, similar to that of computer viruses. These are not rich, Western countries, but places where you are likely to see older, more vulnerable versions of software on the enterprise networks that may lack a full-time, dedicated cybersecurity staff.



The following table displays the top ten affected countries by the overall number of worm detections within each country and percentage of worm detections throughout the world for Q1 2017. Here, Thailand, Vietnam, and Iran show up on our top ten list for the first time.

| | | | |
|---|---|---|---|
| 1 | Philippines | 1,011,797 | 26.91% |
| 2 | Russia | 749,380 | 19.93% |
| 3 | South Africa | 266,944 | 7.10% |
| 4 | Poland | 242,547 | 6.45% |
| 5 | Kazakhstan | 183,016 | 4.87% |
| 6 | India | 152,029 | 4.04% |
| 7 | Turkey | 131,792 | 3.51% |
| 8 | Thailand | 120,683 | 3.21% |
| 9 | Vietnam | 104,687 | 2.78% |
| 10 | Iran | 96,034 | 2.55% |

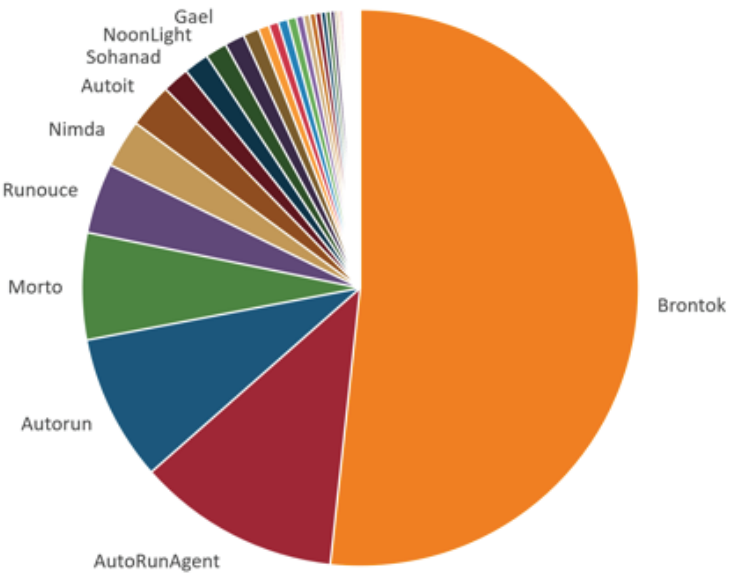
The graphic below shows the same malware data, broken down by ratio and country code. Outside the top ten list above, for example, we also see Indonesia, Ukraine, in Pakistan.




For countries with a minimum of 100 detected worms, Congo, Maldives, Somalia, Cape Verde, Macedonia, Philippines, Nigeria, Yemen, South Africa, and Gambia had the highest percentage of worms compared to overall malware detections. This list serves to strengthen our argument that worms affect poorer nations, as the majority of them lie within Africa.

In Q1 2017, Comodo detected 230 unique families of computer worms, which may be a relatively manageable number for network security personnel. Nonetheless, that assertion presupposes that an enterprise has a dedicated cybersecurity staff.

In Q1 2017, the most common worm detected by Comodo is Brontok, detected within 109 country code domains. Brontok is a Microsoft Windows-based worm that spreads via email. It has its own email engine and sends itself to email addresses found on a victimized computer, spoofing the victim's email address as the purported sender.

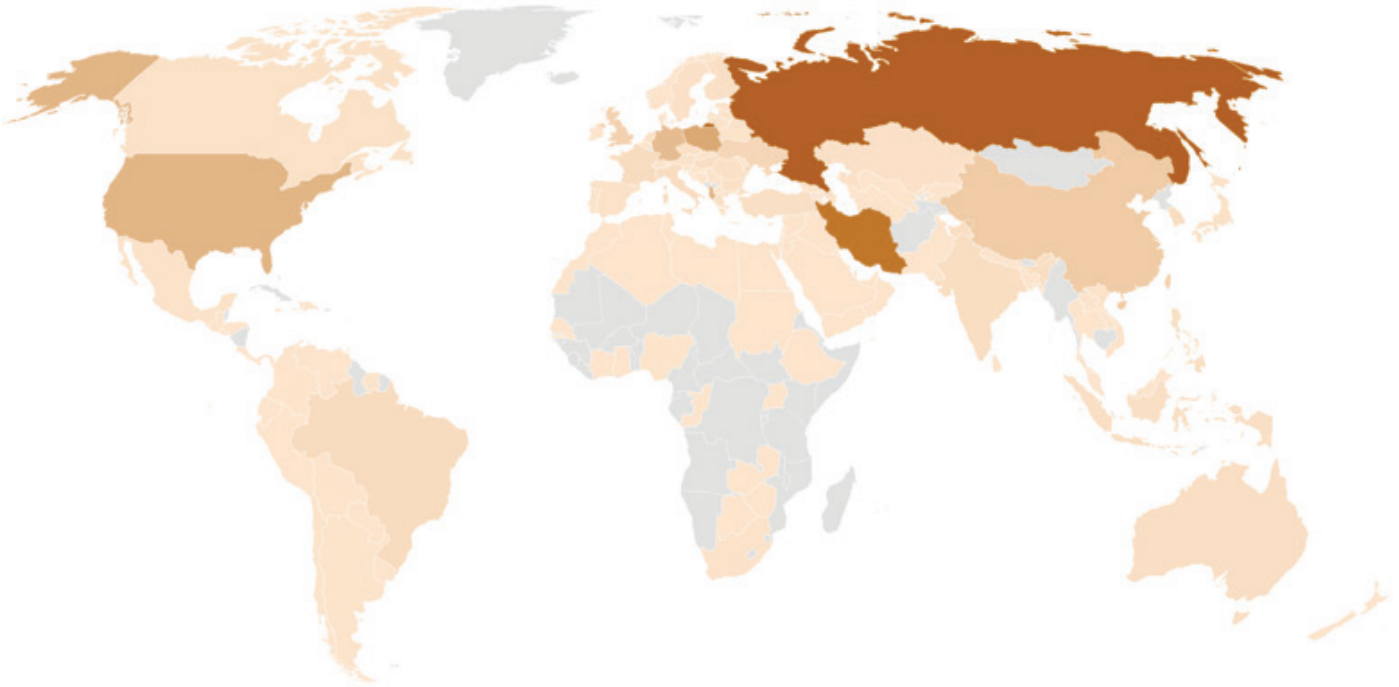



Brontok has been used for hacktivist purposes in the past, including attacks on the Israeli government and Playboy magazine. In such cases, the nature of the target can help with attribution, as the victim may have some idea of who would attack them for political, military, criminal or intelligence purposes.

## Ransomware

In 2017, ransomware has been one of the hottest topics in cybersecurity. This type of malware is a “cryptovirus” that can cause a denial of access to one’s data by encrypting it and holding it hostage for extortion. Older versions of ransomware were typically scareware, displaying fake warning messages and/or blocking applications, but increasingly they use professional, public key encryption, which can be impossible to decipher without paying a ransom payment. Until the payment is made, the private key is withheld from the victim, and that is required to recover the data. There are many ways that ransomware code propagates through the internet, but most commonly cybercriminals use malicious email attachments, botnets, or malicious drive-by attacks on tainted websites. In most cases, social engineering plays a role. Cryptocurrencies like Bitcoin allow anonymous, online payment.

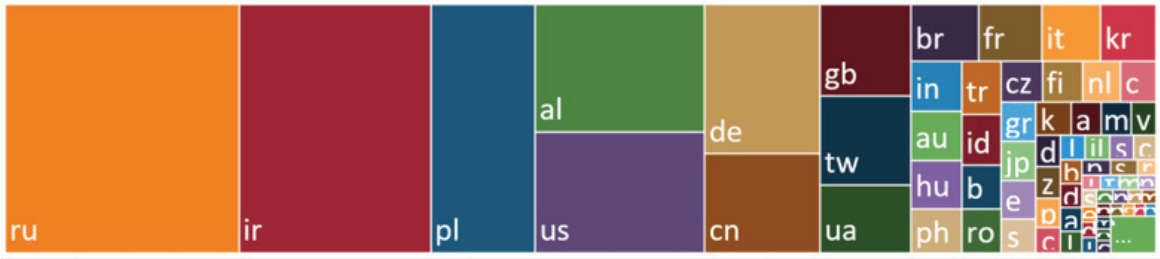
In Q1 2017, Comodo detected 99,828 cases of ransomware in 127 countries, in nearly every corner of the globe. Russia and Iran were the most frequent targets, but Poland and the U.S. were rising in the data as Q1 2017 progressed. There was an interesting mix of affected nations: some are probably more vulnerable, such as Russia and Iran, while others offer a potentially higher return on investment, such as Germany and the U.S. Cybercriminals experiment and practice in order to hone their skills and software and to find a “sweet spot” in which targets are found who are able and willing to provide an extortion payment.



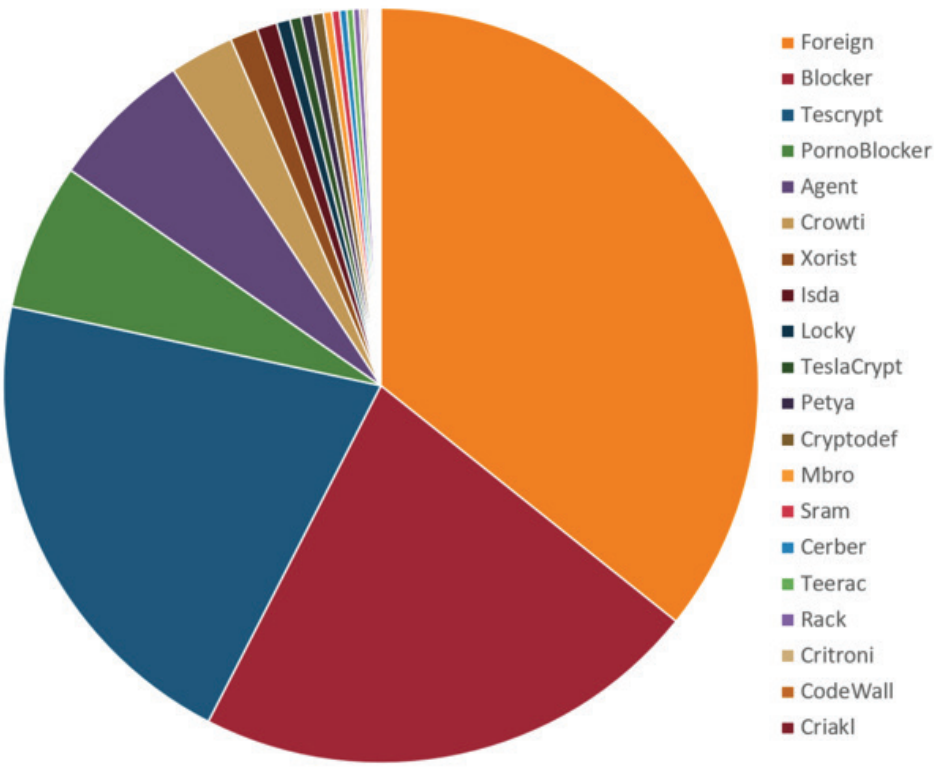
The following table displays the top ten affected countries by the number of ransomware detections within each country and its percentage of ransomware detections throughout the world for Q1 2017. Interestingly, African nations do not appear on this list, which may indicate that cybercriminals simply do not see poorer nations as a good investment for their ransomware (although Albania stands out as an anomaly).

| | | | |
|---|---|---|---|
| 1 | Russia | 15,603 | 15.63% |
| 2 | Iran | 12,810 | 12.83% |
| 3 | Poland | 6,989 | 7.00% |
| 4 | Albania | 5,807 | 5.82% |
| 5 | USA | 5,510 | 5.52% |
| 6 | Germany | 4,644 | 4.65% |
| 7 | China | 3,068 | 3.07% |
| 8 | United Kingdom | 2,242 | 2.25% |
| 9 | Taiwan | 2,177 | 2.18% |
| 10 | Ukraine | 1,650 | 1.65% |

The graphic below shows the ransomware data, broken down by ratio and country code. A bit deeper into the data, we see a real mix of targets, including some rich nations such as Australia, and some poorer nations like Indonesia.



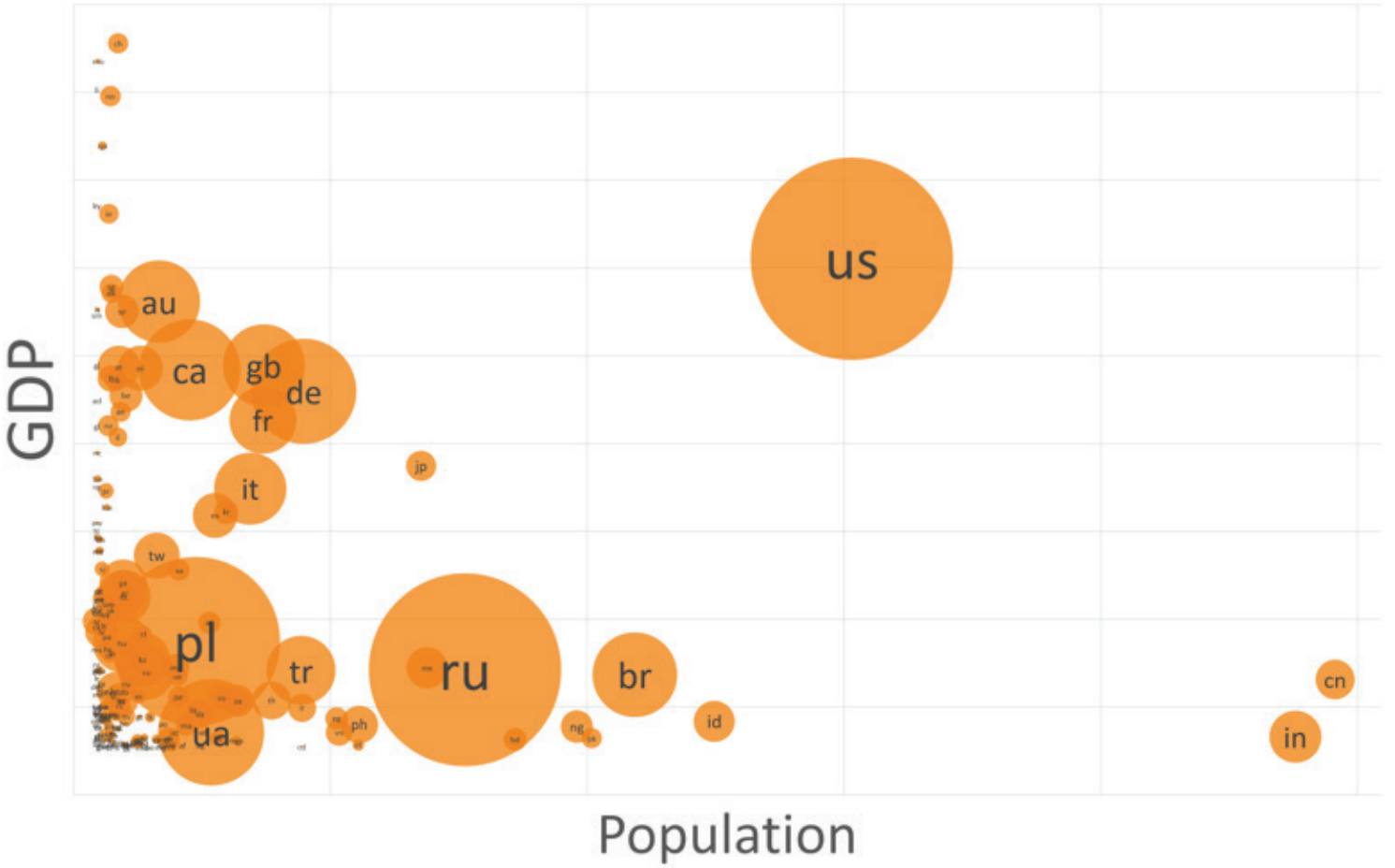

In Q1 2017, Comodo detected 44 unique families of ransomware, but in fact of some these are simply generic categories of ransomware that refer to a variety of malware that encrypt your files, demand payment (for example, via Bitcoin), and provide a way to collect the extortion payment.



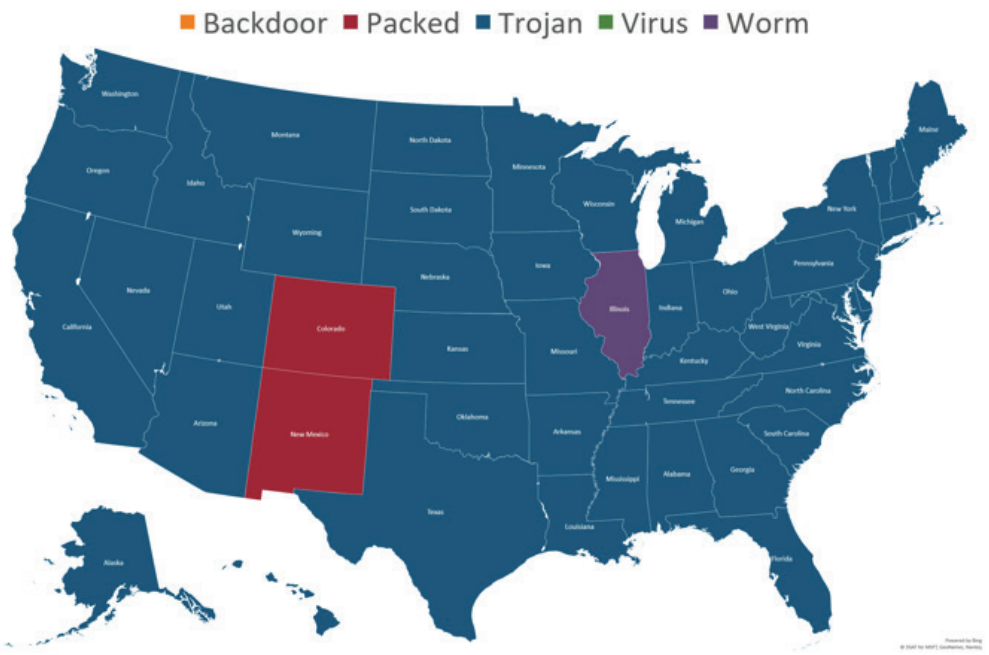

In the face of this significant new cyber threat, Comodo recommends that enterprises immediately designate personnel to study the issue, develop contingency plans, create a list of emergency points of contact, and conduct awareness campaigns. However, the single most important thing to do is to ensure an enterprise has offline data backup, not connected to networked resources. Network security personnel should also severely limit the use of macros, embedded code, pop-ups, unknown attachments, .exe files, etc. On the social engineering side, teach your employees to never trust unsolicited communications. It is possible to detect ransomware functionality during the early stages of an attack and to prevent your data from being encrypted, but this requires quick action on the part of the victim. Law enforcement strongly discourages the ransom payment, as there is no guarantee you'll get your data back and hackers may have already left a backdoor for future harassment and targeting.

## United States Analysis

Why do criminals rob banks? Because that is where the money is. The chart below shows why the United States is a popular target for cybercriminals and spies. On balance, it has the most people with the most money, the largest overall economy, and the world's foremost military capability. The United States also happens to be the most connected country in the world — sitting right at the center of cyberspace.



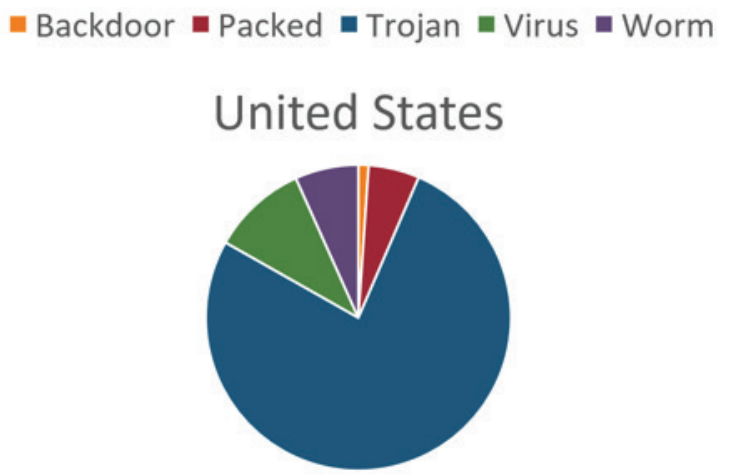
In terms of malware profile, there is less variation within individual countries than between different countries. Thus, a malware map of the United States — or any other country — should look more uniform than a zoomed-out world map. Thus, in 47 of the 50 United States, trojan is the dominant malware category, and the overall map appears blue. Further, apart from three states where packed malware and computer worms were the top malware threat, there were no states where virus or backdoor was the top threat in Q1 2017.




However, there is one interesting divergence to note: Colorado and New Mexico were both red. This commonality is even more interesting given that the states are neighbors, suggesting that geographic proximity is one determining factor of a nation or state malware profile. Illinois was the only other outlier, with computer worm as the top malware category.

Throughout the United States, Comodo in Q1 2017 detected 378,380 trojans, belonging to 711 unique families, making this data subset one of our most complex. The most common trojan in the U.S. was the banking malware Kryptik, which accounted for 24% of all trojan detections.

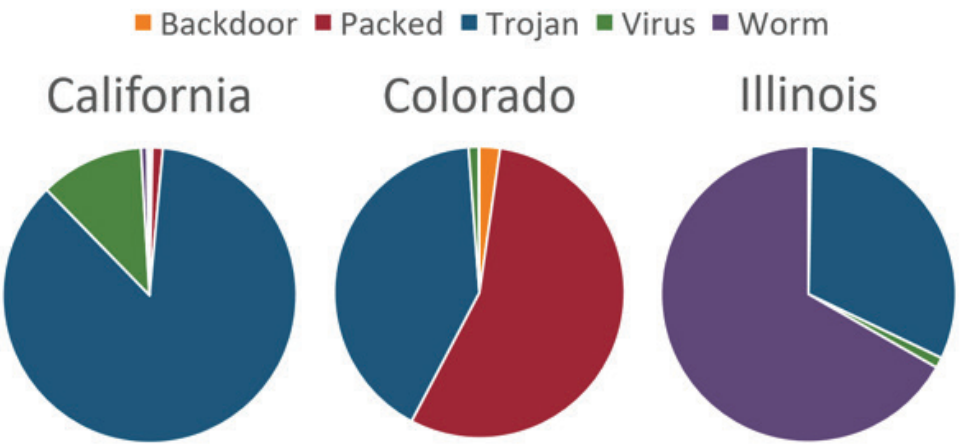
Taken all together, the top five malware categories for all 50 states had the following breakdown, depicted in the pie chart below. When compared to the world as a whole, the U.S. had relatively more trojans and packed malware, somewhat fewer backdoors, and far fewer viruses and worms.




The following table displays these same data by number and percentage. Clearly, system administrators must take the threat from trojans seriously. However, with malware, quality is often more important than quantity. Packed malware and backdoors may be fewer in number, but ultimately far more damaging to an enterprise. With packed malware, someone has taken the trouble not only to write malicious code, but also to cleverly hide within another communications stream. And backdoors effectively give unknown hackers a secret port of entry into your enterprise, but may be used at any time, and for any purpose.

| | | | |
|---|---|---|---|
| 1 | Trojan | 1,068,493 | 76.72% |
| 2 | Virus | 140,506 | 10.09% |
| 3 | Worm | 93,569 | 6.72% |
| 4 | Packed | 75,194 | 5.40% |
| 5 | Backdoor | 15,014 | 1.08% |

Each state, of course, has its own malware profile. For this comparison, we will only have a look at three states whose profile is quite different. Many U.S. states had similar malware profiles, but California, Colorado, and Illinois did not.




California had a malware profile rather like the U.S. as a whole, with trojans accounting for the majority of attacks. Comodo classified most of these within the generic "obfuscated" malware family, which encompasses hidden exploits in HTML, JavaScript, PDF documents and more, all of which attempt to evade security software detection by hiding their malware payloads in different ways. California's most common virus was Ramnit, which is common throughout the world, and propagates via removable drives, infected files on public download servers, malicious advertisements, dodgy applications, or links distributed through social media. It is designed to steal sensitive information, such as passwords or bank credentials.

Colorado was an anomaly in the U.S., with a high volume of packed malware in Q1 2017. The top family was MUPX, or the modified "Ultimate Packer for Executables," an open source, highly efficient software detailed in the malware section above, that is compatible with numerous file formats and operating systems. The most common trojan in Colorado was XPack, which Enigma Software reports as malware that uses unique encoding to disguise its components while downloading and installing it, as well as to hide from security programs.

Illinois experienced significant worm activity. The top worm was Autorun, which F-Secure describes as Windows malware that spreads by creating and inserting itself into an autorun.inf file within the root directories of hard drives and various removable media such as USB sticks. Once installed, the worm can spread to other computers via shared network drives. Autorun can be used to propagate malicious payloads such as backdoors and trojans. The top trojan in Illinois, HackKMS, does not appear to have been studied in-depth at this time and needs further analysis.

## World Analysis

Let's turn back to the world map. Here, Comodo, as a generation-old company with over 85 million software installations around the world, has a lot to say. In Q1 2017, Comodo detected malware in almost every nation on Earth. And just as humans have unique traits and characteristics, so do nations. Every nation, state, enterprise, and individual has its own malware profile, which can be compared and contrasted to discover hidden relationships and strategic trends.

In the age of the internet, criminals, soldiers, and spies cross international borders at will, with little fear of prosecution or retaliation. Successful cyber investigations are rare, as hackers exploit the global, maze-like architecture of cyberspace to steal, block, and manipulate data — often in foreign countries, far from the long arm of the law. Further, international conflicts, such as in Ukraine, Syria, and North Korea, frequently lead to politically-motivated cyberattacks, which may be initiated by nation-states or even citizen-hackers.

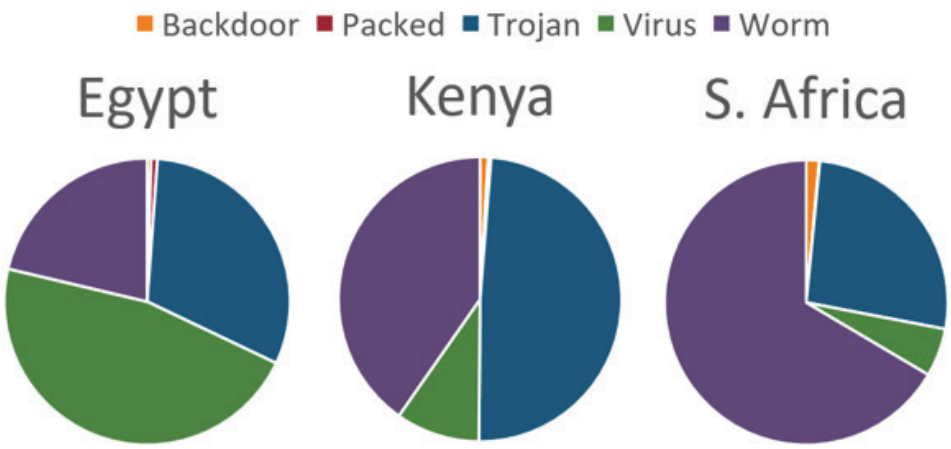
A cyberattack is not an end in itself. Hackers use exploits against vulnerabilities for a wide variety of political, military, intelligence, and criminal goals, which can be studied and fingerprinted in the same way that traditional law enforcement methods are used to solve traditional crimes. Further, every nation and region of the world has unique economics and geopolitics, which naturally shape hacker tactics and targets. In this section, Comodo's strategic malware analysis is used to examine the unique malware profiles of nations — and even whole regions of the world.

## 1 | Africa

Africa is an immense continent, encompassing over 30 million km², 54 countries, and over 1.2 billion people. Nonetheless, it is possible to identify some trends that are particular even to such a large region of the world. For example, Africa suffers from a higher than average volume of viruses and worms, suggesting that these malware types may take advantage of software that is more often older, unlicensed, or unpatched due to financial constraints. War in Congo and Somalia, as well as corruption in Nigeria and South Africa, may help to account for these numbers.


On balance, this map looks quite different than that of North America or Europe, and bears a greater resemblance to Southeast Asia. Worms in particular appear to afflict nations that are struggling politically or economically.

Let's look at three nations with quite different malware profiles: Egypt, Kenya, and South Africa. Visual depictions such as a pie chart can help cyber defenders to quickly see where they should focus their time and attention.



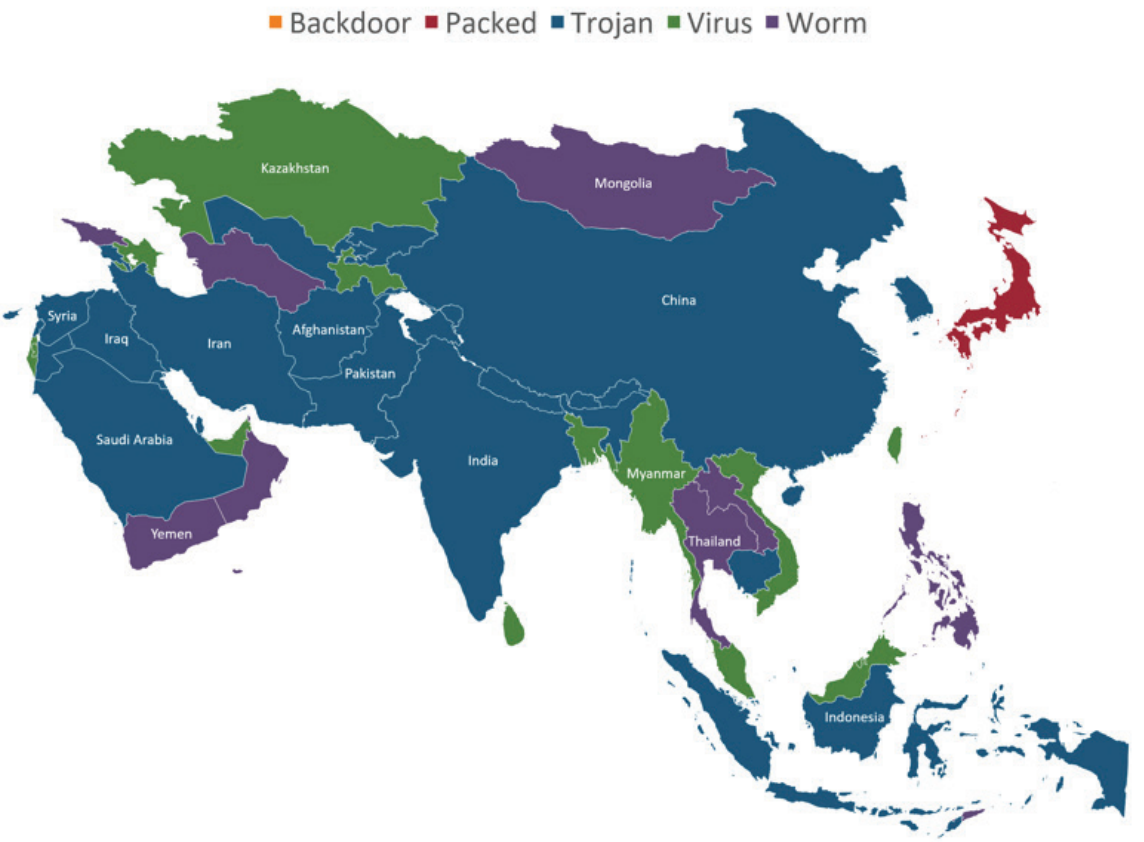

Egypt has a high percentage of virus cases, the majority of which were in the robust Sality family, which has affected Microsoft Windows systems since 2003. Sality communicates over peer-to-peer (P2P) networks for spam dissemination, data exfiltration, web server attacks, distributed password cracking, and more.

Kenya had many trojans, of which Scar was the most prevalent. Microsoft has reported that Scar is a cybercrime trojan created for financial theft, which redirects web browsers from legitimate websites to another IP address under an attacker's control, where an imitation logon screen can capture victim credentials.

South Africa was plagued by an extremely high number of worms. Brontok was the most widely seen, which is profiled above. The second most common worm in South Africa was Runounce, which spreads via email in infected attachments.

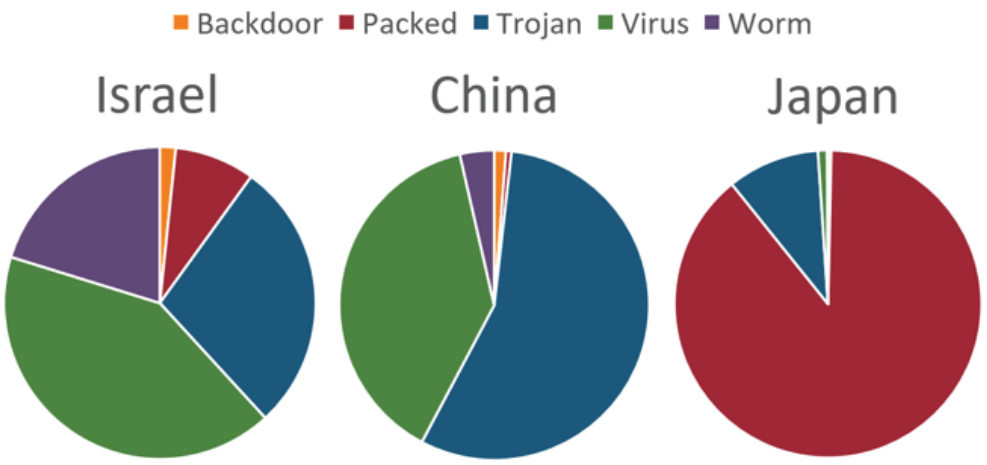
## 2 | Asia

Asia is the Earth's largest and most populous continent. Like Africa, Asia is home to 54 nations, whose length stretches all the way from Europe to the Pacific Ocean. Asia's malware landscape is as vast — and complex — as its terrain. As a whole, Asia exhibits a typical malware profile, with trojans as the top threat, followed by viruses, and then worms. However, given the region's diverse political, economic and military landscape, a closer look highlights some fascinating national and regional patterns.




Some parts of the map, including Central Asia, the far reaches of the Arabian Peninsula, and Southeast Asia look similar to the malware profile in Africa. Computer viruses afflicted many nations, from Kazakhstan to the United Arab Emirates and Vietnam. Surprisingly, virus was also the top malware threat in Israel, given that nation's large high-tech sector and professional cyber defense capability. In Yemen, Mongolia, and Thailand, worms were the most prevalent malware type. Perhaps the most interesting anomaly, similar to the United Kingdom in Europe, was the predominance of packed malware in Japan.

Israel, China, and Japan have very different geopolitics — and malware profiles. It will be interesting to see if these patterns hold in Q2 2017. We will let you know soon as our Q2 report is just around the corner.




Surprisingly, given its high standard of living and celebrated cybersecurity prowess, Israel suffered from a very high ratio of viruses and worms. Ramnit, detailed above, accounted for 88% of these detections. Gael, which affects Microsoft Windows, and often downloads a trojan and/or backdoor of the same name, was the most common worm.

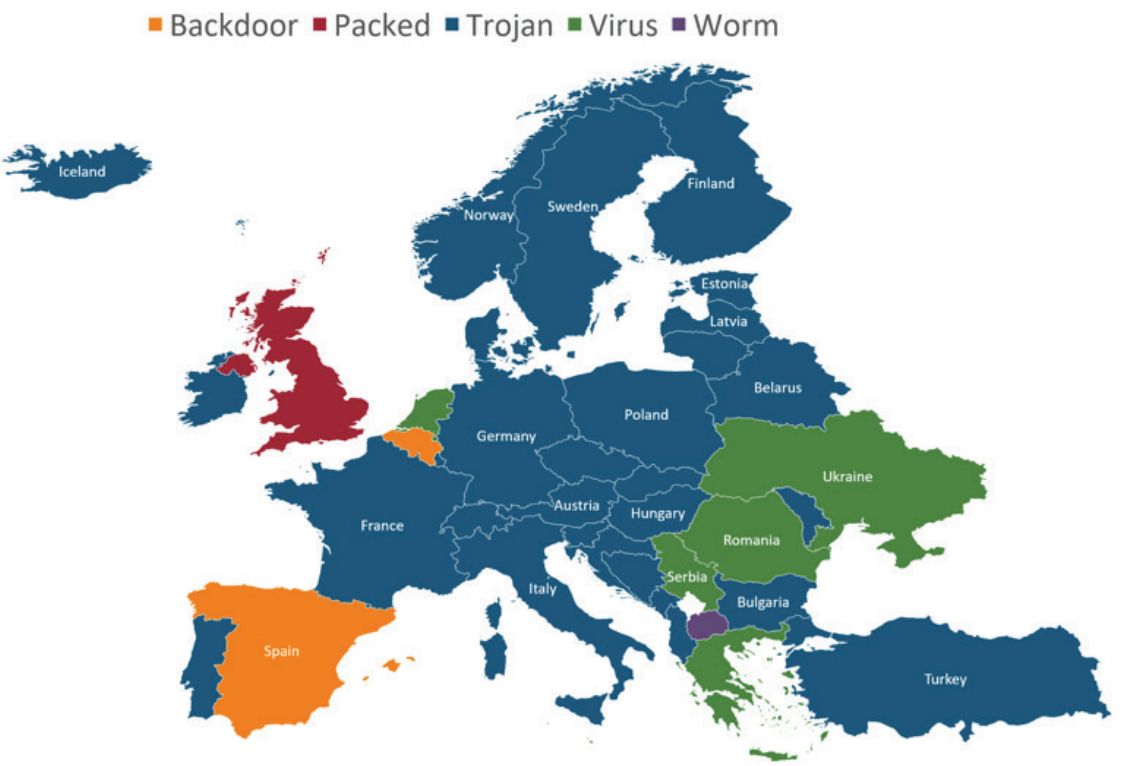
China is closer to Comodo's world average, with a preponderance of trojans, followed by a clear number two malware type in viruses. For trojans in China, the most common was Iframe, which is a malicious JavaScript file embedded into compromised webpages, often via SQL injection. To avoid detection, the trojan may be hosted on a different webpage. Ramnit, described above, was the most common virus.

In Q1 2017, Japanese detections were an anomaly, with a very high ratio of packed malware. MUPX, detailed above, accounted for 99% of these detections.

Australia and New Zealand, which technically fall outside of Asia and within "Oceania," had somewhat average malware profiles, with trojans in first place, followed by viruses. Australia had a relatively higher number of backdoors while New Zealand had a higher volume of packed malware.

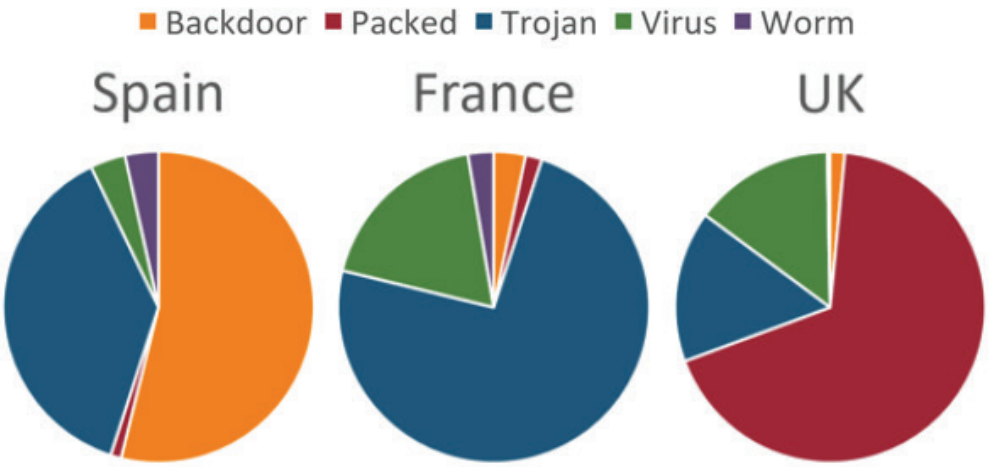
### 3 | Europe

Europe, which enjoys majority membership in the strongest political and military alliances on Earth — the European Union (EU) and North Atlantic Treaty Organization (NATO) — seemingly should present a more cohesive and defensible cyber target. However, in Q1 2017, Comodo detected clear differences between the malware profiles of even the most connected countries of Europe, coloring its map in much more diverse colors than that of the U.S.




Most of Europe, including Scandinavia, the Baltics, and Turkey, had trojans as the top malware type. However, on Europe's East and West flanks, there were two important trends to note. In Southeast Europe, similar to South America and Africa, there were numerous geographically connected countries were plagued by viruses. Macedonia, in the same neighborhood, is the only country in Europe to have worm as the top malware threat. In the West, on the Atlantic coast, Belgium and Spain had an unusually high number of backdoors, while the UK (similar to Japan) struggled with packed malware.

In Q1 2017, Comodo malware detections in Spain, France, and the UK were surprisingly unique, so let's look at them in a bit more detail.




Spain (along with Belgium), suffered an extremely high number of backdoors. Nearly 92% of backdoor detections were DarkKomet, described above. Spain's top trojan was Refroso, which Microsoft has labeled a "severe" threat that stops Windows Security Center and exploits a Windows operating system vulnerability in an attempt to spread to other computers on a local network.

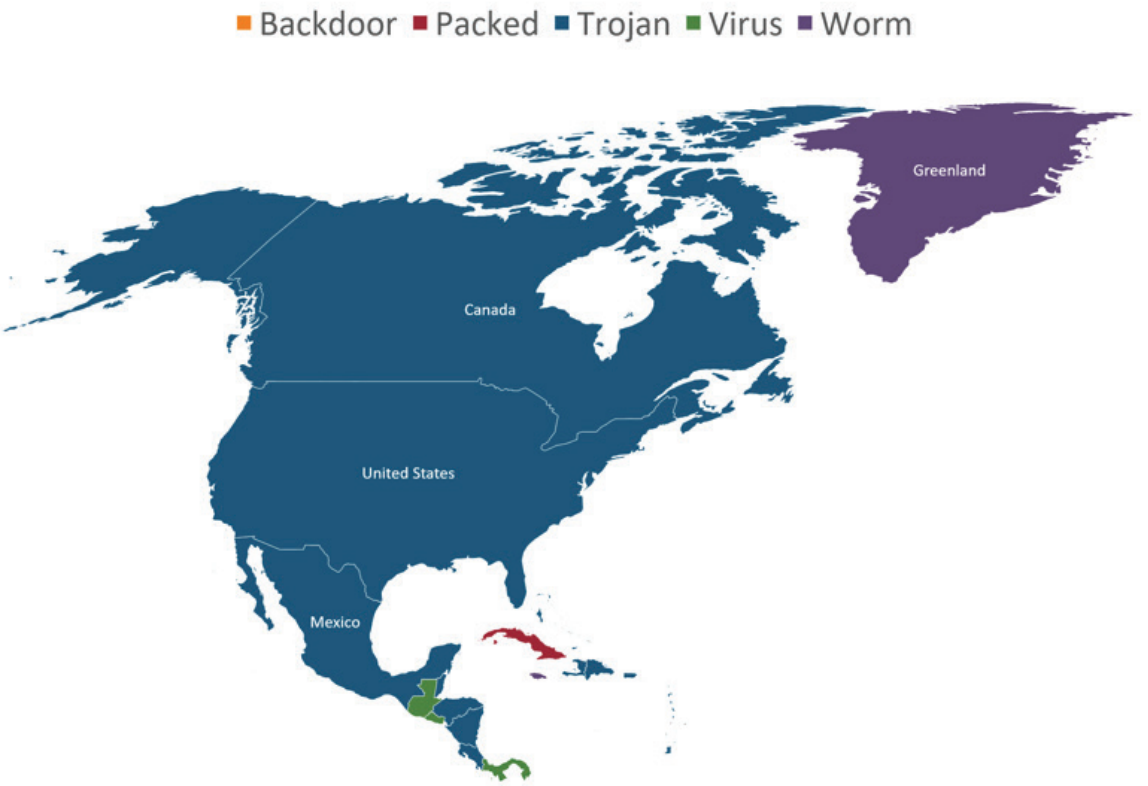
France had a more typical malware profile for Q1 2017, with the highest ratio of trojans, followed by viruses. However, its top trojan, "HackKMS", does not appear to have been studied in-depth at this time, and is in need of further analysis. France's top virus, Expiro, is a Windows threat, first seen in 2011, that steals personal data, lowers security settings, and more.

The UK saw an incredibly high volume of packed malware: 533,940 cases, out of a worldwide total of 1,148,231 — or 46% of Comodo's packer detections for Q1 2017. Thus, similar to its unique role in Europe (see Brexit), the UK appears to have a unique malware profile as well.

Russia, which lies at the intersection of Europe and Asia, and whose enormous landmass naturally disfigures either map, also had a somewhat unusual malware profile. Trojans occupied first place. However, as with many lower socio-economic countries, worms were prominent in Russian malware detections, overtaking viruses for second place. This analysis in part confirms what we already know, that there is a large gap between rich and poor in Russia.

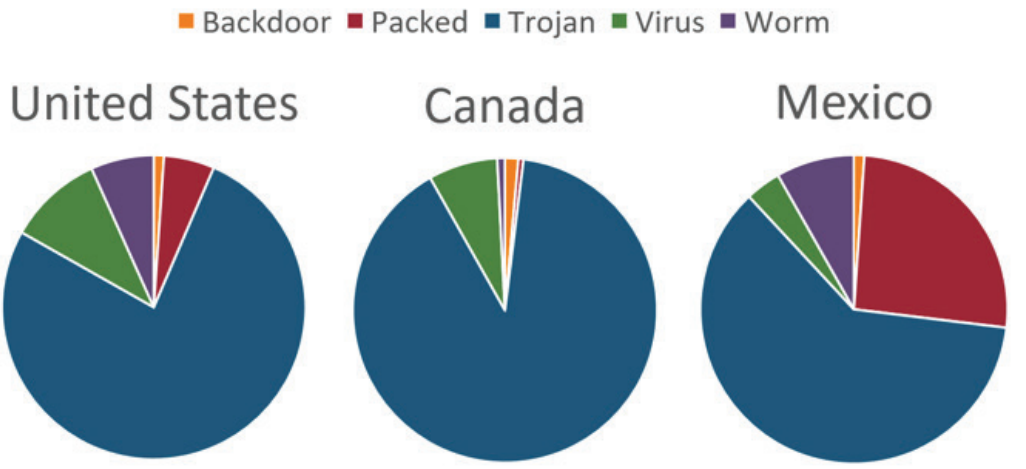
### 4 | North America

The North American continent is dominated by three countries: The United States, Canada, and Mexico, which together account for 84% of the continent's population and an even greater percentage of its Gross Domestic Product (GDP). Perhaps unsurprisingly, the U.S. and Canada share a similar malware profile (with trojans as the top malware type), as does Mexico to a certain extent. However, Mexico suffered a much higher volume of packed malware, which may be connected to similar detections that Comodo discovered in Cuba.




In Central America, Guatemala, El Salvador, and Panama show that this region has a problem with computer viruses similar to Africa and South America. And Greenland, with only 56,000 inhabitants, was also an outlier in the category of computer worms. On balance, we can learn from this analysis that geographically proximate nations should be able to help each other within the discipline of cyber defense because their threat profiles frequently share similarities.

Between the big three countries in North America, the U.S. had the highest ratio of viruses, Canada had the highest ratio of trojans, and Mexico had the highest ratio of packed malware.




In Mexico, BrowseFox was the most common trojan, which Microsoft describes as a "poor reputation" application that injects unwanted processes onto a system, changes browser settings, and installs unwanted browser extensions. Among malware packers, MUPX accounted for 99% of Comodo's detections in Mexico for Q1 2017.

In Canada, Comodo detected 135 unique families of trojans. The most common was Waski, which accounted for 74% of Comodo's overall trojan detections. According to ESET, Waski is a trojan downloader that spreads malware seeking to obtain banking credentials, and has particularly targeted English-speaking countries. Waski can arrive within a ZIP file as an attachment to a spam email, or as an executable file within the icon of a PDF file.

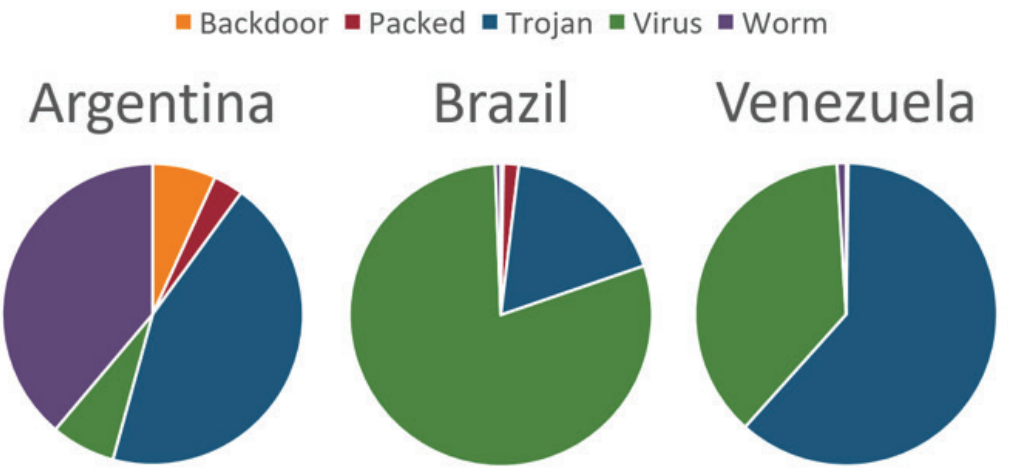
In the United States, Comodo detected an astonishing 378,380 trojans, divided into 711 unique families, making this country and malware combination one of Comodo's most complicated datasets. The most common trojan in the U.S. was Kryptik, which accounted for 24% of trojan detections in the U.S. According to ESET, Kryptik is a banking trojan that has also been used for ransomware operations in the past.

### 5 | South America

In Q1 2017, South America had a rather unique malware profile, divided between the blue and green states depicted below. While the majority of the continent followed the typical pattern of trojans as the top malware category, Brazil, Paraguay, Columbia, and Peru form a band across the middle of the continent that was highly prone to computer viruses.


It will be interesting to see if this trend continues in Q2, and there is a good chance that it will. Based upon these data, a logical hypothesis is that geographic, political, economic, linguistic, or other commonalities help regions to develop a similar malware threat profile. Nothing comes from a vacuum, and cyberspace is merely a reflection of traditional human affairs. Therefore, cyber defense researchers should always try and place their strategies and tactics within a broader geopolitical context in order to maximize their investments.

Argentina, Brazil, and Venezuela have highly divergent malware profiles, so let's see how they compare.




Argentina's top trojan was the generic "Agent," and its top worm was "Brontok," both of which are profiled above.

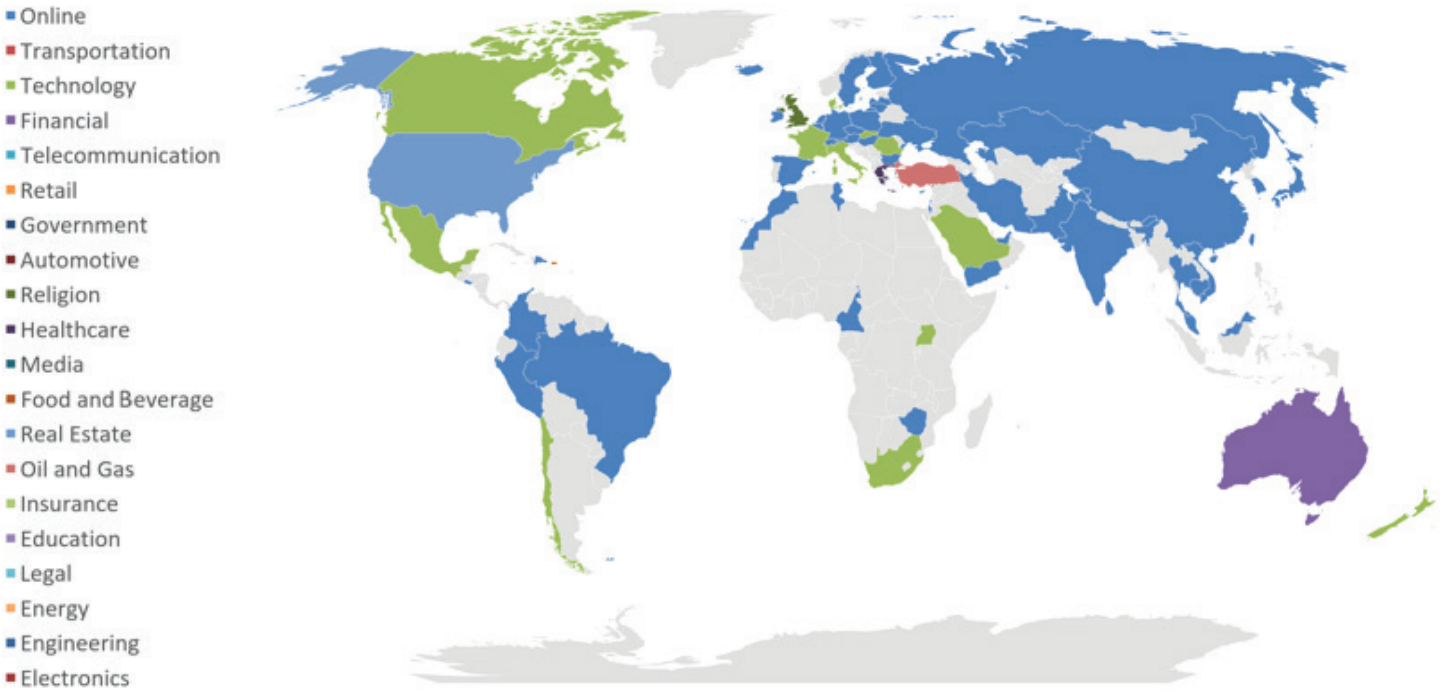
Brazil, similar to Egypt, had a very high volume of viruses, the most common of which was Sality. Sality, which has affected Microsoft Windows systems since 2003, accounted for an amazing 96% of virus detections in Brazil. Sality communicates over a peer-to-peer (P2P) network for spam dissemination, data exfiltration, web server attacks, distributed password cracking, and more.

Venezuela experienced a closer to average malware profile. Venezuela's top trojan belonged to the generic "Obfuscated" malware family, which encompasses hidden exploits in HTML, Javascripts, PDF documents, and more, which try to evade security software detection by hiding malware payloads. Similar to Brazil, Venezuela's top virus was Sality.

## Verticals

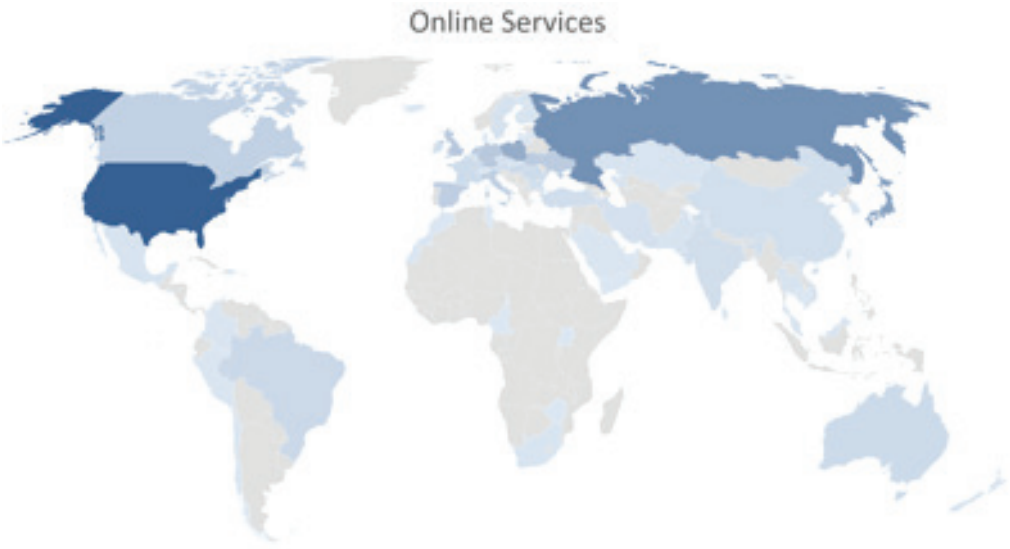
Comodo has begun a large research effort to place its clients in "verticals", or economic sectors, in order to analyze the scope, intent, and impact of cyberattacks upon them individually and for comparative purposes. We expect vertical research to yield significant insight into cyber threats, threat actors and malicious campaigns, which will lead to far better understanding of how to architect and orient cyber defenses.

Based on Comodo detections, here are the top targeted verticals, within each country, for Q1 2017.

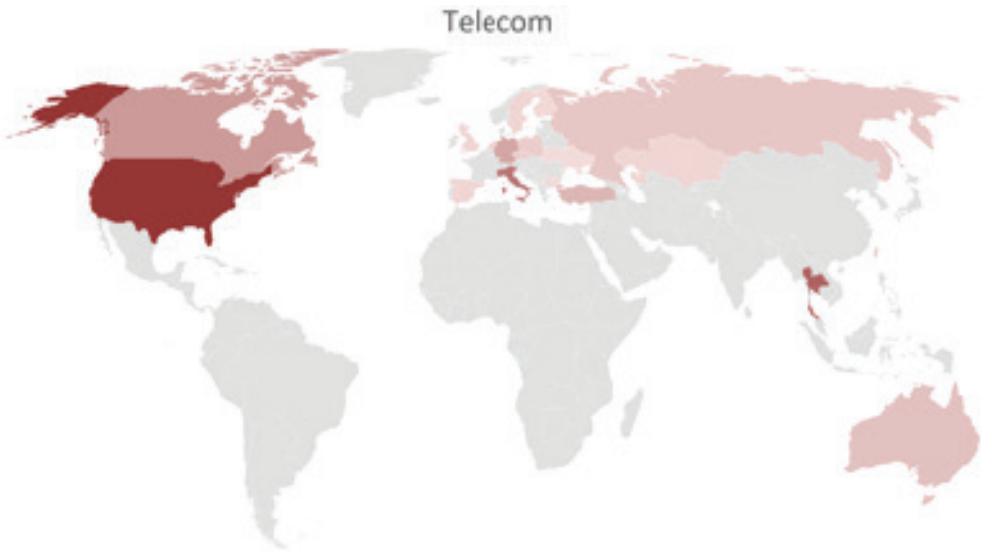



Comodo has only begun to draw this type of map, but even in this first iteration, our research clearly shows the wide variety of verticals that are targeted by cyberattackers. Further, it highlights that nations are not only unique, but every country has unique assets to protect, as well as unique threat actors to defend against — whether they are soldiers, spies, or common criminals.

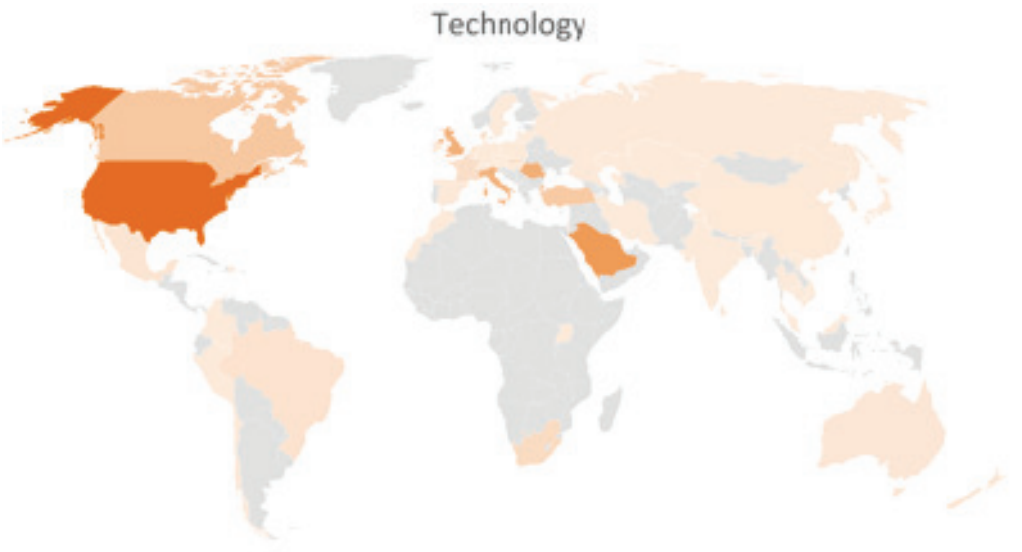
Attacks versus online services pose not just a business threat, but also present a national security challenge to governments around the world. Today, nearly all financial transactions are accomplished via digital means, and critical infrastructures are managed remotely by information technology. The map below shows our malware detections within the Online Services vertical.



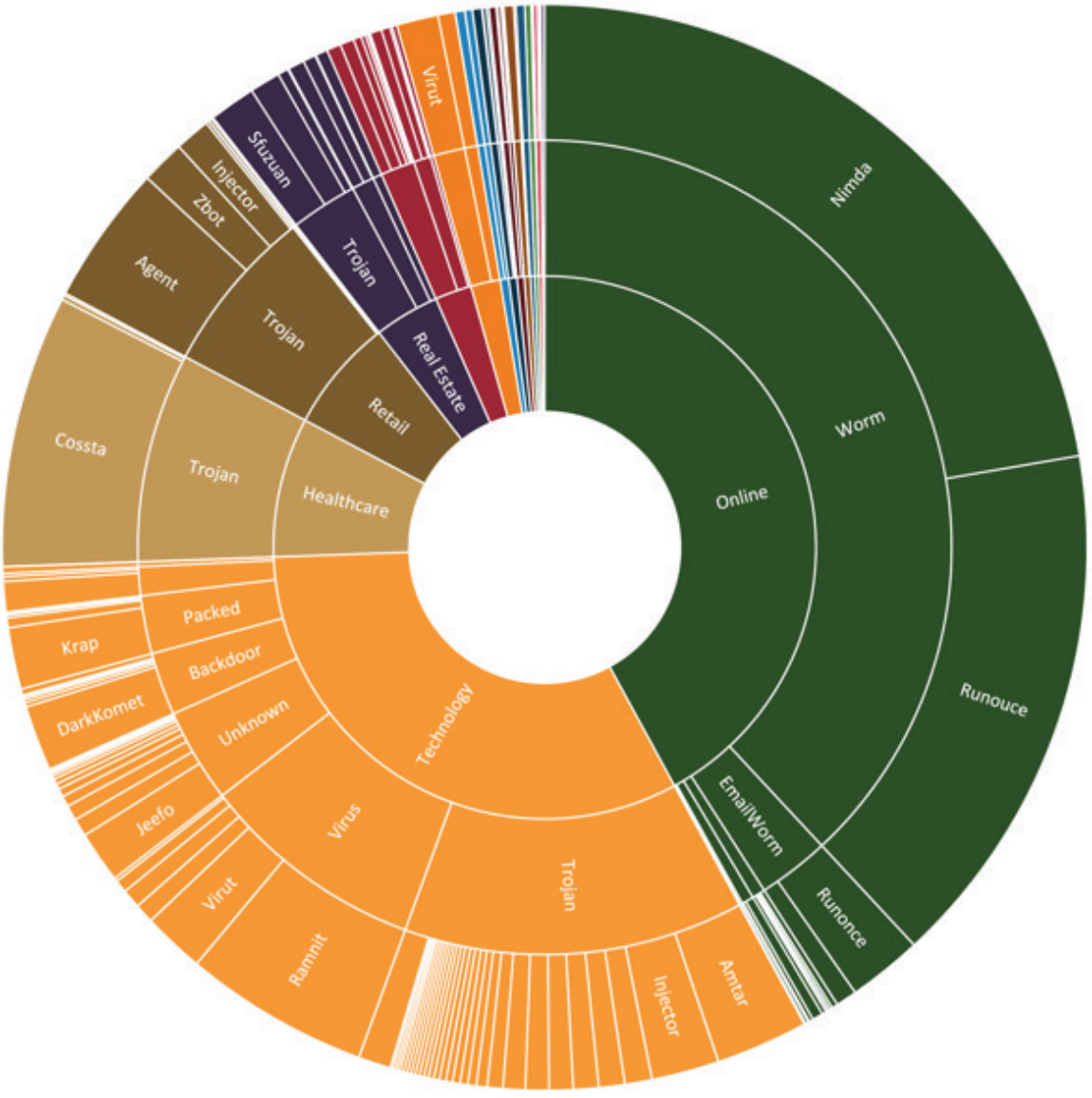

Nation-states and advanced cybercriminals seek to undermine the security of telecommunications providers, from telcos to ISPs to websites, so that they can perform espionage, denial-of-service, and data manipulation against a nearly infinite array of targets. The map below shows Comodo's malware detections within the Telecom vertical.



Hardware and software developers offer the keys to the virtual kingdom of cyberspace by allowing attackers to invade computers, operating systems, and applications in supply chain attacks before they are even deployed, potentially permanently compromising entire portions of the internet. The map below shows our malware detections within the Technology vertical for Q1 2017.



There is an infinite variety of ways to visualize complex datasets, especially in the era of big data. Here is a “sunburst” chart that has three rings, depicting the most frequently targeted verticals, as well as their most common malware types and families. As you can see, for Online Services, computer worms were the chief threat, with Nimda and Runounce the most common malware families. Some verticals, such as Healthcare, currently offer relatively simpler malware profiles. Technology, however, presents an incredibly rich and complex target set, with every malware type detected and hundreds of families to watch out for.



In this final treemap, we take a look at a Malware type that we have mostly neglected in this report: malicious or suspicious applications. In Q1 2017, Comodo discovered such dubious applications, by ratio, within the following verticals.


Below, you can see the top five affected verticals by the overall number of detections as well as their percentages.

| | | | |
|---|---|---|---|
| 1 | Technology | 8,547 | 48.06% |
| 2 | Real Estate | 3,896 | 21.91% |
| 3 | Oil and Gas | 1,543 | 8.68% |
| 4 | Education | 1,133 | 6.37% |
| 5 | Retail | 905 | 5.09% |

Given the prevalence of hidden or obfuscated malicious code around the world, it is wise for system administrators and network security personnel to minimize the use of untrusted applications because there is a good chance that at least some of their functionality may be putting your enterprise data and employees at risk.

## About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals to mid-sized companies to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey, and branch offices in Silicon Valley, Comodo has international offices in China, India, Philippines, Romania, Turkey, Ukraine and the United Kingdom.
**For more information, visit comodo.com.**



**Keep up to date with the Latest Comodo News:**
Blog: *https://blog.comodo.com/*
Twitter: *@ComodoNews*
LinkedIn: *https://www.linkedin.com/company/comodo*

## About Comodo Threat Research Labs

The Comodo Threat Research Labs (CTRL) is made up of more than 120 IT security professionals, ethical hackers, computer scientists and engineers, all full-time Comodo employees, analyzing and filtering input from across the globe. With offices in the U.S., Turkey, Ukraine, Philippines and India, the CTRL team analyzes millions of potential pieces of malware, phishing, spam or other malicious/unwanted files and emails every day, using the insights and findings to secure and protect its current customer base and the at-large public, enterprise and internet community.

**Comodo Group, Inc.** | 1255 Broad Street, Clifton, NJ 07013 US
Tel: +1 (888) 266-6361 | Tel: +1 (703) 581-6361 | Fax: +1 (973) 777-4394