COMODO

# Comodo Threat Research Labs

## Q2 2017 REPORT

# Table of Contents

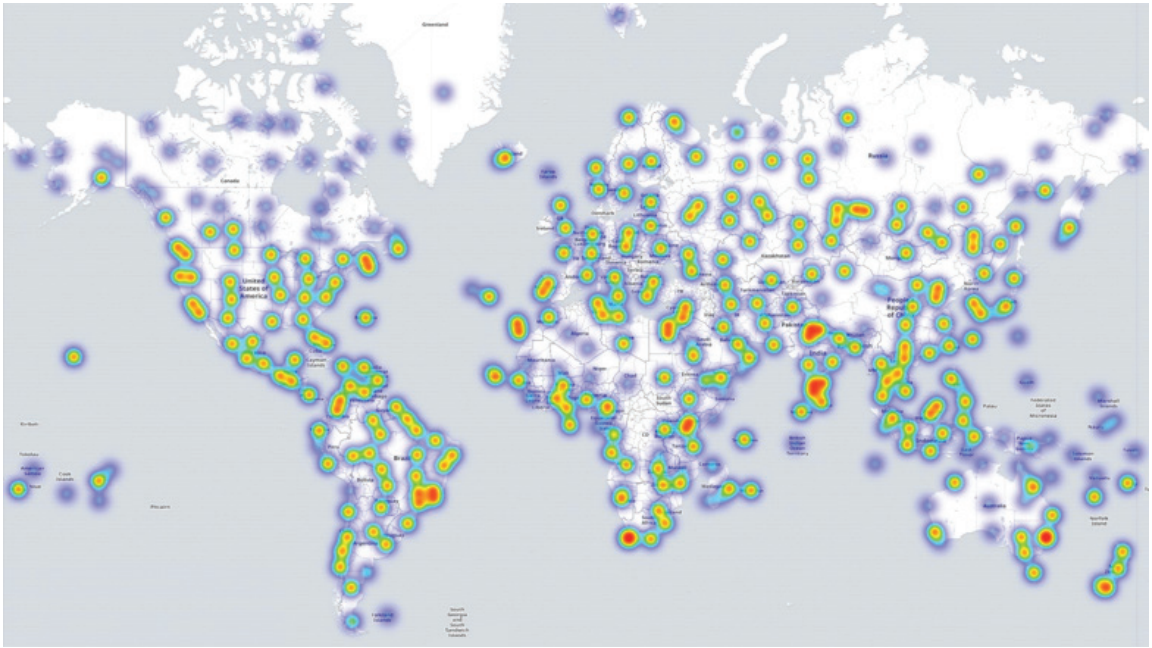
## Executive Summary

- Comodo detected 97 million (M) malware incidents in every corner of the globe
- Detections occurred in 236 of the world's 253 country code top level domains (ccTLD)
- The most acute malware threats were 5.8 M trojans, 4.5 M worms, 2.6 M viruses and 209 thousand (K) backdoors
- The beginning of Q2 saw a dramatic rise in worm propagation
- Viruses returned at the end of Q2, moving back into 2nd place
- Russia had a steady level of malware detections throughout Q2
- The Philippines and Indonesia had a very high infection rate at the start of Q2
- The U.S. experienced dramatic swings, with its sharpest spike during the week of May 8
- The U.S. was almost exclusively dominated by trojan detections
- The Philippines, Russia and Indonesia suffered the highest number of worm infections
- Russia was the top target for viruses and Poland for backdoors
- Upatre was the top trojan, with the U.S. as its top detection country
- Brontok was the most common worm, from which the Philippines suffered most
- Ramnit was the most common virus and Russia its top victim
- DarkKomet was the top backdoor, with Poland and Turkey its top detection countries
- Vertical analysis reveals that attackers are currently focused on Telecom, Technology and Online Services

## World Map of Malware

This is Comodo's Q2 2017 report on malware detections worldwide. On balance, things do not seem to be getting better. With international security in a state of rapid evolution, from NATO to the Middle East and North Korea to the South China Sea, the challenge of fighting malicious code has not gotten any easier – a situation that has led to the rise of professional cybercrime, a "golden age" of espionage and even preparations for cyberwars. In Q2 alone, Comodo detected nearly 97 M malware incidents within 236 of the 253 country code top level domains (ccTLD).

The map below clearly shows that, wherever there is human civilization, from the Falkland Islands to the Faroe Islands and from Bermuda to Seychelles, there is malicious code. Planet Earth is literally covered in malware.

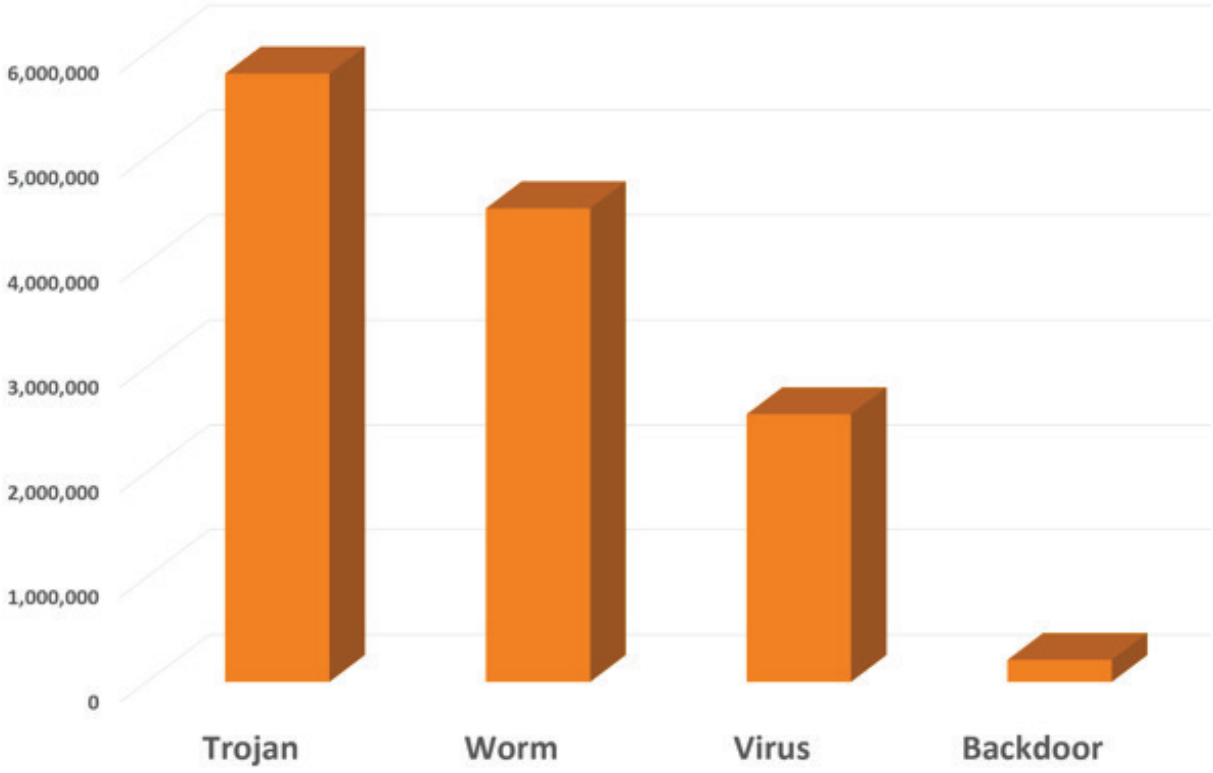


Comodo has been creating information technology for nearly 20 years and has software installations in every nation. Thus, our company is ideally suited for strategic analysis in the cybersecurity domain. The deep red clusters, visible in India, South Africa, Brazil and the U.S., show the higher malware concentrations for Q2 2017, but the most important takeaway from this map is simply the breadth of the cybersecurity problem.

Cybersecurity is fundamentally an international problem that takes advantage of the limited sovereignty of governments and the finite jurisdictions of law enforcement to create a space in which crime, espionage and even preparations for war take place in a dimension characterized by a high level of anonymity, deniability and immunity from retaliation or prosecution. Imagine you are an American hacker wanting to rob an American bank. With a little work up front, you can route your digital communications through compromised computers in China, Iran and Zimbabwe and bang – you have near instant anonymity. Why? Because the odds that law enforcement, counterintelligence and network security managers in that collection of countries are going to collaborate on an international investigation are very low. Thus, the victim is often left with only poor choices: to hack back (which is illegal) or call the Avengers.

## Primary Malware Types

In this Q2 2017 Report, we will focus primarily on the most common – and dangerous – threats facing most enterprises today: trojans, worms, viruses and backdoors. These top four categories comprise more than 13 M incidents, including 5.8 M trojans, 4.5 M computer worms, 2.6 M computer viruses and 209 K backdoors.




First, let's define these four malware types. A "trojan" borrows its name from the famous wooden horse in Greek mythology, which was used to facilitate the invasion of Troy. It refers to any seemingly useful or benign computer program that has hidden, usually malicious, functionality. Attackers often use social engineering to trick users into downloading and installing these programs, via email or malicious advertising.

A computer worm travels the internet autonomously, exploiting vulnerabilities in network defenses as it spreads from network to network and computer to computer. Its goal is typically to deliver a malicious payload to the victim computer, which can lead to the installation of a trojan or the creation of a backdoor. However, even worms without a payload can consume enormous bandwidth, diminish network or local system resources and possibly cause a denial-of-service.

A 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. However, unlike a worm, 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 and potentially damaging hardware, software or data.

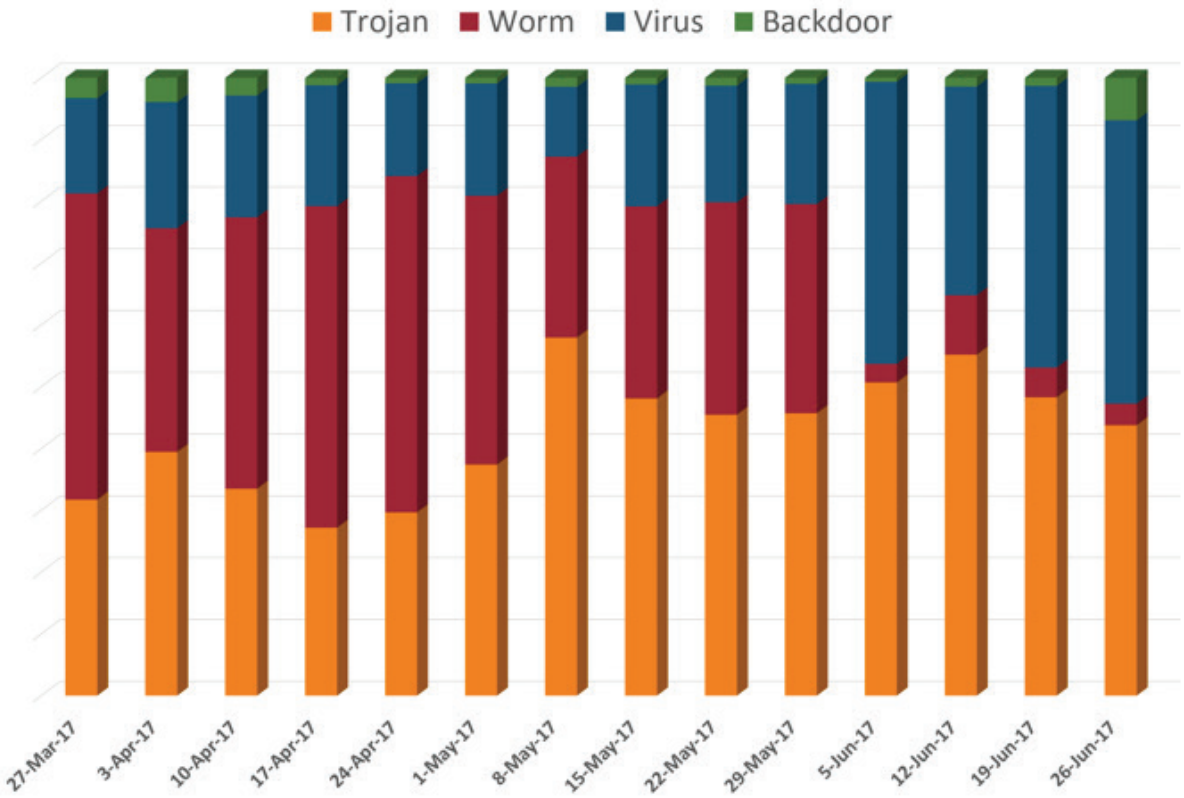
A backdoor is a hidden way to bypass normal user authentication, which can be leveraged to gain covert, remote access to a computer system, cryptosystem or algorithm. A backdoor can be an installed program (such as Back Orifice) or it can be a modification to an existing, legitimate program. Backdoors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

Remember, a cyberattack is not an end in itself, but a means to a wide variety of criminal, political, intelligence and military goals. All of the malware types above are designed with the aim of giving an unknown, remote attacker access to and control over your computer. From there, the possibilities are myriad and limited only by the imagination of the attacker. However, attacks do tend to fall into one of three primary categories: data denial, data theft and data manipulation. There are some logical overlaps in many operations, of course, but usually an attacker wants to 1) stop you from doing something with a digital denial-of-service; 2) steal your data, such as banking credentials; or 3) alter data, such as a stock price.

## Malware Timelines

The next two graphics show a timeline of discovery, worldwide, by malware type and country of detection. Some hours, days and weeks have dramatically different volumes of data transmission – and malware detection – so these bar charts have been set to a 100% scale, by week, for Q2 2017, so that they are easier to read.

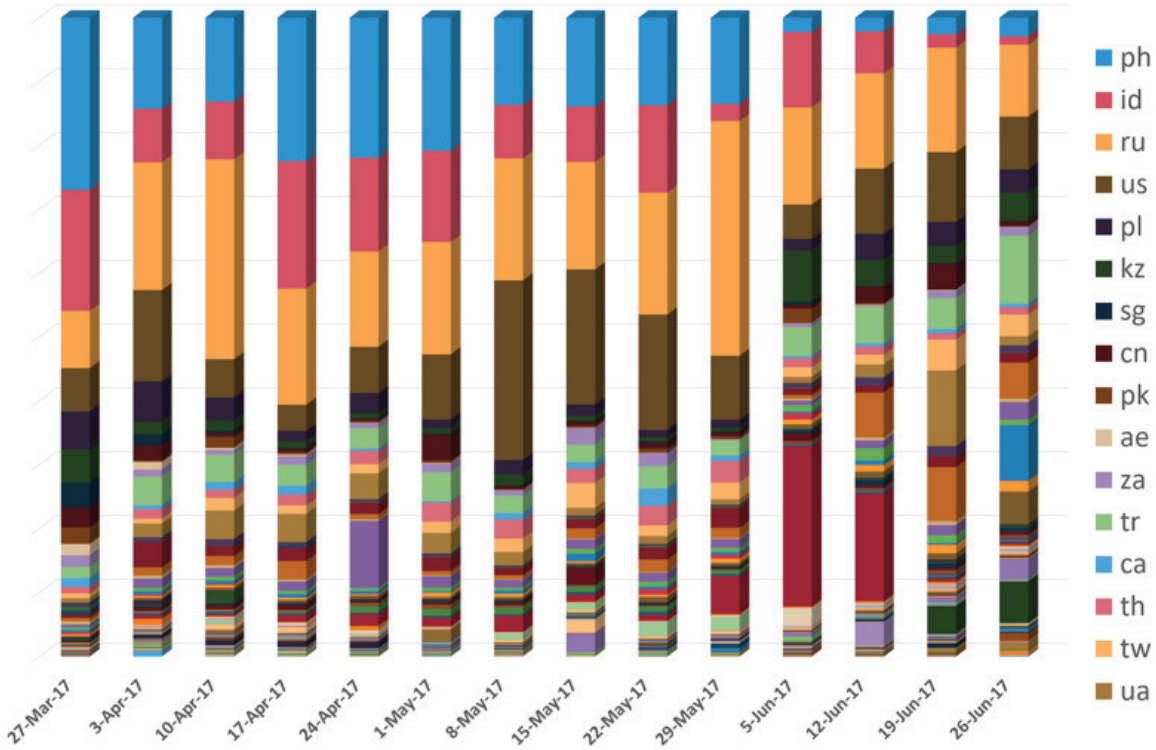
The first timeline shows the relative detection rate for each malware type as compared to the others. A timeline, by the way, is one of an analyst's best friends. Albert Einstein famously said that time exists so that not everything happens at once. Placing the data in this format highlights trends and cause-and-effect relationships (especially when both cyber and non-cyber incidents are considered) and even allows for the creation of models for prediction.




This timeline clearly shows that the beginning of Q2 saw a dramatic wave of worm propagation, only to taper off by the end of the quarter. At the end of June, trojans had regained their position – as in our Q1 2017 data – as the world's #1 malware type, with virus (again) in second place.

Backdoors were again our 4th ranked type but had clear spikes at both the beginning and end of Q2. Each of these malware types will be examined separately in its own section later in this report.

In the next graphic below, we can see that not only malware types, but also victim networks and nations, have a highly dynamic quality and change during every hour of every day. This bar chart depicts the weekly, combined volume of detections for the four top malware types – trojan, worm, virus and backdoor – by country, for Q2 2017. This chart demonstrates at least two things: 1) how malware infections spread across the Earth and 2) which countries experience outbreaks at any given time.




In the first half of Q2, for example, the Philippines and then Indonesia, had a very high infection rate, which settled down by the end of the quarter. Given the two nations' geographic and socioeconomic similarities, this makes logical sense. Further, it is important to realize that cyberspace is merely a reflection of traditional human affairs. Therefore, all major political and military events have their digital reverberations. While it is difficult to prove that any two events have a direct cause and effect relationship, both

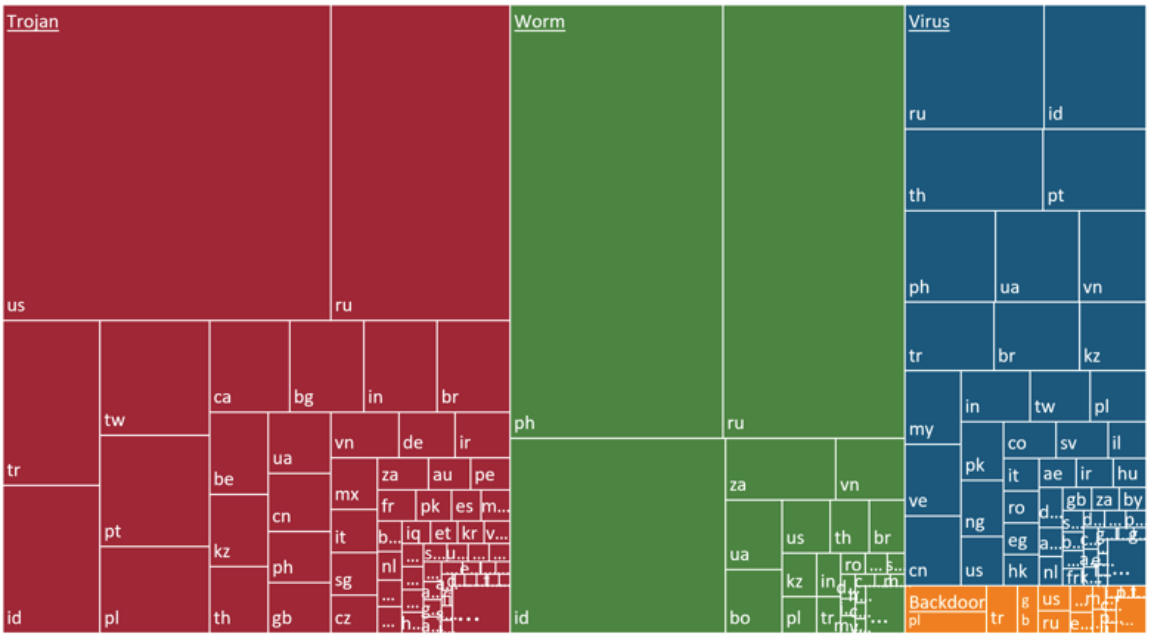
the Philippines and Indonesia had their share of political turmoil during this time period. For example, the BBC reported that in May 2017, martial law was imposed on the Philippine island of Mindanao due to political violence; and in Jakarta, the capital of Indonesia, the city's Christian mayor received a two-year jail sentence for blasphemy.

Russia had a steady level of malware detections, with spikes during the weeks of April 10 and May 29. The U.S. experienced more dramatic swings than Russia, with its sharpest spike during the week of May 8. Turkey suffered its biggest outbreak during the final week of Q2. And finally, further down in the data stack, notice the purple spike on April 24? That's Vietnam. The rising red bars at the beginning of June? Portugal. For each of these countries, it is possible that malware outbreaks and campaigns had a purely cybercriminal logic and rationale, but deeper analysis may reveal that political, intelligence or military operations were the real causes – either directly or indirectly.

If you want to know more about where your country, city, state or province lies within Comodo's data – and why – please send an email to malwaresubmit@avlab.comodo.com.

## Malware Types by Country

Now let's take a different perspective on the same data. Where exactly were these malware infections detected? In the chart below, the top four malware types are depicted by ratio, along with the specific countries of infection. Here we have a greater opportunity to associate malware types – and eventually families, campaigns and threat actors – with real world people, places and things.




Trojan, the most widespread and complex malware type, found its most spacious and comfortable home in the U.S. As we saw in Comodo's Q1 report, a combination of large population, high connectivity and national wealth combine to make the U.S. the most lucrative overall target for cybercriminals (as evidenced by the rise of ransomware and its recent migration from the Former Soviet Union to the U.S.). Overall, - trojan is a high class of malware, deployed for a high return on investment. This is why we see not only the U.S., but other countries with a relatively high gross domestic product (GDP), including Turkey, Taiwan, Portugal, Poland and Canada, near the top of the list.

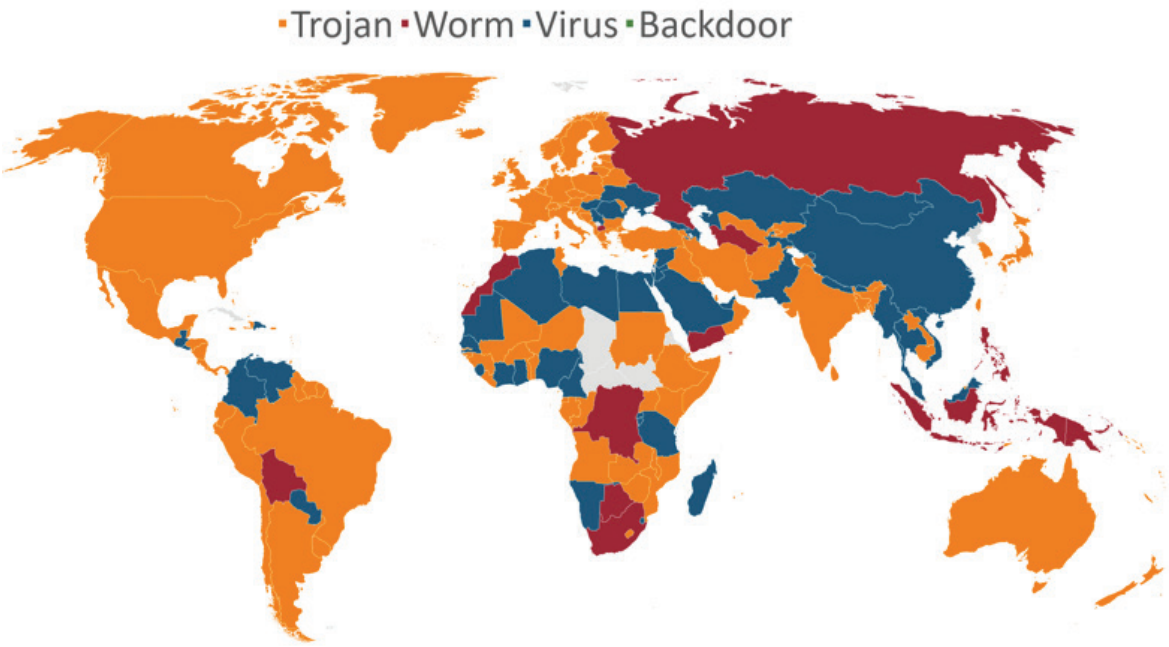
Computer worms, in Q2 2017, found many vulnerable networks to exploit across the world. Indeed, worms displaced viruses as Comodo's #2 malware threat based on our overall number of detections. However, from a strategic perspective, worms have a very different victim set. Look at where the detections took place: in descending order, they are the Philippines, Russia, Indonesia, South Africa, Vietnam, Ukraine and Bolivia. What this means is that worms, which travel the world autonomously seeking low-hanging cyber fruit, are typically taking advantage of older, unpatched and perhaps unlicensed software. Countries with a high ratio of computer worms to overall malware detections are generally not in good political and/or economic shape; thus, worms are themselves, from a national perspective, an "indicator" of other types of non-cyber compromise.

Viruses are similar to worms, both in architecture and in target set. Other nations making an appearance on this list include Thailand, Brazil, Kazakhstan, Malaysia, China, India, Pakistan and Nigeria. However, it is also important to note that viruses are a more complex malware set, evidenced by the greater number of victims and their more evenly spread distribution in the chart, which means that viruses are not confined to a small group of victim nations but are fairly evenly scattered throughout across the world. Nonetheless, it should be noted that the countries most impacted by viruses tend to be in the lower socioeconomic tier of GDP.

Finally, backdoors are an even higher value and higher return-on-investment malware type than trojans. The top country for backdoor detections was Poland, followed by Turkey, the United Kingdom and the U.S. As detailed in Comodo's Q1 malware report, countries with the highest ratios of backdoors to overall malware detections are the richest within these four top malware types. Cyber attackers are not stupid and will use their most valuable malware against the most valuable targets. The reasons are clear: first, the target probably has a professional network security staff, which presents a greater obstacle; second, the potential rewards, in terms of intelligence collection or facilitated cyber operations, are simply worth the investment.

Each of these malware types will be covered in greater detail later in this report.

Next, let's plot these data on a world map, with each country painted according to its top malware type. Immediately, Comodo's strategic data set yields surprising insight and points to numerous high-level trends, both in cyberspace and in traditional geopolitical space.



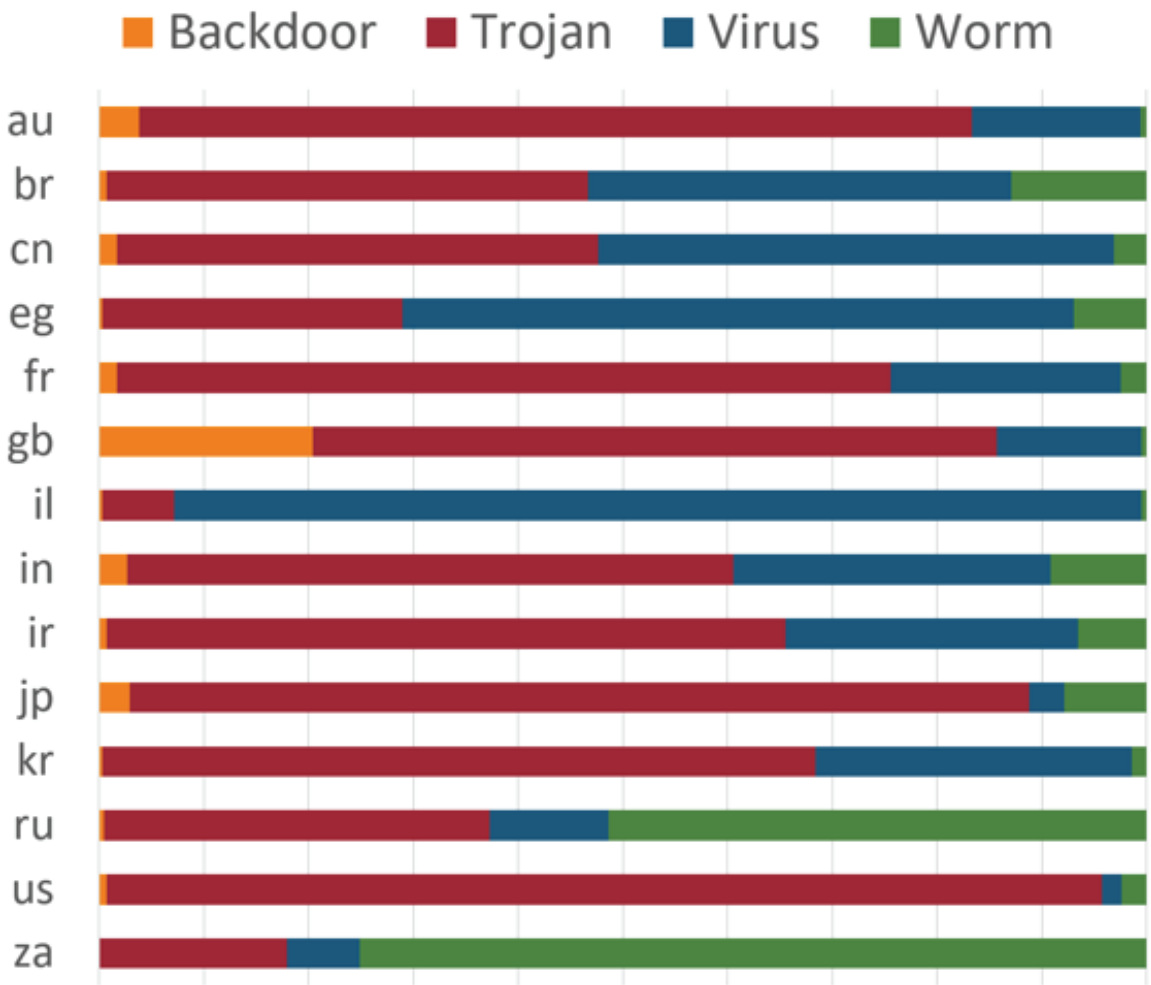

First, trojans uniformly dominate the richer regions: North America, Western Europe and Australia are all the same color. For system administrators and network security personnel, this means that 1) they have a particular, identifiable problem on their hands and 2) possessing this strategic insight can help them to solve it.

Second, South America, Africa, Asia, the Former Soviet Union and Southeast Europe, relatively speaking, have many more viruses and worms. In fact, in many of these countries, viruses and worms were the top overall malware threats. In these countries, it is time to take cybersecurity more seriously. Viruses and worms take advantage of low-hanging cyber fruit – especially worms, which do not even need the added human help of opening a malicious attachment or clicking on a bad hyperlink (as with a virus).

Third, it is hard to miss the fact that so many countries with similar malware profiles are next-door neighbors. What this means for network security administrators and cyber defense analysts is that geographic, linguistic and telecommunications associations will help to determine any nation's threat profile and local experts, who are suffering through the same challenges, should be called up for help. This is great intelligence and should be heeded by network security specialists.

## Malware Ratios within Countries

Now let's go a level deeper and examine the ratio of each of the top four malware types within a sample of world nations. This analysis helps to highlight strategic trends across the planet and gives each country a good idea of its biggest current threat category.




Notice that Australia (au), France, (fr), Japan (jp) and the U.S. (us) have similar malware profiles, with a clear predominance of trojans. These countries are peers in traditional geopolitics and that fact is reflected in the malware data. The UK (gb) is a bit of an outlier here with a much higher percentage of backdoors, which echoes what we saw in Comodo's Q1 report. Continental Europeans – and Brits – have always felt that the UK was bit different and here is further proof.

Brazil (br), China (cn) and Egypt (eg) have a much higher detection rate for viruses at the expense of trojans. Each case may have unique aspects to it, but if you want more data, please send Comodo an email. And something unusual definitely happened in Israel, which saw the most viruses in this group by far. Socioeconomically, Israel appears to be the outlier in this group, since it possesses a highly advanced economy and is well-known for its cyber defense prowess.

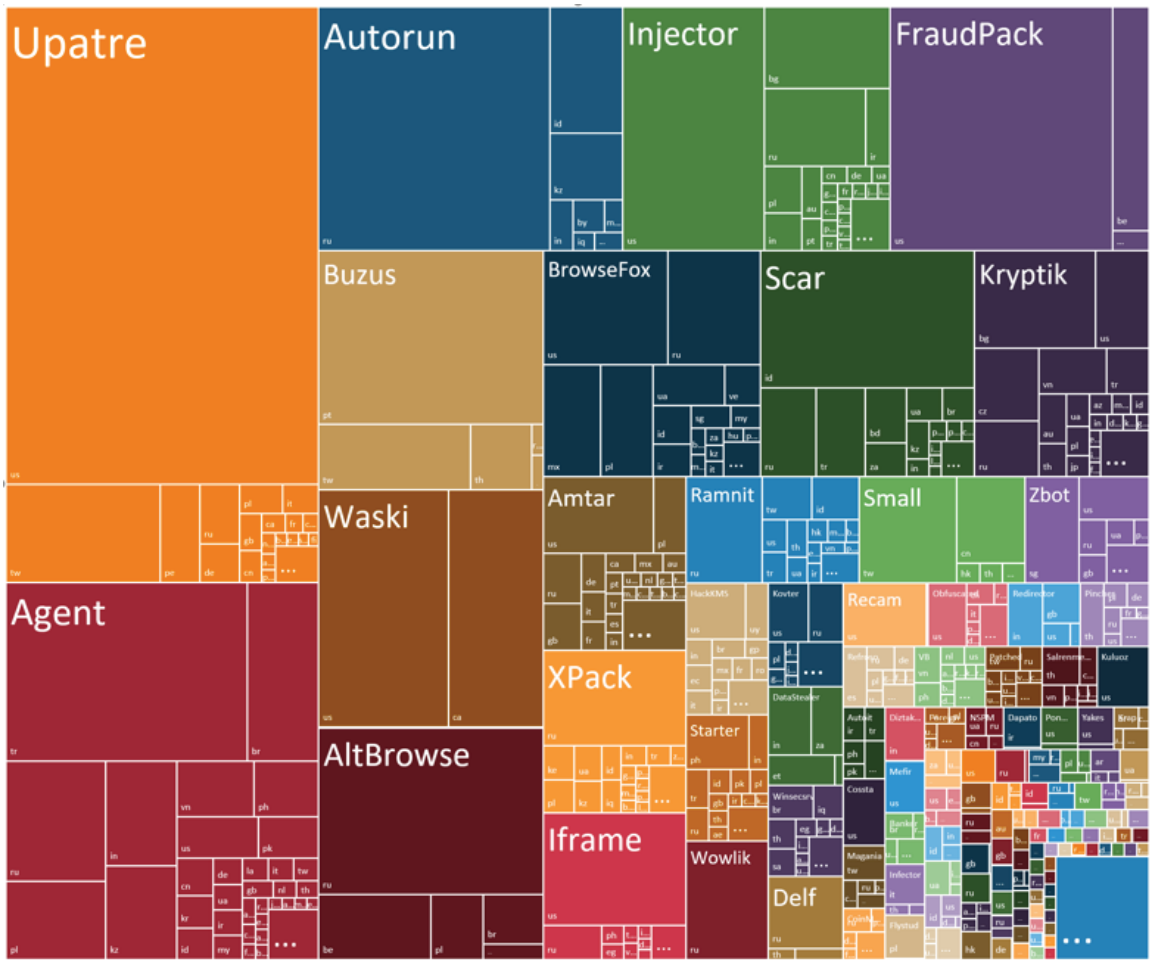
India (in), Iran (ir) and South Korea (kr) were somewhere in between the first two groups, with mostly trojans but also many worms. These are three very different nations; however, they are all located in Asia and have large, well-connected IT sectors. Still, more analysis is necessary.

Finally, Russia and South Africa suffered the highest volume of computer worms when compared to any of the other countries in this peer group. Frankly, this situation should be urgently addressed within Russian and South African IT security communities. Given the nature of worms, what this means is that many networks in these countries do not have nearly enough licensed, patched and professionally managed hardware and software. Part of this problem, of course, is non-cyber and may take years to rectify.

## 1 | Trojans

Now let's have a closer look at each malware type to include the individual malware families they comprise. The charts below show not only the malware type and families, but also the countries in which the detections took place. Thus, each chart displays literally millions of malware incidents from around the world and contains highly actionable strategic and tactical intelligence.

This chart shows that each nation has a unique malware profile and a close study of the following pages can help cyber defenders in any country to zero in on the most important current cyberthreats facing them and tailor their defenses in the most optimal ways.



Trojan is currently the world's most prevalent – and complex – malware type, which means that trojans are at the same time the most urgent and yet challenging cybersecurity problem. Furthermore, once a trojan is installed, it can be used for any purpose. Essentially, trojans give an unknown, remote attacker control over your computer and anything is possible, from the theft of passwords to the installation of ransomware and outright data destruction.

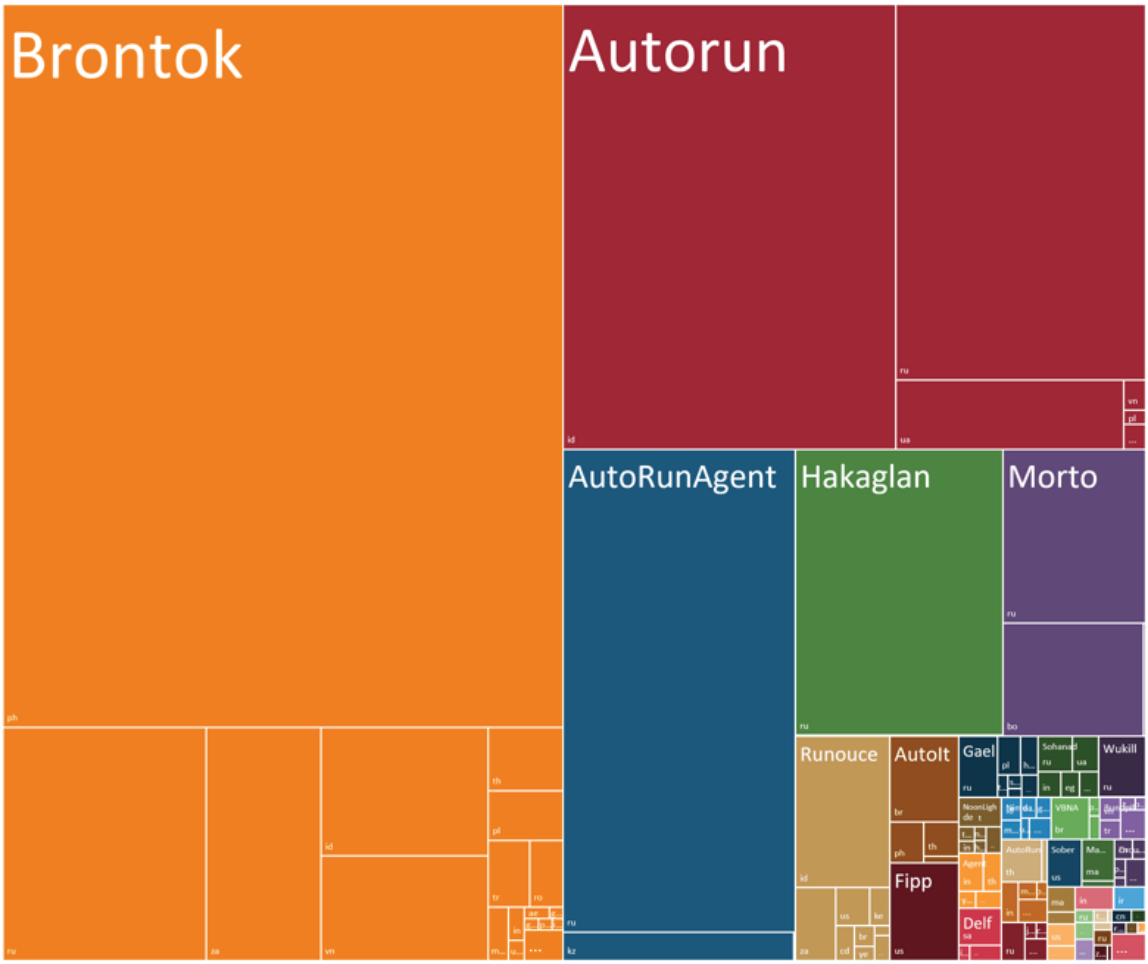
The U.S. was the clear top victim for Upatre, Injector, FraudPack, Waski, Amtar, Iframe and more. Russia, by contrast, suffered the most from Autorun, AltBrowse, XPack, Ramnit, Wowlik and Delf. Turkey should focus on Agent, Portugal must tackle Buzus, Indonesia should figure out Scar and Bulgaria must confront Kryptik, etc.

Let's take a closer look at Upatre, which was Comodo's most frequent trojan detection for Q2 2017. According to Microsoft, this Windows-based trojan has a "Severe" threat rating. Upatre has been disseminated as an attachment to spam, for example, from the Cutwail botnet and will attempt to download further malicious software such as Zbot or the password stealing malware Win32/Dyzap. An example attachment name is "Case_<random number>.zip" and email messages have referred to healthcare, car licenses or taxes.

If you would like more specific threat intelligence for your country, city, state or enterprise, please send an email to malwaresubmit@avlab.comodo.com.

## 2 | Worms

Computer worms were Comodo's second most common malware type in Q2 2017 and there were some severe outbreaks in Q2. However, these outbreaks were mostly confined to the second half of the quarter, most notably in the Philippines, Russia, South Africa and Indonesia. When compared to trojans, this malware type is simpler, specifically in the number of families to watch out for.



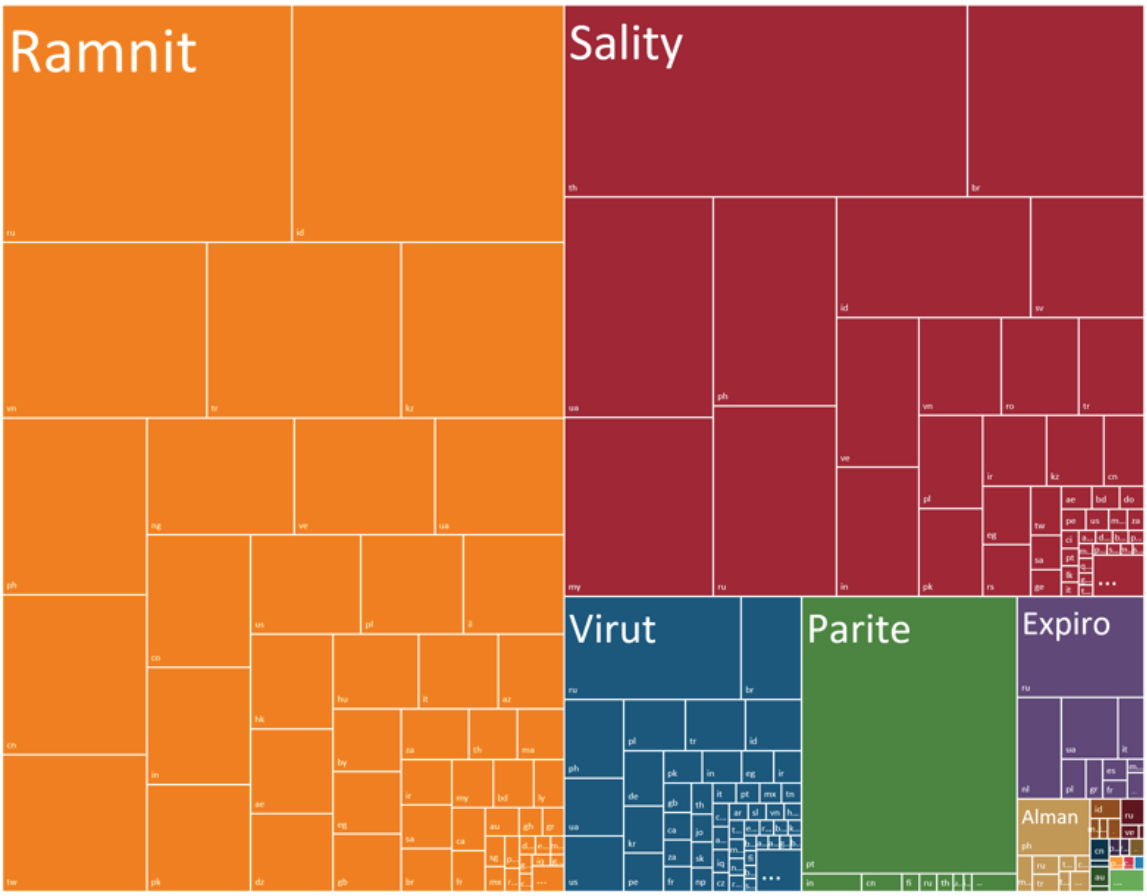
Just as in Q1, Brontok was Comodo's most frequently detected worm. According to Microsoft, Brontok is a "Severe" threat to Windows that spreads via email. It has its own email engine and sends itself to email addresses found on a victim computer, spoofing the victim's email address as the purported sender. It can also copy itself to USB and pen drives.

Brontok can disable antivirus and security software on an infected machine. Brontok has been used for hacktivist purposes in the past, including denial of service (DoS) attacks, such as in 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. In Q2, the majority of Brontok infections were in the Philippines, followed by Russia, South Africa, Indonesia, Vietnam and Thailand.

Another key takeaway from this chart is the prominence of Russia, which was not only the second most affected country by Brontok and Autorun (the second most frequently detected worm), but Russia was the top victim of the next three most common worms: AutoRunAgent, Hakaglan and Morto. In a strategic sense, this means that Russia currently faces an incredible cybersecurity challenge. Worms take advantage of older, unlicensed or poorly patched computers and networks. This situation poses a long-term threat to the health of Russian cybersecurity efforts, which will take enormous time, effort and money to fix.

### 3 | Viruses

Virus was Comodo's third most common malware type detected in Q2 2017. The chart below tells a mixed story: as compared to computer worms, there were overall fewer viruses, but they infected more countries. Thus, it is hard to say whether this is a more or less complicated dataset than recent computer worms.

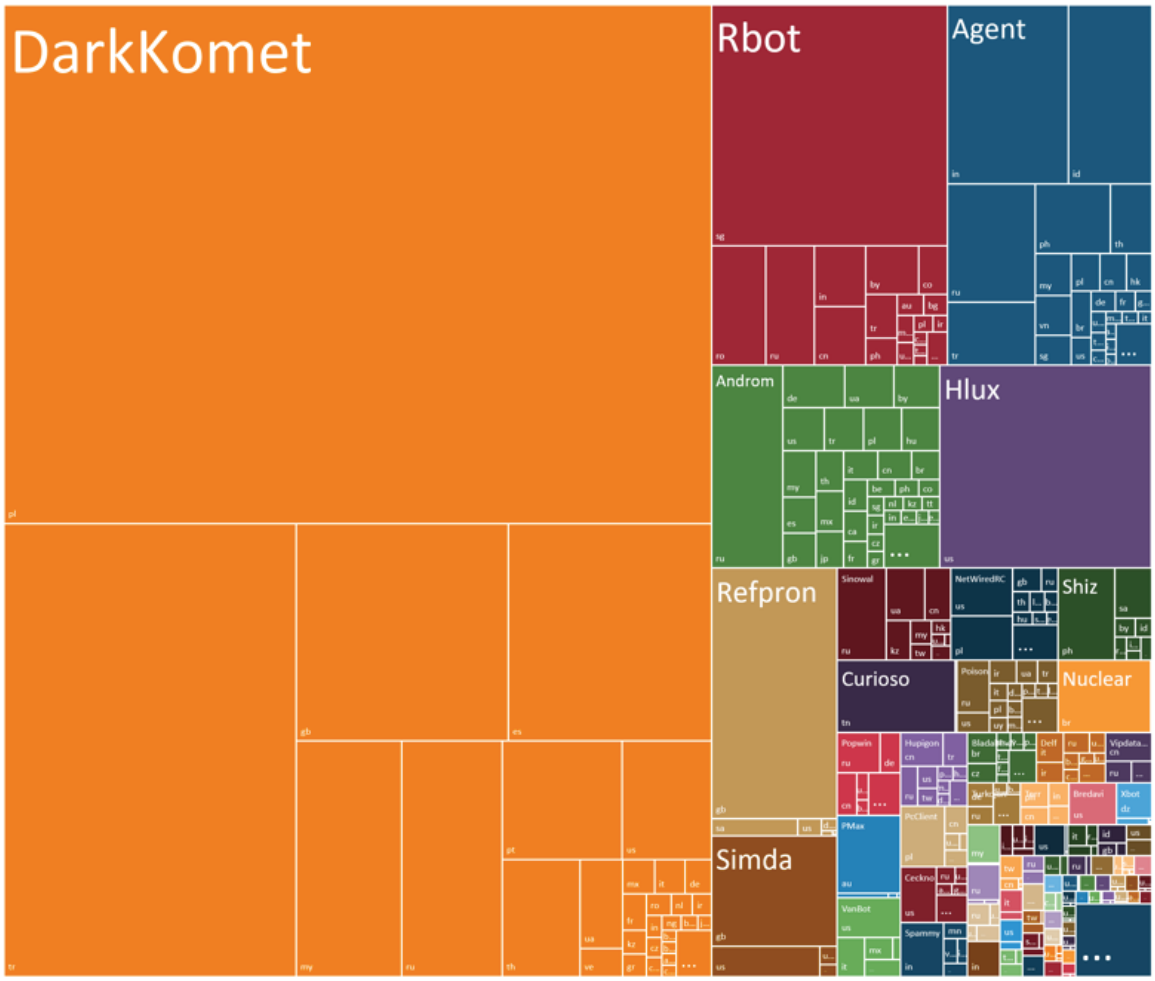


As in Q1, Ramnit was the most common virus detected. Microsoft rates this virus as a “Severe” threat to Windows systems, which can propagate via executable files with extensions like .exe, .dll, .scr or removable drives such as a USB stack and seeks to steal sensitive data, including account passwords and banking credentials. Ramnit will also try to disable security software and make changes to Windows registry settings. This virus was most prevalent in Russia, followed by Indonesia, Vietnam, Turkey, Kazakhstan, the Philippines, China and Taiwan.

Other prominent viruses were Sality, whose top victim country was Thailand; Virut and Expiro, with Russia as their top target; and Parite, which almost exclusively penetrated Portugal.

## 4 | Backdoors

As discussed in Comodo's Q1 report, backdoors are a high value and high return-on-investment type of malware. And while their overall detection rate is the lowest of the top four malware categories, backdoors offer a secret way into a computer system that can be devastating for the victim, especially over the long-term.



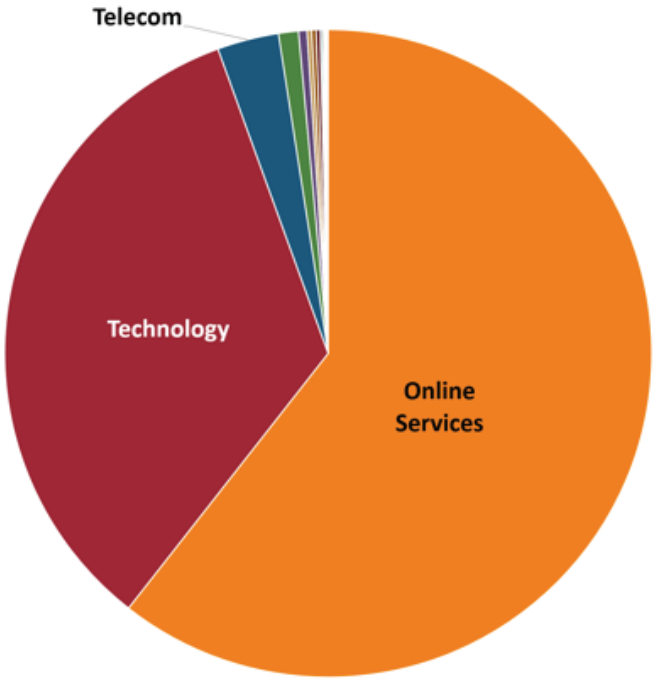
Despite its smaller overall size, this chart shows that backdoors are, in fact, a highly complex malware type, with many families and many victims. One family – DarkKomet – dominates the overall numbers, but the right side of the chart is a virtual maze of colors – and deep compromises – around the world. Further, our data suggest that backdoors are used with precision targeting: DarkKomet dominated Poland and Turkey, Rbot primarily penetrated Singapore, Agent was most active in India, Androm in Russia, Hlux exclusively in the U.S. and Refpron and Simda in the U.K.

Why are backdoors so dangerous? Let's take a closer look at DarkKomet (or DarkComet), which is a remote administration tool (RAT) that has been refined since it was created in 2008. DarkKomet is frequently disseminated via drive-by attacks by malicious code embedded on websites or by sending tainted links through social media. It allows an attacker to control a compromised system via graphical user interface (GUI) and can be used to take screen and sound captures, log keystrokes and crack passwords. Its resume includes use in nation-state operations, reportedly in the U.S., Syria and France.

## Vertical Analysis

One exciting new research effort at Comodo is to place our clients within certain "verticals" or economic sectors. This initiative will allow for a better categorization of malware threats, actors and campaigns. And what we have found so far is not entirely surprising but still eye-opening. The pie chart below shows our vertical analysis for Q2 2017, with Telecom, Technology and Online Services already identified as top targets.

Attackers are going after information technology (IT) creators and providers in a big way. Why? The reason is because, in military parlance, subverting IT is a "force multiplier." By compromising the software that is used by millions of users around the world, attackers can increase the number and variety of victims to a virtually unlimited number. Today, nearly all financial transactions are accomplished via digital means and even critical infrastructures are managed remotely by information technology.




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. This type of targeting is so serious that it poses not only a threat to business, but to national security, democracy and human rights as well. Today, advanced cybercriminals, as well as nation-states, seek to undermine these systems so that they can perform espionage, denial-of-service and data manipulation against a nearly infinite array of targets.

## 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, the 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, the 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