COMODO

Comodo Threat Research Labs

GLOBAL MALWARE REPORT 2017

Table of Contents

Executive Summary

Top Malware Types: Trojans (41%), Applications (24%), Backdoors (10%)

- Comodo Malware Detections
  - Trojans in 225 countries; Russia #1 at 9%
  - Applications in 226 countries; U.S. #1 at 3%
  - Backdoors in 184 countries; Russia #1 at 19%
  - Worms in 200 countries; Russia #1 at 19%
  - Unsafe applications in 183 countries; U.S. #1 at 4%
  - Unwanted applications in 184 countries; U.S. #1 at 5%
  - Viruses in 190 countries; U.S. #1 at 9%
  - Malware packers in 189 countries; U.S. #1 at 2%
- Top Ten Countries of Detection
  - Russia, U.S., Brazil, India, Canada, Germany, China, Poland, Turkey, UK
- Malware Trends
  - Most malware types remained even or declined in Q4 2017
  - Notable exception: backdoors saw a significant rise in Q4 2017
  - Comodo predicts that backdoors will continue to rise in Q1 2018

Geopolitical Correlations

- North America
  - U.S. - Mexico political disputes
  - 2017 U.S. elections
- Europe
  - Political turmoil in Czechia
  - Elections in Norway
- Asia
  - North Korean nuclear and missile tests
  - Chinese, U.S., Japanese military activities
- Middle East
  - Crises in Qatar, Egypt
  - Military exercises and operations in Israel and Syria
  - Trump visit to Saudi Arabia
- South America
  - Political crisis in Peru
- Africa
  - Political crisis in Morocco
- Oceania
  - Philippines-China dispute; military operations against ISIS

Vertical Analysis

- Online services and technology the most-targeted verticals in 2017

Malware Analysis

Overview

Malicious software, or malware, refers to computer code that can be harmful to both computer systems and their users. Malware comes in different forms, including executable code, scripts, active web content, and more. It can be a typical computer file or even "file-less" — resident only in memory. Even well-known computer software bought in a legitimate store can have hidden, undesirable functionality, and be considered malware. Thus, malware is best defined by its harmful intent and behavior.

Figure 1, below, shows the malware types that Comodo security software detected and classified in 2017.

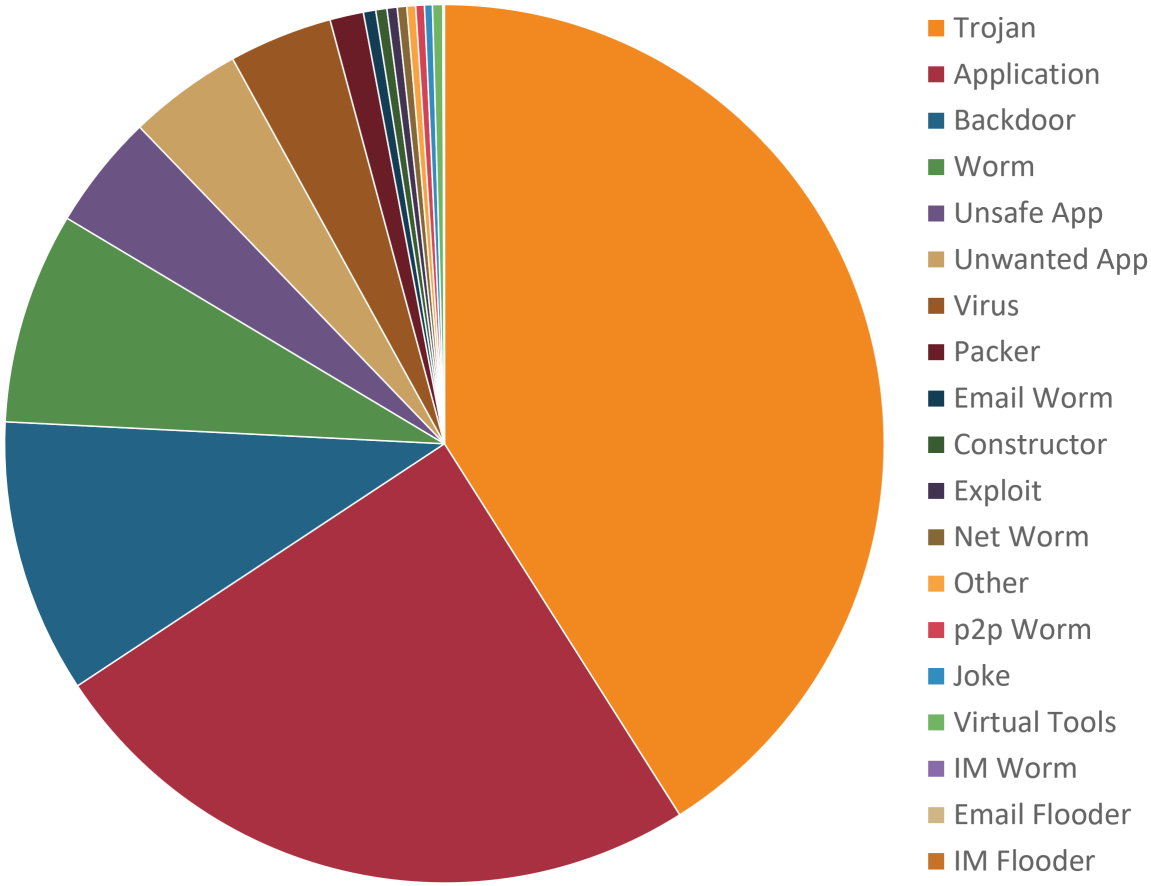

Figure 1: Malware Types

Trojans dominated the malware landscape with 41.0% of Comodo detections. Applications exhibiting malicious, unsafe, or undesirable behavior came in second place at 24.7%. And backdoors were the third-most detected form of malware at 10.1%. The top eight malware types seen above are addressed in greater detail, in their own individual sections, below.

Within these malware types, there exist thousands of individual malware families. And within each type and family, there can be significant overlap in appearance and functionality.

Figure 2, below, shows the wide range of malware families that Comodo detected in 2017.

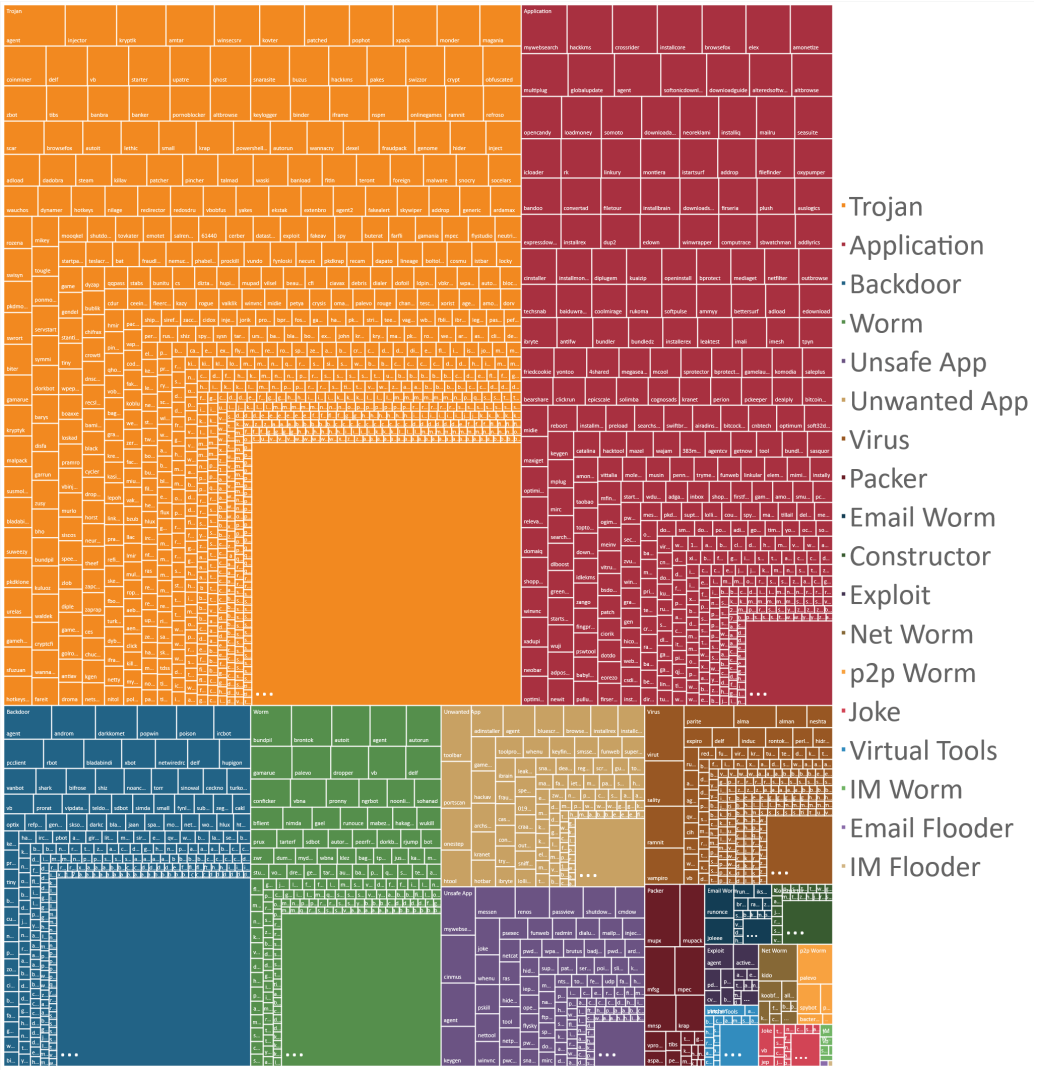

Figure 2: Malware Types and Individual Families

The array of complexity here is astonishing. For example, in 2017, Comodo detected 3,704 unique trojan families, 708 unique application malware families, and 1,621 unique backdoor families. The challenge of cybersecurity grows even more complicated when you consider the international architecture of the internet. Hackers take advantage of limited political and legal jurisdictions to attack vulnerable systems anywhere in the world, creating headaches for both network security and law enforcement personnel.

Figure 3, below, shows the countries in which Comodo security software detected malware in 2017.

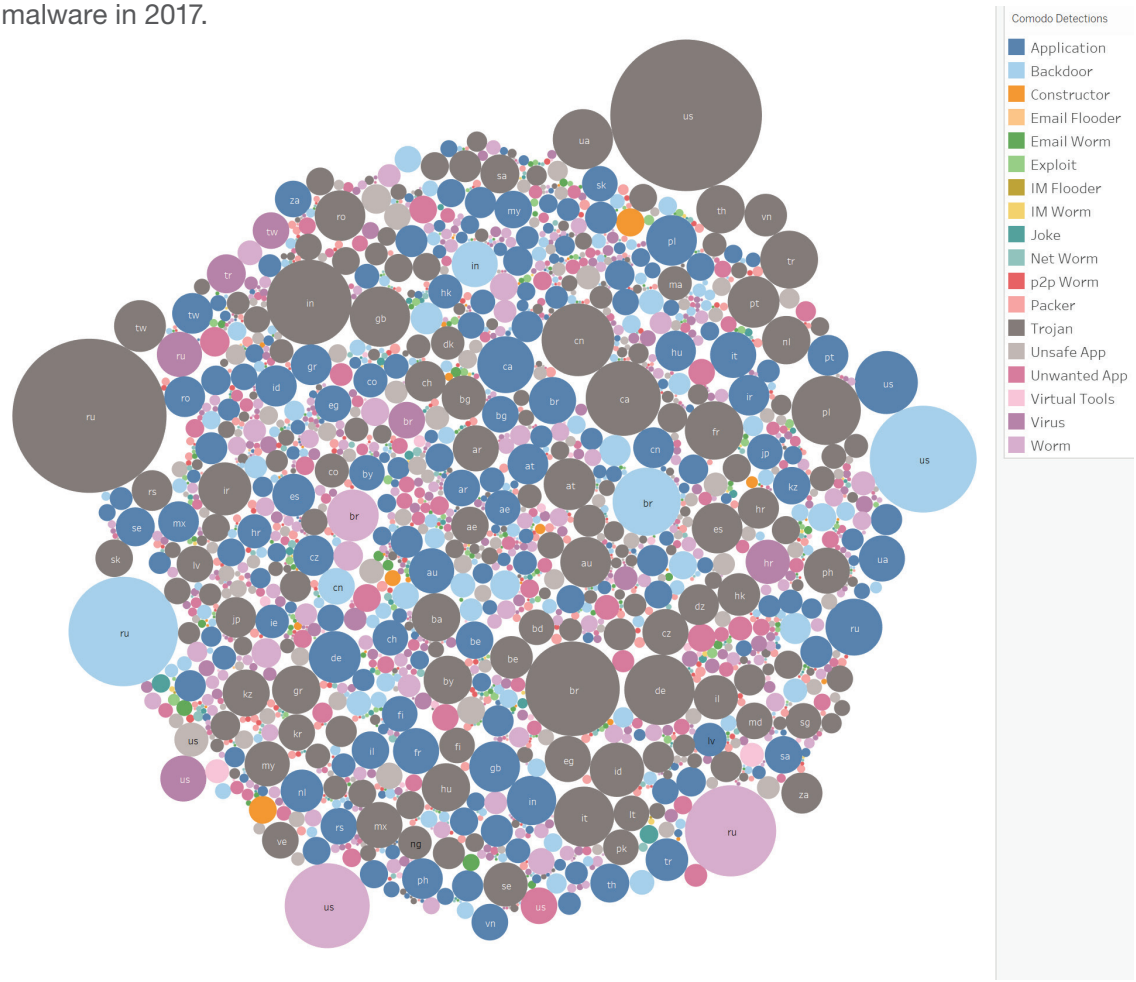

Figure 3: Malware Detection by Country of Detection

Russia and the U.S. clearly stand out in this chart as home not only to large human and computer populations, but also as home to the most malware. Russia saw 8.8% of detections, and the U.S. 8.6%. Rounding out the top 10 were Brazil, India, Canada, Germany, China, Poland, Turkey, the UK, and Ukraine.

1 | Trojan

Trojan horse malware takes its name from Greek mythology and refers to any seemingly useful or benign computer program that has hidden (usually malicious) functionality that can steal, block, or manipulate data on a victim computer. Attackers use numerous tricks to get users to install a trojan on their computer, from phishing to malicious advertising.

Figure 4, below, shows the 225 countries in which Comodo detected trojan malware in 2017.

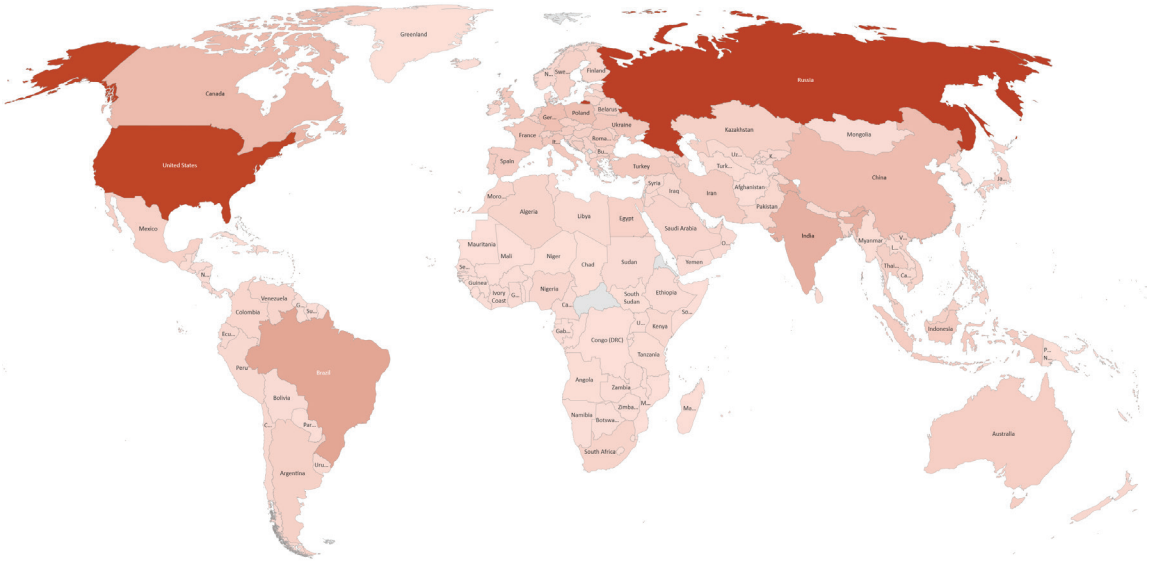

Figure 4: Malware Detection by Country of Detection

Top 10 Countries of Trojan Detection:

Russia	9.7%
U.S.	9.3%
Brazil	3.6%
India	2.9%
Canada	2.3%
China	2.2%
Germany	2.0%
Poland	2.0%
Italy	1.5%
Ukraine	1.5%

Here are Comodo's trojan detections for Q4 2017, paired with the country of detection.

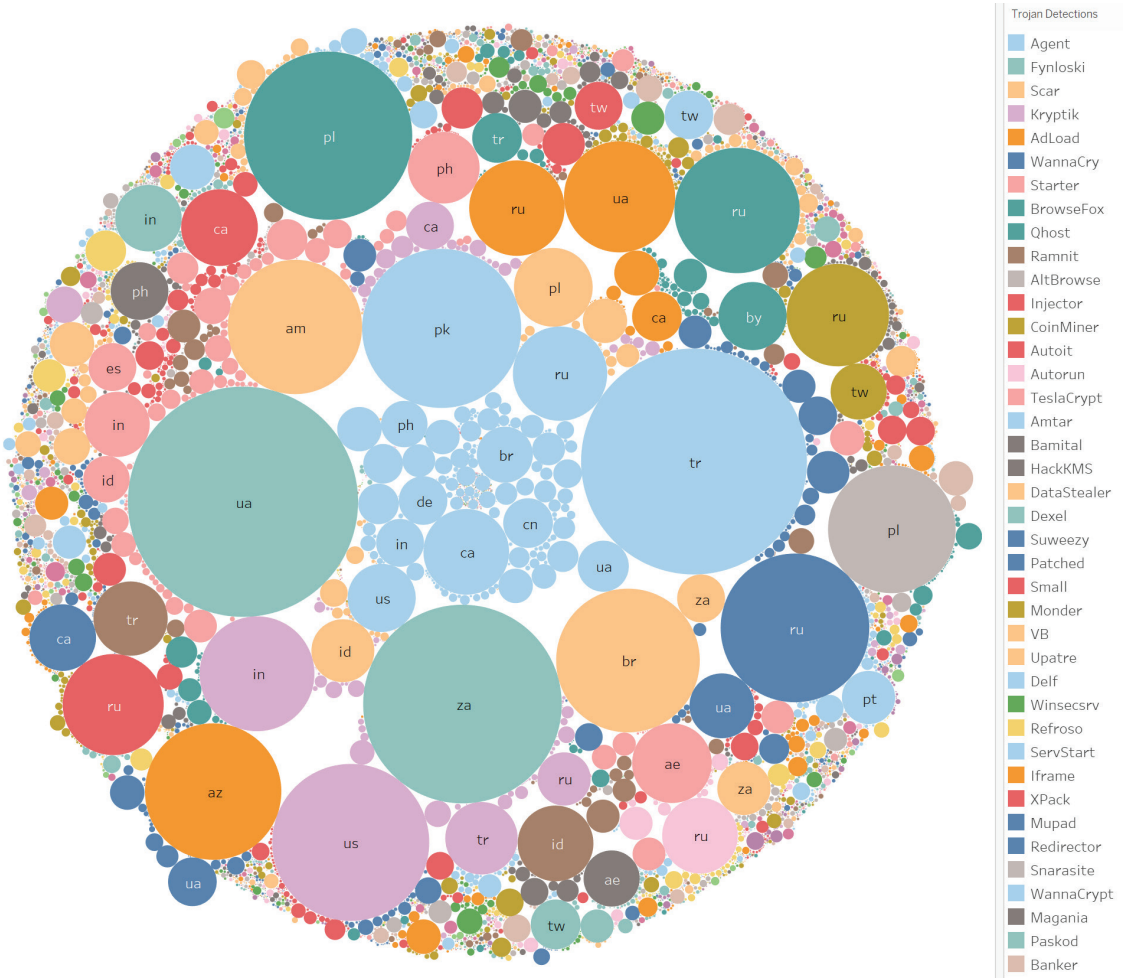

Figure 5: Trojan Families and Countries of Detection

The most common trojan detected in Q4 2017 was "Agent," representing a generic malware family that is difficult to characterize more precisely, and it was detected most often in Turkey (.tr), Pakistan (.pk), and Russia (.ru). In second place was Fynloski, a serious remote access tool (RAT) for Windows that plagued Ukraine (.ua) and South Africa (.za). And third, the banking trojan Scar was seen most often in Brazil (.br), Armenia (.am), and Poland (.pl).

Now let's look ahead to 2018. Malware is a highly dynamic phenomenon, and cybersecurity has always been hard to predict, but that shouldn't stop us from trying to see how vulnerabilities and exploits are evolving and where the bad guys might go next. It will be interesting to see whether and how these trends continue into 2018, especially since the end of a calendar year is filled with holidays and even cybercriminals and spies might decide to take a vacation.

These sections will only make use of simple linear timelines. As Comodo analysis progresses in 2018, we will experiment with more data and new methods in order to see which works best.

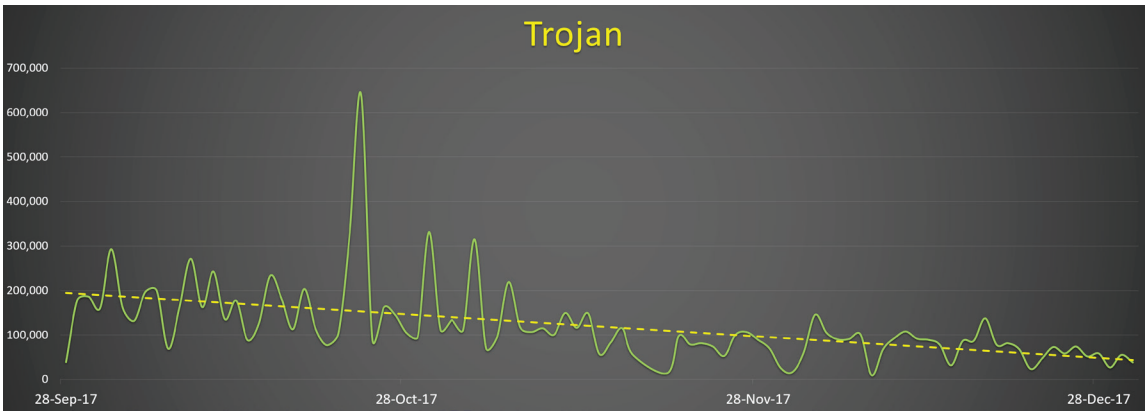

Figure 6: Trojan Detection Timeline

In this trojan timeline from Q4 2017, there is a clear downturn in detections, even taking into account the dramatic rise in October trojan discoveries. In our Q1 2018 report, our best guess is that trojan detections will make a rebound, but we'll let you know for sure at RSA 2018.

2 | Application

Malicious — and merely suspicious — applications occupy a dangerous position in the malware landscape because we often intend to download and use such software. Comodo frequently flags them due to the fact that they exhibit behavior that users may be unaware of and would comfortable with if they were to discover them. This category often includes commercial monitoring applications such as keyloggers that typically have functionality that is invisible to the user and hidden from the operating system. Sometimes, such applications are freeware or subscription software and often purport to help the user or computer when, in fact, they are malicious.

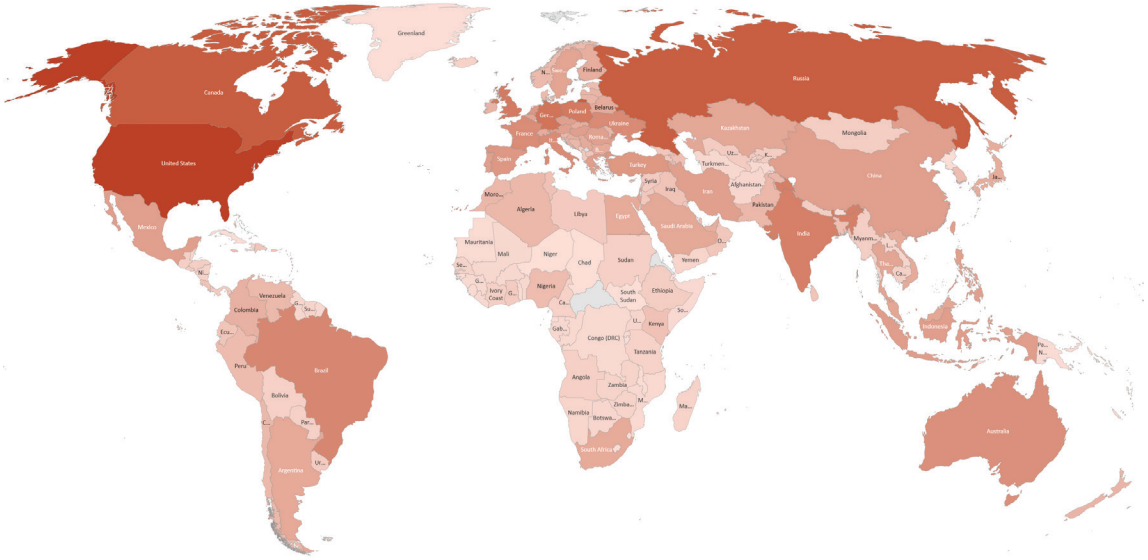

Figure 7: Application Malware

Comodo detected malicious or suspicious applications in 226 countries, as seen in Figure 7. Compared with trojans, there is a much more even distribution across the planet.

Top 10 Countries of Application Detection:

U.S.	2.7%
Canada	2.2%
Russia	2.2%
Germany	1.8%
Poland	1.7%
UK	1.7%
India	1.6%
Brazil	1.5%
Ukraine	1.4%
Italy	1.4%

Here are Comodo's application detections for Q4 2017, with application families paired with the country of detection.

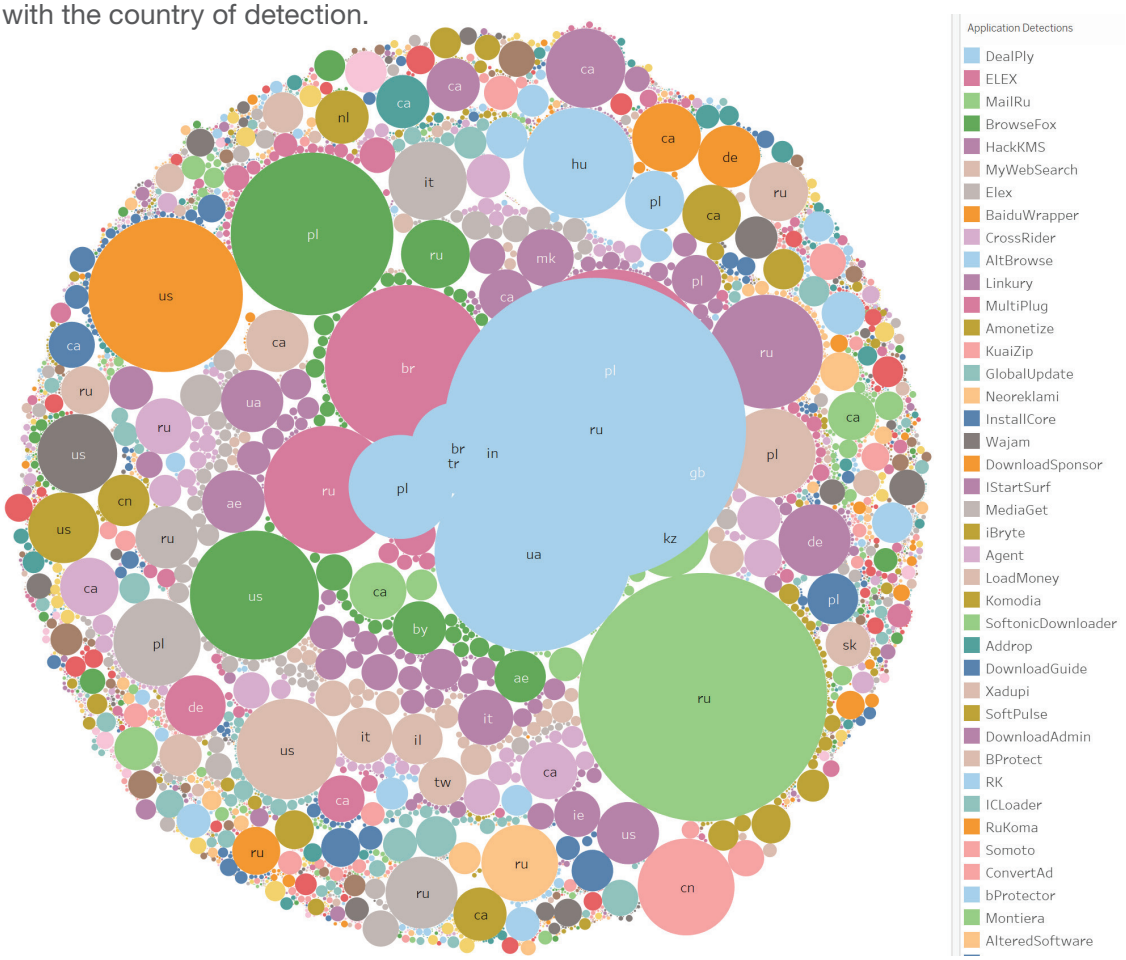

Figure 8: Application Families and Countries of Detection

For Q4 2017, the adware program DealPly came in first place, affecting, in particular, the Former Soviet Union and Eastern Europe. Second, ELEX, often bundled with other junk downloads, victimized Brazil (.br), Poland (.pl), and Russia (.ru). Third, MailRu was common throughout Russia. And fourth, BrowseFox was discovered around the world, from the U.S. to Poland, Russia, Belarus (.by), and the United Arab Emirates (.ae).

The relatively even distribution of application malware around the world should mean that the detection rate would remain fairly even, and that is exactly what we saw in Q4 2017. In the chart below, application detections appear somewhat erratic, but the trendline clearly shows only a minor drop-off over time.

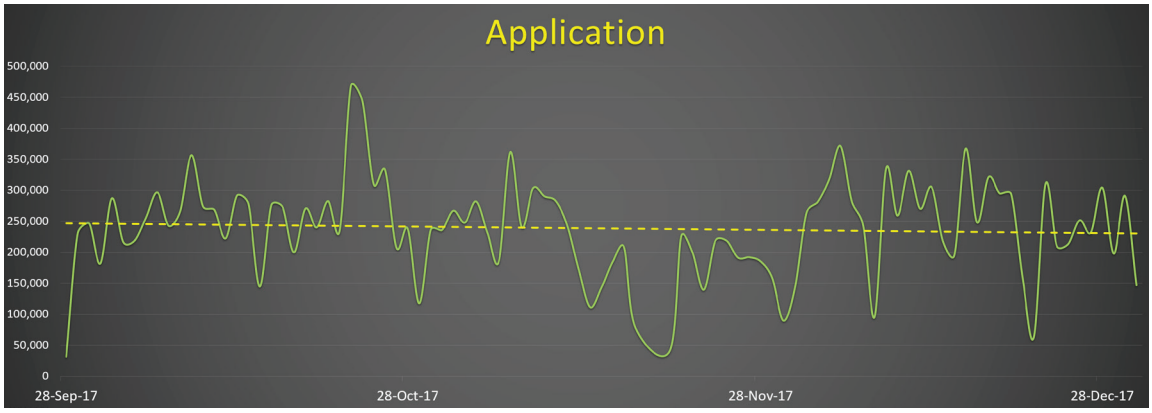

Figure 9: Application Detection Timeline

Comodo expects that the even keel might continue into 2018, as the wide range of countries by detection will make this forecast easier to predict.

3 | Backdoor

A backdoor is a hidden way to bypass normal user authentication to gain covert, remote access to a computer system, cryptosystem, or algorithm. Backdoors can be a part of installed programs as well as modifications to existing programs. Thus, they can have legitimate, administrative use, or can be secretly installed with the aid of other malicious software such as a rootkit.

Comodo detected backdoors within 184 countries, as shown in Figure 10, below.

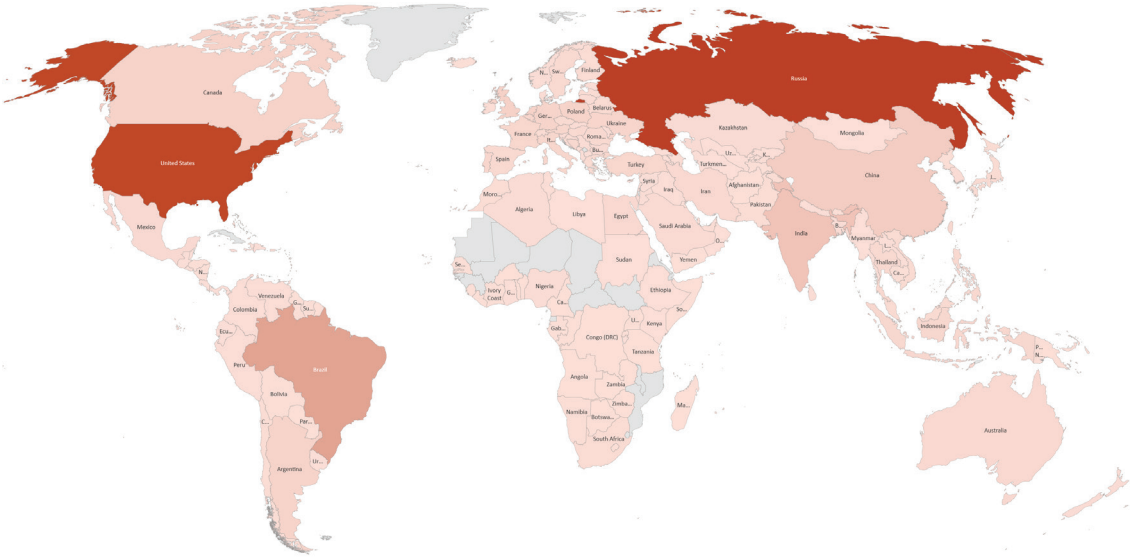

Figure 10: Backdoors Detected in 2017

In general, we can say that backdoors are a higher class of malware, often used in targeted operations for a high return on investment. The map reflects that fact nicely, including a potential geopolitical rationale, with Russia and the U.S. dominating the backdoor landscape in 2017.

Top 10 Countries of Backdoor Detection:

Russia	19.7%
U.S.	18.8%
Brazil	7.6%
India	3.5%
China	2.2%
UK	1.7%
Canada	1.6%
Netherlands	1.5%
Argentina	1.5%
Poland	1.4%

Here are Comodo's backdoor detections for Q4 2017, with backdoor families paired with the country of detection.

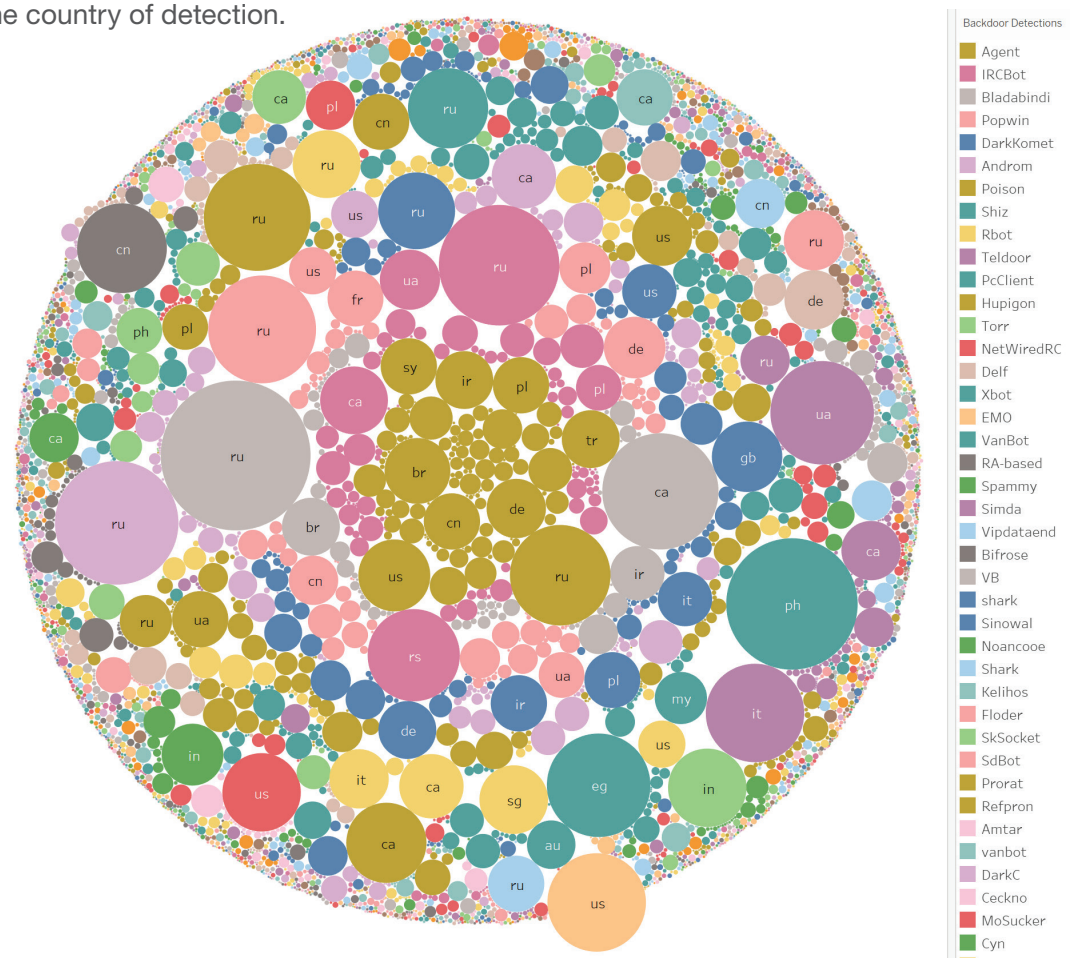

Figure 11: Backdoor Families and Countries of Detection

In Q4 2017, Russia clearly suffered the most from malicious backdoors, in particular from Bladabindi, Androm, and IRCBot. The Philippines (.ph) was plagued by the banking trojan Shiz. Canada suffered from Bladabindi. Ukraine (.ua) had Teldoor. In the U.S., Comodo detected EMO and NetWiredRC as the top two backdoors.

If there are any country and family pairings that you are interested in seeing, please email: **malwaresubmit@avlab.comodo.com**

In this analysis, backdoor malware was our only category in which the volume of detections clearly rose during Q4 2017. Given the high concentration of backdoors within the U.S. and Russia, it however is possible that the trend will be reversed in the future. However, Comodo predicts that backdoor detection rates will continue to rise in Q1 2018 vis-à-vis other malware types.

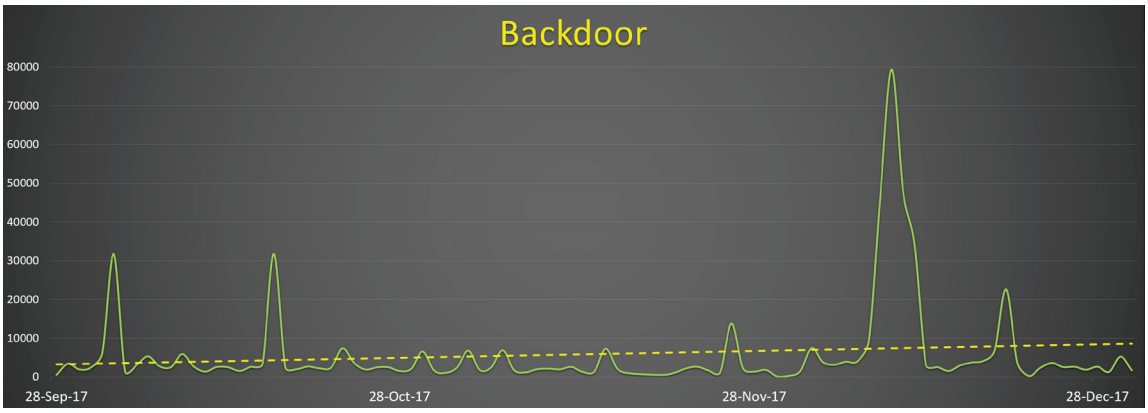

Figure 12: Backdoor Detection Timeline

Over time, as enterprises hire and retain more professional cybersecurity staff, their exposure to vulnerabilities associated with common viruses and worms might decrease, and we might see an offsetting rise in backdoor, trojan, and packer detections. We'll keep an eye on these trends and let you know how this ratio evolves in 2018.

4 | Worm

A computer worm is similar to a virus but travels the internet autonomously, exploiting vulnerabilities in network defenses as it spreads from network to network and computer to computer. The goal of a worm is to deliver a malicious payload to a target machine, which can then lead, for example, 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.

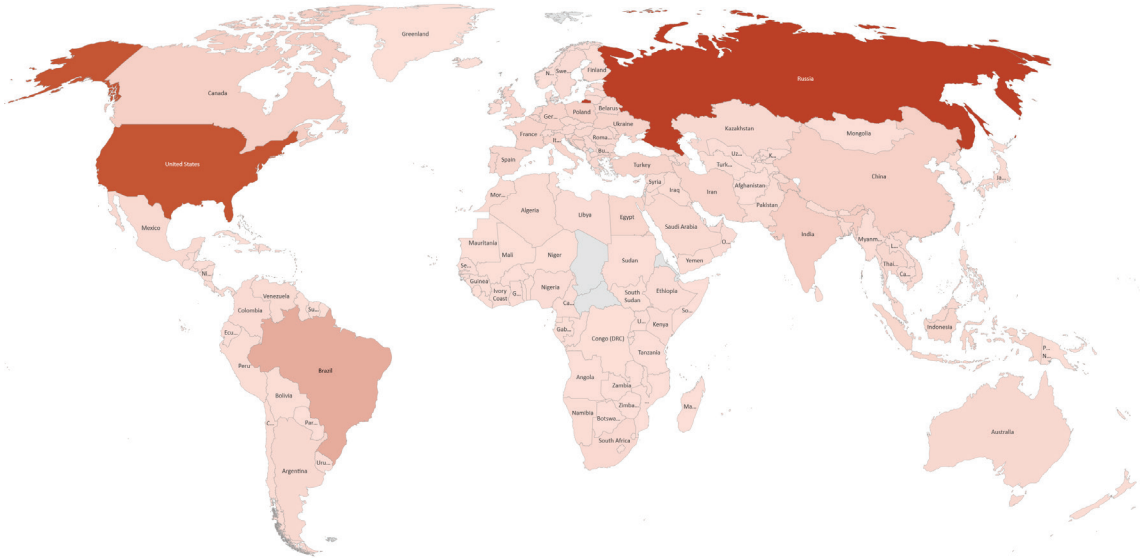

Figure 13: Computer Worms Detected in 2017

In 2017, Comodo detected computer worms within 200 countries, which are displayed in Figure 13.

Again, Russia and the U.S. are the clear frontrunners in this malware category, followed by Brazil with India a distant fourth.

Top 10 Countries of Worm Detection:

Russia	17.8%
U.S.	15.5%
Brazil	5.9%
India	1.9%
Canada	1.8%
China	1.7%
Croatia	1.6%
Poland	1.4%
Turkey	1.3%
Ukraine	1.2%

Here are Comodo's worm detections for Q4 2017, with worm families paired with the country of detection.

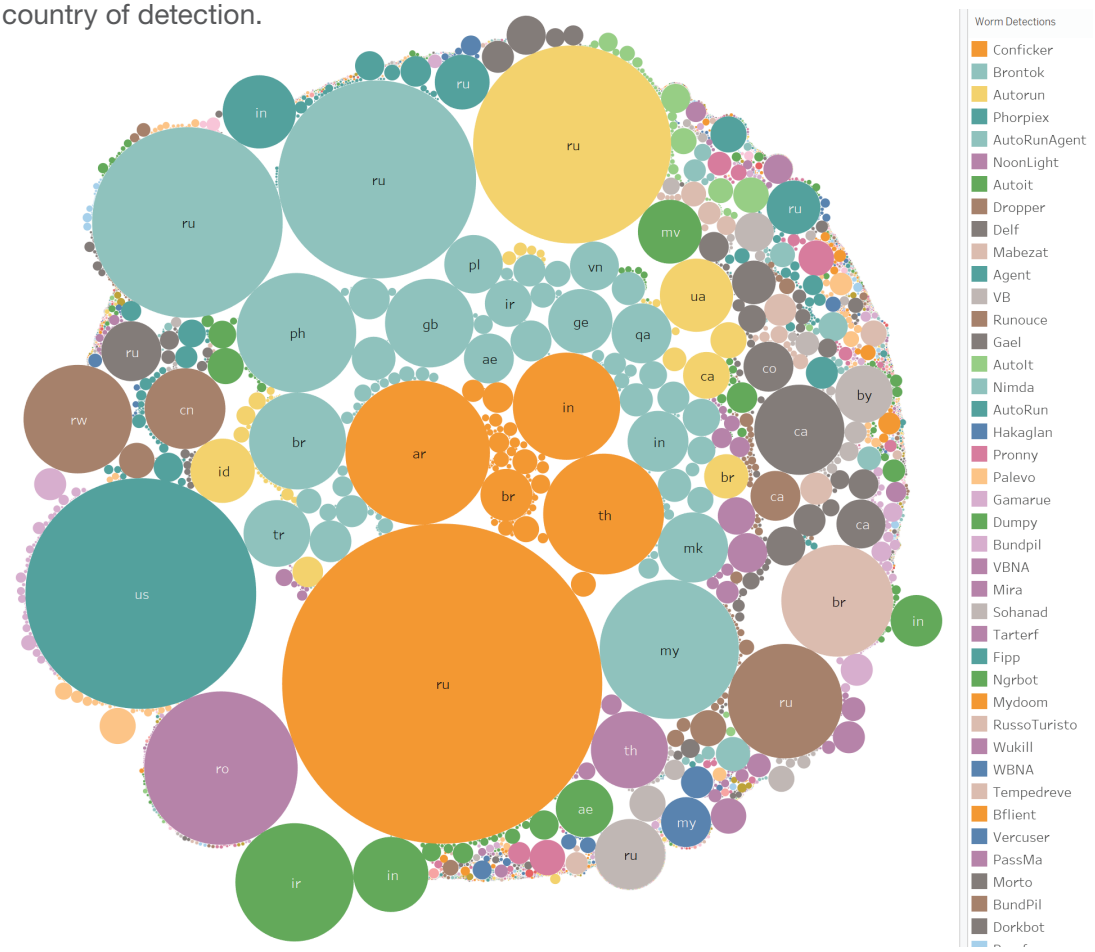

Figure 14: Worm Families and Countries of Detection

In this chart, Russia stands out as having a severe problem with computer worms. In Q4 2017, Russia's most prevalent worm was the notorious Conficker, which has been around since at least 2008, and has propagated via botnets to claim millions of computers around the world. In the U.S., the biggest outbreak was Phorpiex, an outbreak that was detected in the state of Florida. After Conficker, the most common worm detected across the internet was Brontok, an email-based worm that in the past has been used for hacktivist denial-of-service attacks.

In the chart below, worms trended down in Q3 2017, as you can see with the wave crests less frequent and the troughs longer. This could be good news in that network defenders were able to defend networks more effectively or the power of computer worms was more ephemeral — or both.

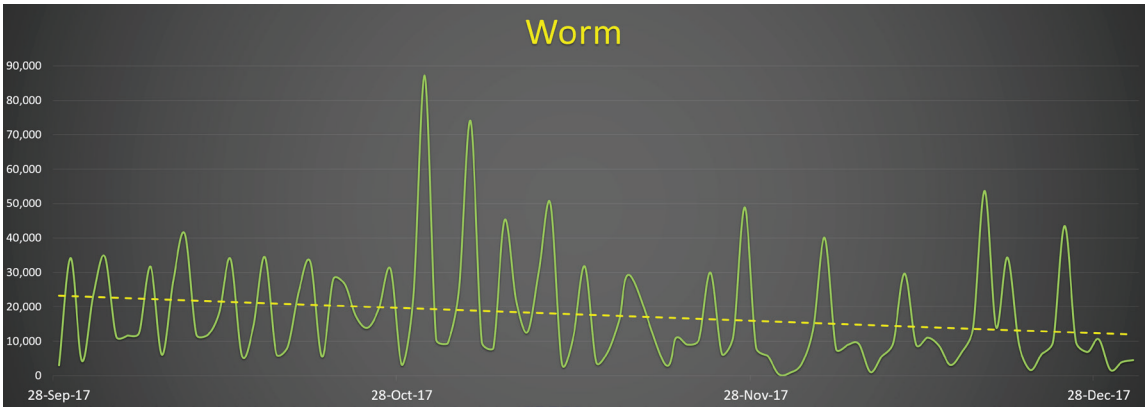

Figure 15: Worm Detection Timeline

This will be a fascinating trend to watch in 2018. There is no guarantee that computer worms will pose a less serious threat to computer networks. In general, worms are used to deliver a malicious payload that might include a trojan or a backdoor. Thus, they are a precursor to other kinds of malicious activity, so we'll have to see whether other malware categories experience a subsequent downturn.

5 | Unsafe Application

Unsafe applications are seemingly legitimate programs, but in fact they are frequently abused by coders and hackers with malicious intent. Often, they claim to help users with administrative or security functionality — but do the opposite. Fake anti-virus, free Internet Relay Chat (IRC) clients, and keyloggers are some prominent examples.

In Figure 16, below, you can see the 183 countries in which Comodo detected unsafe applications.

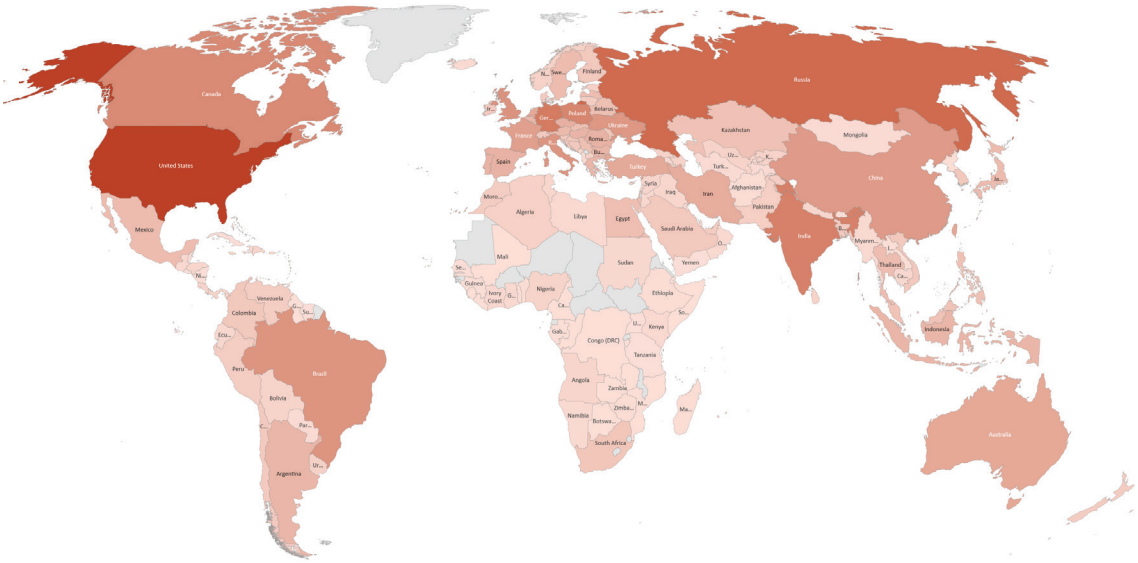

Figure 16: Unsafe Applications Detected in 2017

While the U.S. came in first place, there is a fairly even distribution around the world, which means that on a per capita basis, those countries in the top 10 have less of a problem with unsafe applications than many other countries.

Top 10 Countries of Unsafe Application Detection:

U.S.	4.6%
Russia	3.4%
Germany	2.9%
India	2.7%
Poland	2.6%
Canada	2.5%
UK	2.3%
Brazil	2.2%
Italy	2.2%
Ukraine	2.1%

Here are Comodo's unsafe application detections for Q4 2017, with their families paired with the country of detection.

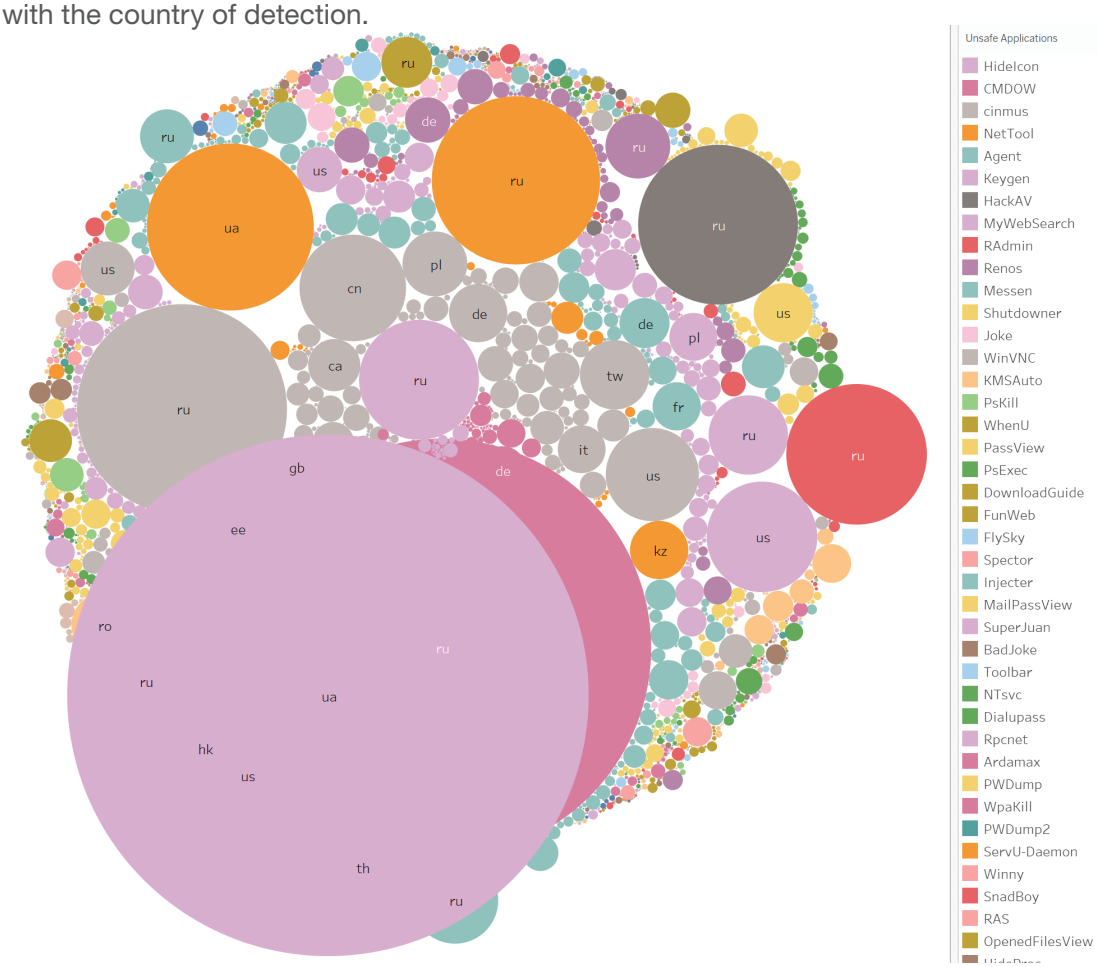

Figure 17: Unsafe Application Families and Countries of Detection

In this chart, we can see that Ukraine and Russia were home to the largest detections of unsafe applications in Q4 2017. Ukraine (.ua) experienced a massive outbreak of the HideIcon malware that originally propagated via the Google Play store in 2015. However, the challenge that Russia has in overcoming unsafe applications is far greater: CMDOW, Cinmus, NetTool, HackAV, and RAdmin all constituted serious outbreaks. In the U.S., the most frequent detections were MyWebSearch and Cinmus.

As seen in the previous chart, unsafe applications appear liable to wild swings of use and detection. For example, Ukraine was only at #10 over the course of 2017 but experienced a huge spike in Q4. Thus, we see in the trendline below that there was a huge decline in unsafe application detections toward the end of the year. Therefore, there is probably at least an even chance that we'll see a sharp rise at the beginning of 2018 when cybercriminals and spies figure out how to hoodwink network security staff again.

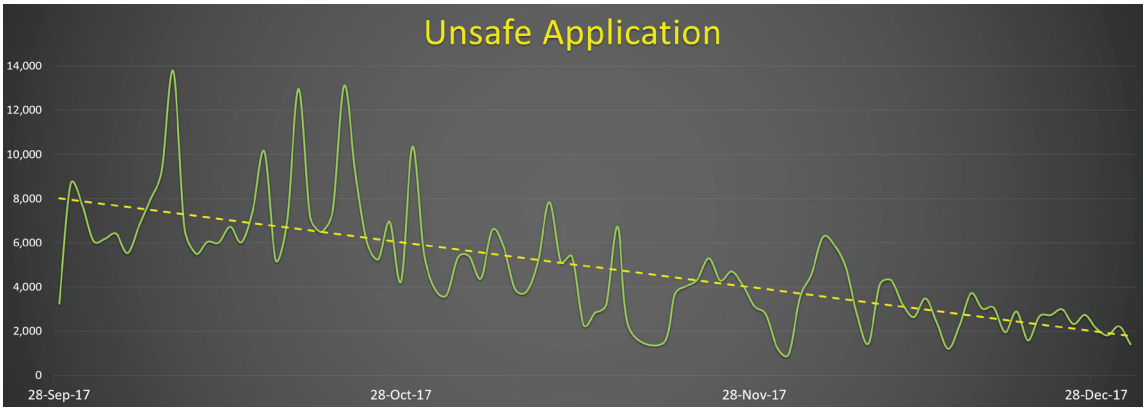

Figure 18: Unsafe Application Detection Timeline

Such dramatic behavior will be interesting to watch, and in our Q1 2018 Report, to be released at RSA in April, we will let you know what happens.

6 | Unwanted Application

The unwanted application malware category is alarming in that, during the course of common computer and internet activity, users often inadvertently install these applications. For example, they include common adware programs, widely disseminated images, videos, dialers, jokes, gossip, and more. However, it is important to know that these kinds of programs can also contain hidden malicious functionality that can allow attackers to steal, block, and/or manipulate your data.

In Figure 19, below, you can see the 184 countries in which Comodo detected unwanted applications.

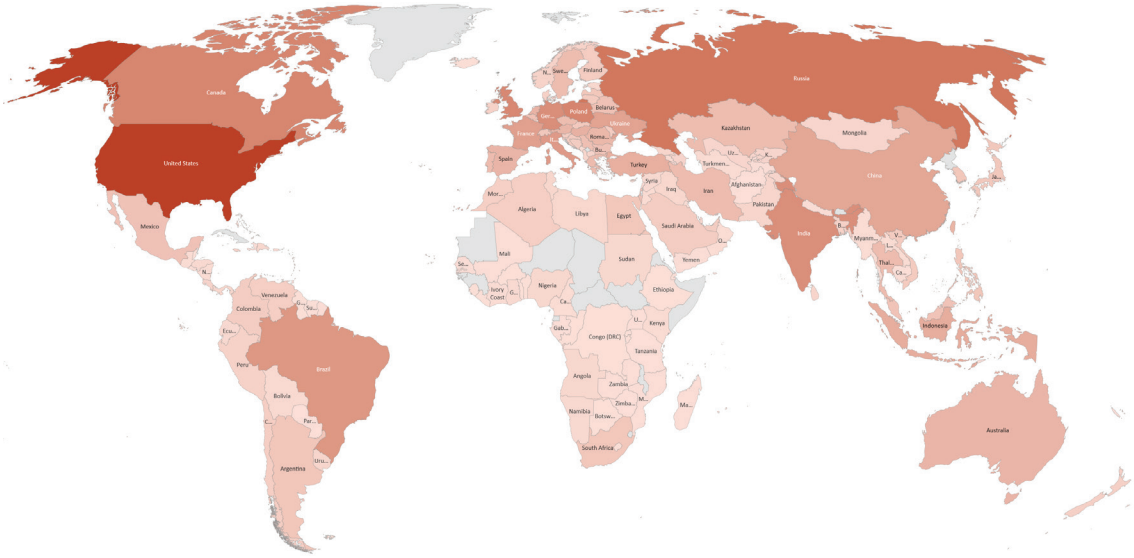

Figure 19: Unwanted Applications Detected in 2017

The U.S. was tops in this category, but overall the distribution was fairly widespread across the planet.

Top 10 Countries of Unwanted Application Detection:

U.S.	5.2%
Russia	3.5%
Poland	3.0%
Canada	3.0%
UK	2.9%
Germany	2.7%
India	2.7%
Brazil	2.5%
Italy	2.3%
France	2.2%

Here are Comodo's unwanted application detections for Q4 2017, paired with the country of detection.

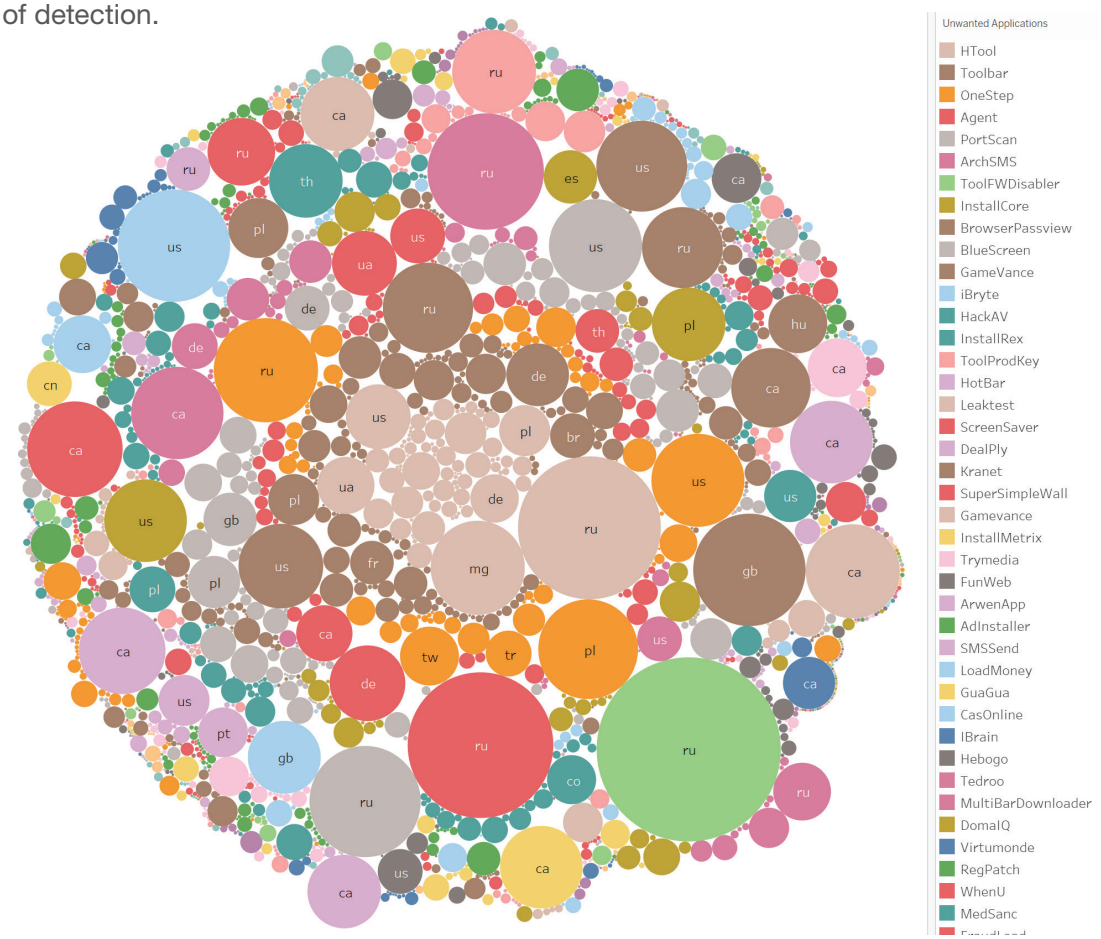

Figure 20: Unwanted Application Families and Countries of Detection

This chart shows that unwanted applications are more evenly distributed between countries. For example, Russia and the U.S. were the two top countries of detection, but none of their top five unwanted applications were the same. Unlike most of the other charts, there is no strong central cluster, and the top families, including Htool, Toolbar, OneStep, Agent, and Portscan, are detected almost everywhere.

The distribution chart above is clearly less concentrated than the unsafe applications above. Therefore, it is unsurprising that we see a greater consistency in the Q4 2017 timeline. Thus, for cybercriminals and spies, this is a more reliable malware type, while at the same time constituting a more vexing problem for cyber defenders.

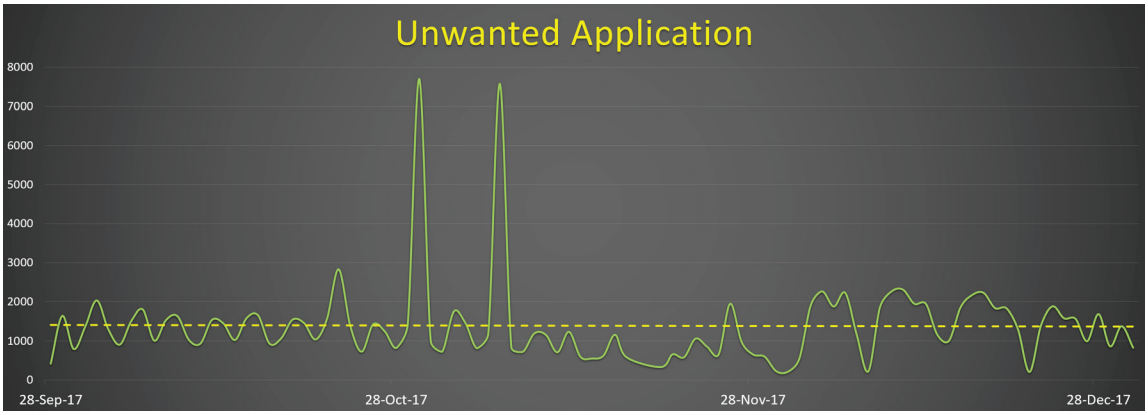

Figure 21: Unwanted Application Detection Timeline

There were two large spikes in October 2017, but apart from that, this malware type is internationally-based and should offer a steady flow of challenges for network security personnel.

7 | Virus

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.

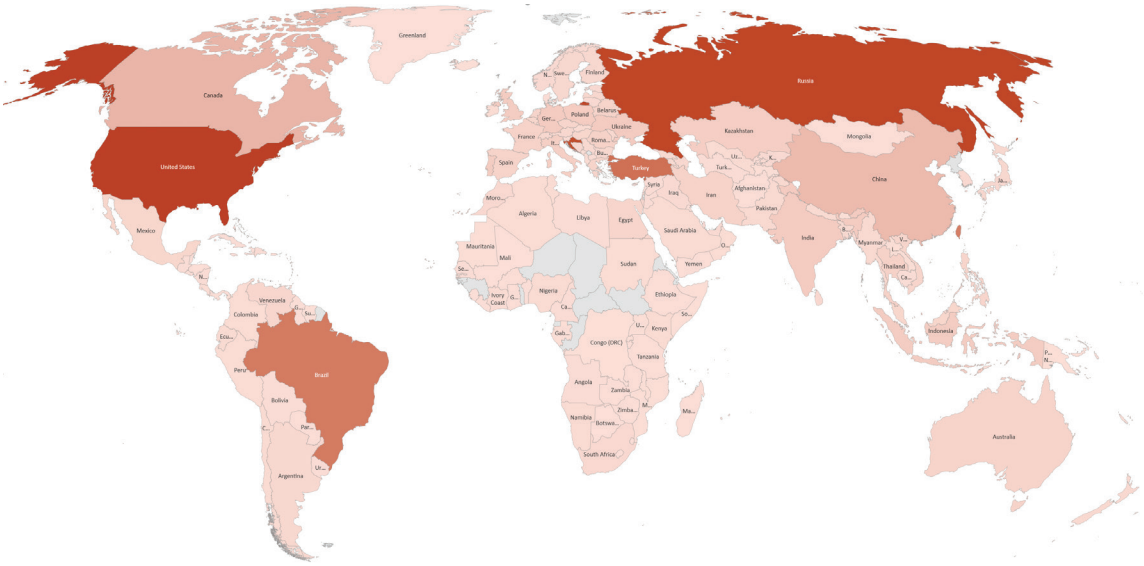

Figure 22: Computer Viruses Detected in 2017

Figure 22 displays the 190 countries where Comodo detected viruses in 2017.

Top 10 Countries of Virus Detection:

U.S.	9.3%
Russia	9.0%
Croatia	8.6%
Turkey	6.7%
Brazil	6.0%
Taiwan	5.8%
Canada	2.5%
China	2.2%
Germany	1.2%
India	1.2%

Here are Comodo's virus detections for Q4 2017, with virus families paired with the country of detection.

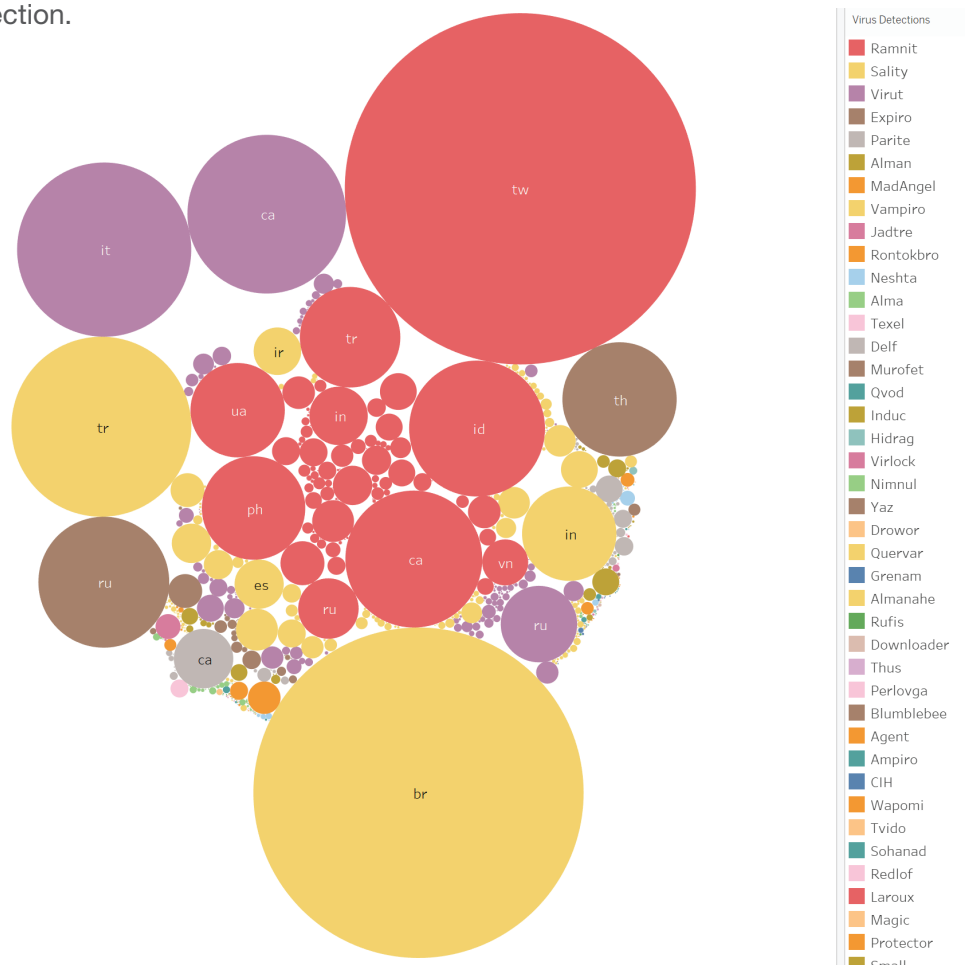

Figure 23: Virus Families and Countries of Detection

This one is easy. Computer viruses, while still dangerous, are overall a simpler data set to analyze. The top virus family was Ramnit, which has been around since at least 2011, has targeted banking credentials in the past, and was the focus of international law enforcement actions in 2015. In Q4 2017, Comodo detected it mostly in Taiwan (.tw), with Canada (.ca), Indonesia (.id), and the Philippines (.ph) also affected. In second place was Sality, which has been victimizing computers since at least 2003, and has evolved over many years to become one of the most complex cyberthreats, using peer-to-peer (P2P) networking for a wide range of tasks, including spam, hiding communications, exfiltrating data, and more.

This is an odd data set. Clearly, there are fascinating ups and downs. While the U.S. suffered the most over the course of 2017, it did not appear at all in our Q4 2017 virus chart. And while one would expect to find wild swings in detection rates, and that is true in the trendline, there is still an even trendline that should hearten criminals and worry network security personnel.

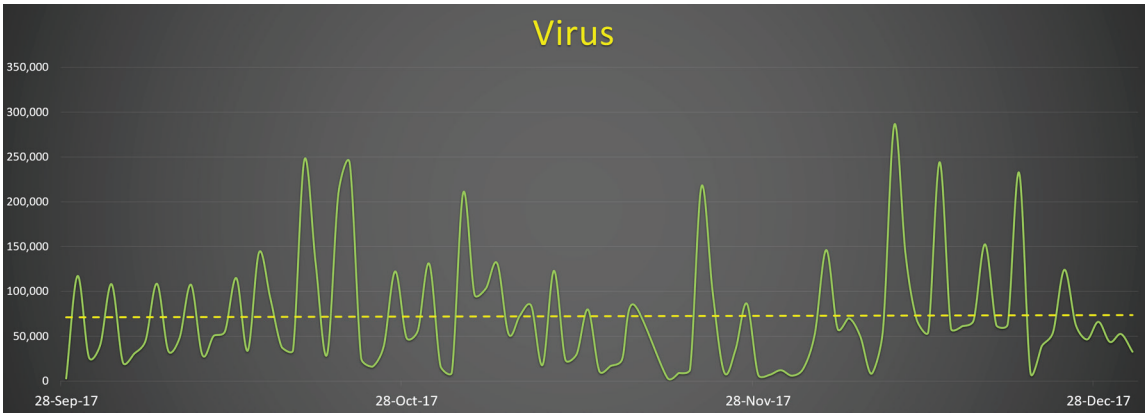

Figure 24: Virus Detection Timeline

We will continue to keep an eye on this one, and it will be interesting to see whether the strange behavior holds moving forward. We will let you know in our Q1 Report.

8 | Packer

Malware that is "packed" refers to any means used to hide or obfuscate malicious, executable code by compressing or "packing" it within larger, seemingly innocuous, data streams. The hostile code can even come in the form of scripts. The compressed data often contains separate decompression code, or even a self-extracting archive, which is used to recreate the original code from the compressed code and then execute the malware. Encryption may also be used to conceal the malware from security software as another means to obfuscate the attack.

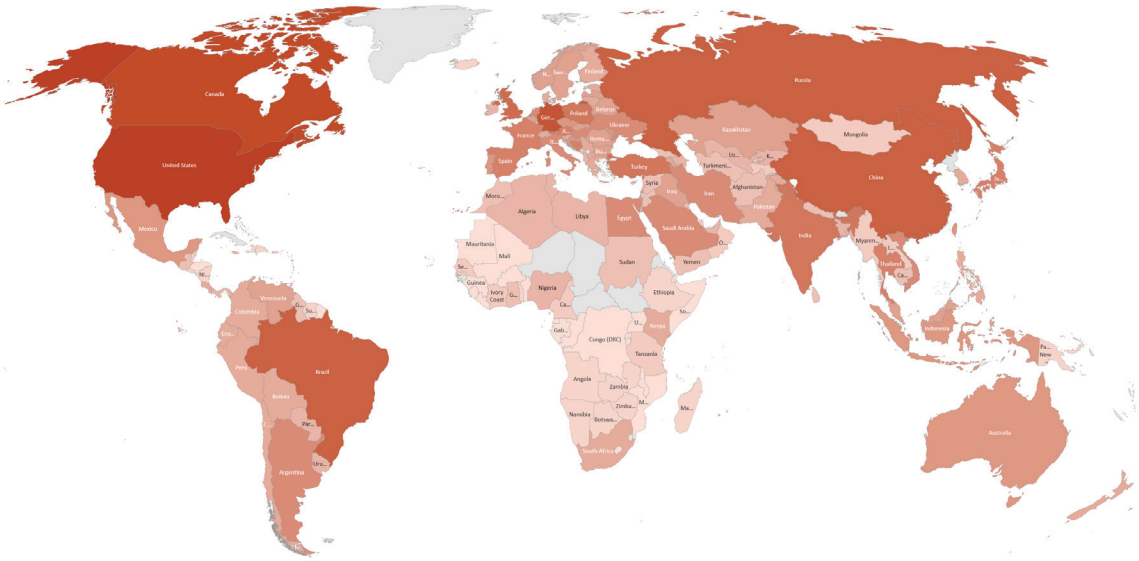

Figure 25: Packers Detected in 2017

Figure 25 shows the 189 countries where Comodo detected packers in 2017. While the U.S. came in first place, the distribution across the planet is very even, with China and India appearing in our top 10.

Top 10 Countries of Packer Detection:

U.S.	1.8%
Canada	1.7%
Germany	1.6%
Brazil	1.5%
China	1.5%
Russia	1.5%
UK	1.3%
India	1.2%
Poland	1.2%
Turkey	1.2%

Here are Comodo's packer detections for Q4 2017, with packer families paired with the country of detection.

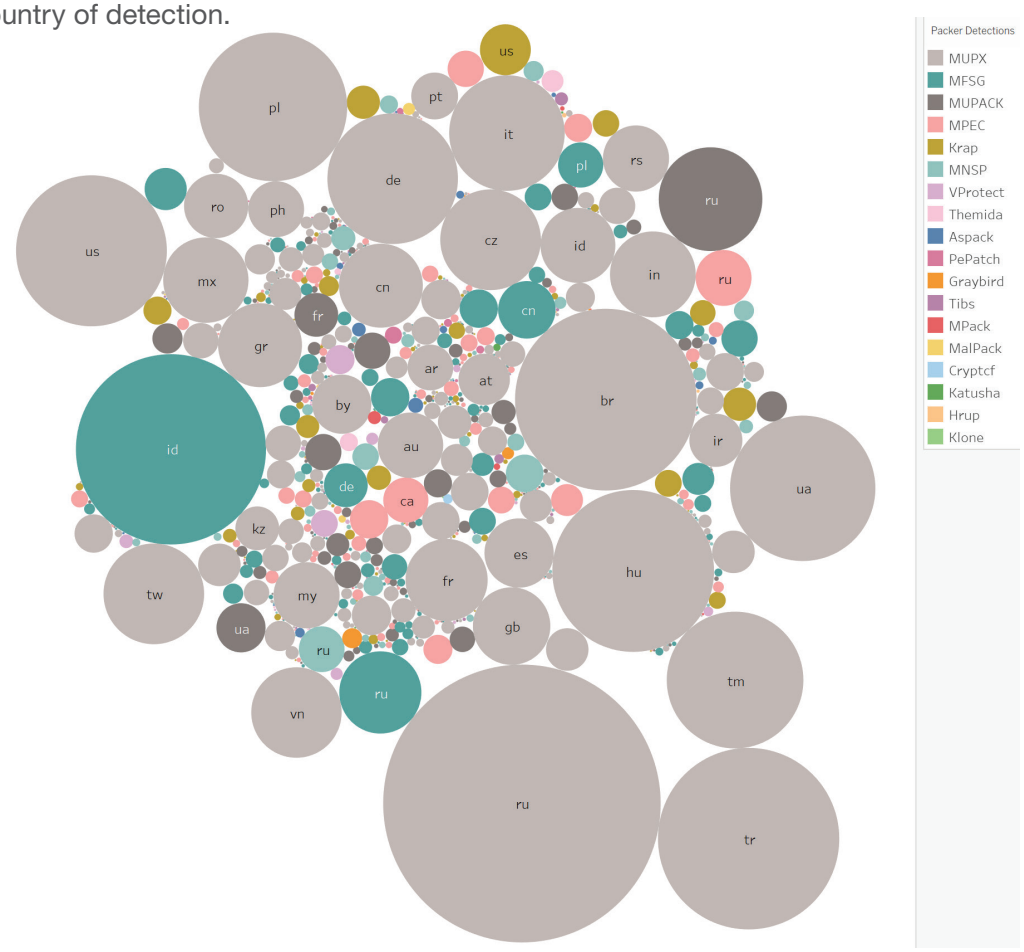

Figure 26: Packer Families and Countries of Detection

Finally, in packer, we have the easiest chart to analyze. There is one type of packer, MUPX, or the modified "Ultimate Packer for Executables," which dominates this malware terrain. MUPX refers to free, open source software that is compatible with numerous file formats and different operating systems. It 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. As shown in the chart, Comodo detected MUPX in Russia, Brazil, Turkey, Poland, the U.S., and Ukraine.

The detection rate for packers declined in Q4 2017, which is not what one might expect given its even distribution across the internet. However, this even distribution may be offset by the simpler dataset overall, which may make packers more susceptible to large-scale detection and mitigation.

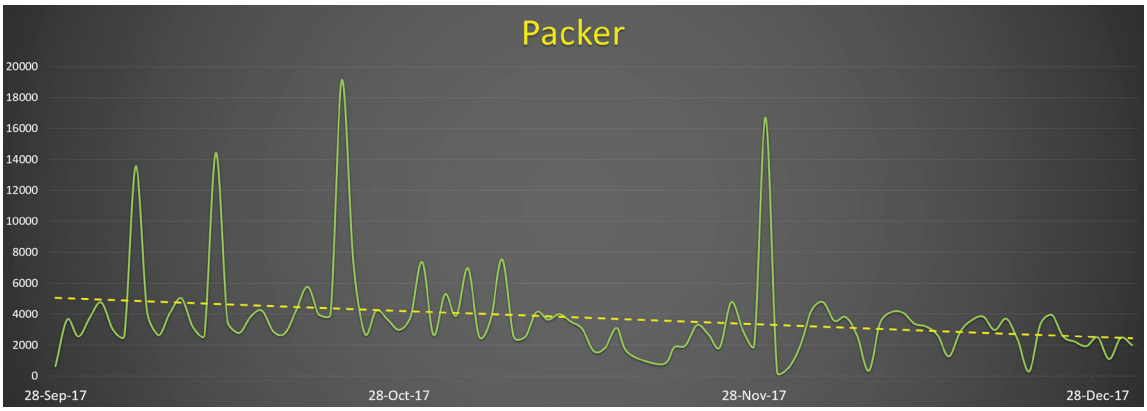

Figure 27: Packer Detection Timeline

Our best guess is that packers will make a rebound in early 2018, but we will certainly let you know in our Q1 2018 Report.

Global Analysis

1 | North America

This map shows the top malware types for North America in 2017, as well as the top three malware families within each type from Q4 2017 for a sample set of nations.

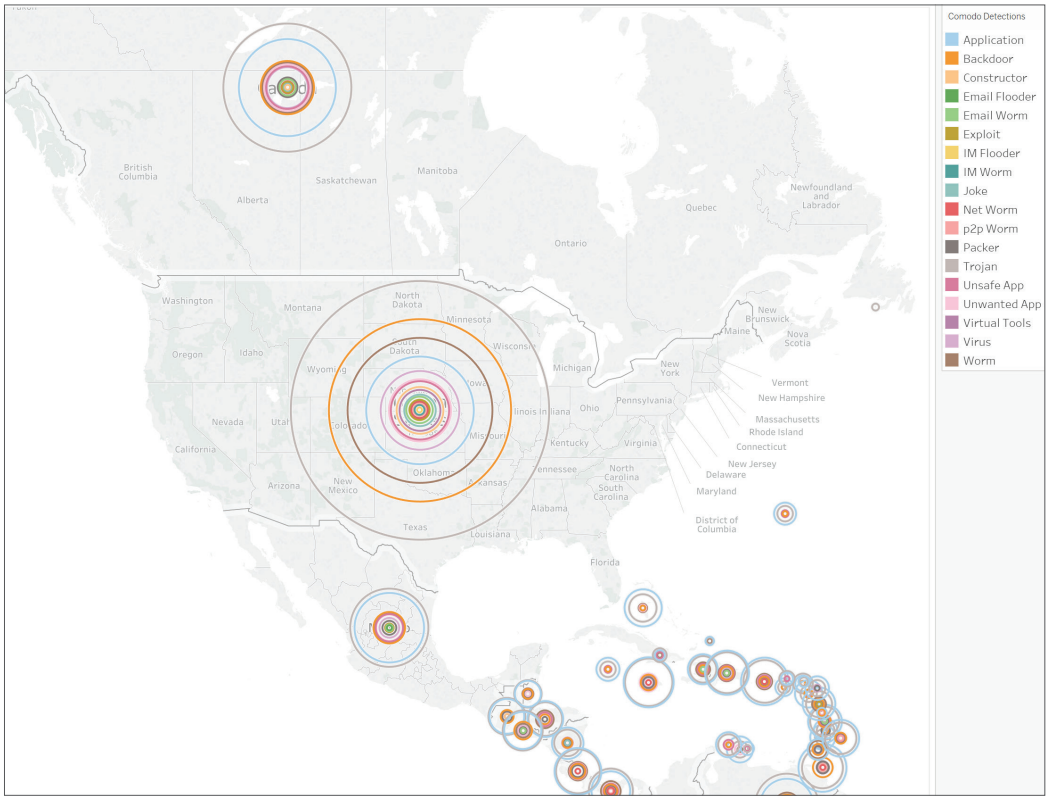

Figure 28: Malware Detections in North America

U.S.	Type: Trojan	Family: Kryptik
	Type: Backdoor	Family: EMO
	Type: Worm	Family: Phorpiex
Canada	Type: Trojan	Family: Injector
	Type: Application	Family: BrowseFox
	Type: Backdoor	Family: DarkKomet
Mexico	Type: Trojan	Family: Mikey
	Type: Application	Family: KuaiZip
	Type: Backdoor	Family: Poison

Potential Geopolitical Correlations

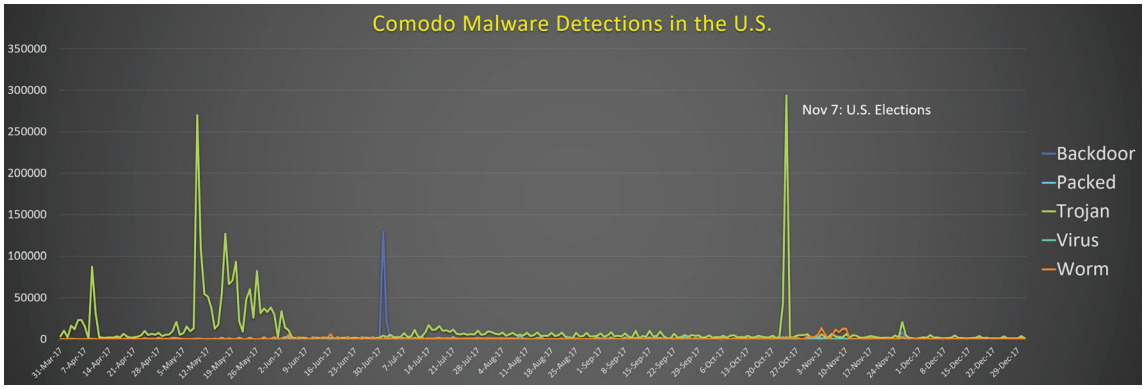

Figure 29: U.S.

In the internet era, all major real-world events have a reflection in cyberspace, often in the form of malware, which can be used to steal, block, or manipulate data in myriad unauthorized ways. Elections are a case in point: on Oct. 24, 2017, Comodo detected a massive spike in Kryptik trojans, over 94% of which were located in the state of Virginia, where a close and hard-fought gubernatorial election took place.

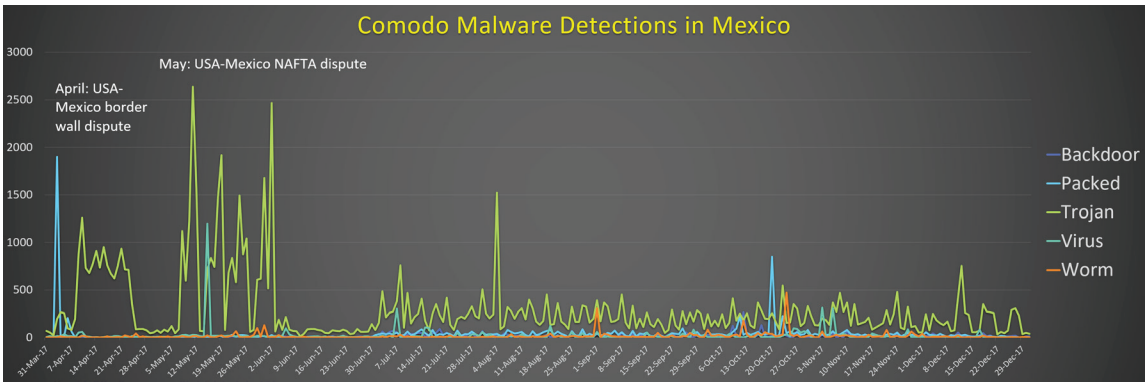

Figure 30: Mexico

In Mexico, there were at least two large waves of malware detections in 2017. It is possible, but by no means certain, that these high rates of detections were associated with, and perhaps driven by, concurrent international tension between the U.S. and Mexico.

2 | Europe

This map shows the top malware types for Europe in 2017, as well as the top three malware families within each type from Q4 2017 for a sample set of nations.

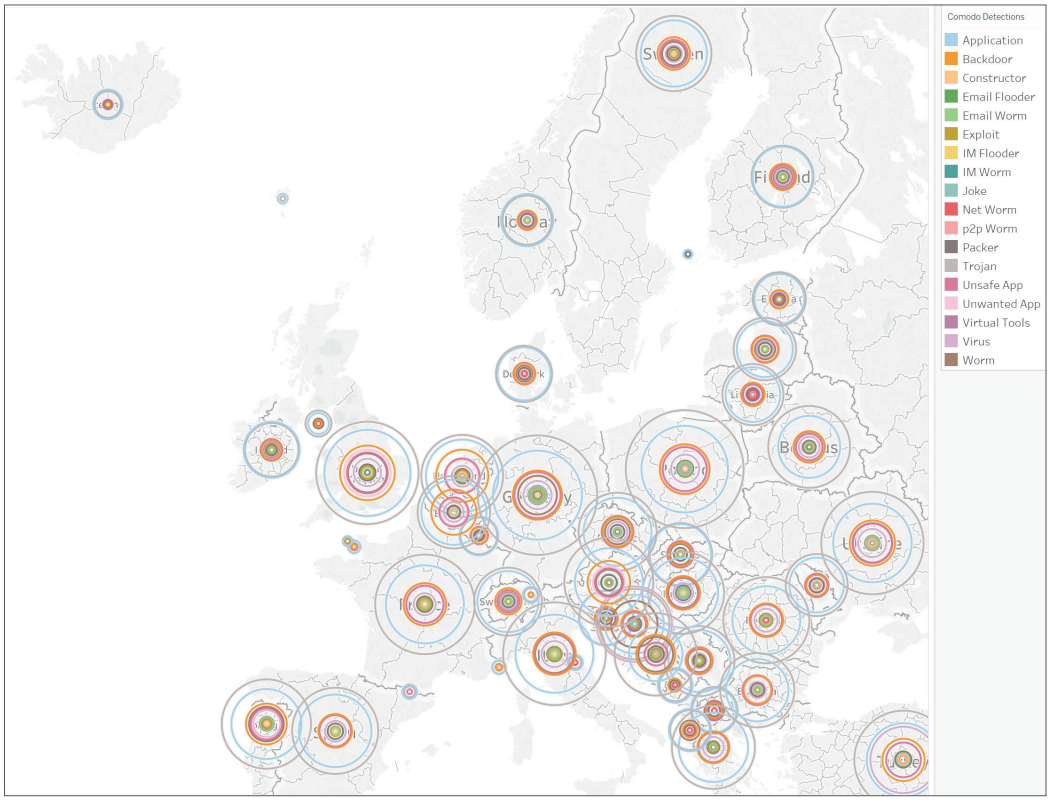

Figure 31: Malware Detections in Europe

Germany	Type: Trojan	Family: FakeAlert
	Type: Application	Family: Linkury
	Type: Backdoor	Family: Popwin
Italy	Type: Trojan	Family: TeslaCrypt
	Type: Application	Family: ELEX
	Type: Backdoor	Family: Teldoor
Poland	Type: Trojan	Family: BrowseFox
	Type: Application	Family: ELEX
	Type: Backdoor	Family: DarkKomet

Potential Geopolitical Correlations

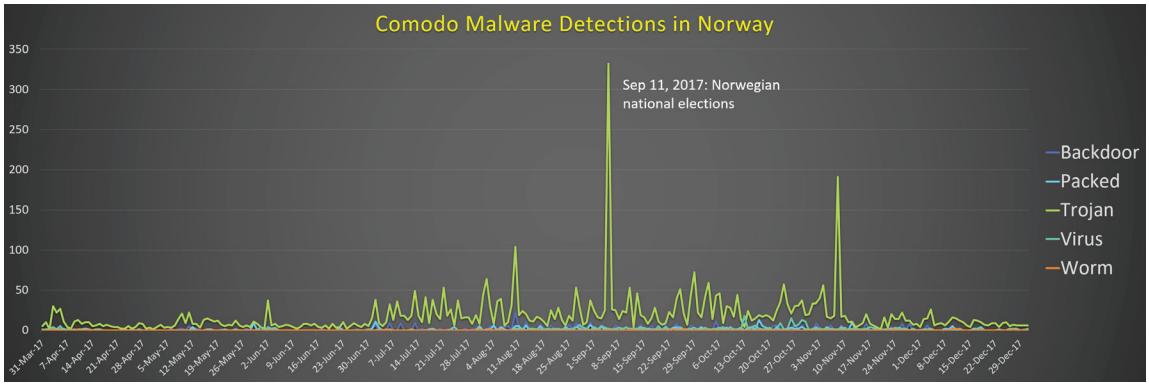

Figure 32: Norway

Here is another case in which elections may have been targeted by hackers. In Norway, Comodo saw by far its highest spike in malware detection on Sept. 5, less than a week prior to Norway's parliamentary elections.

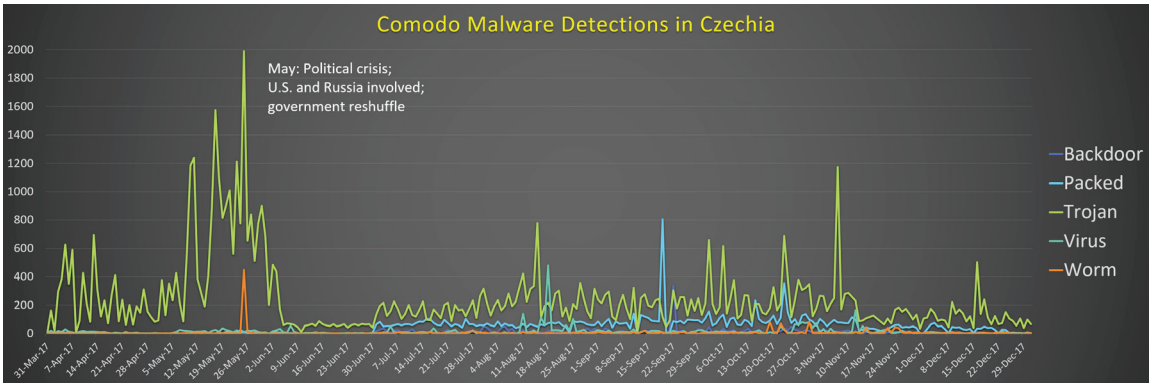

Figure 33: Czechia

Domestic social upheaval is often accompanied by extreme political, intelligence, and law enforcement challenges. Therefore, it is possible that the large wave of malware detections in Czechia was due to a period of domestic and international tension during spring 2017.

3 | Asia

This map shows the top malware types for Asia in 2017, as well as the top three malware families within each type from Q4 2017 for a sample set of nations.

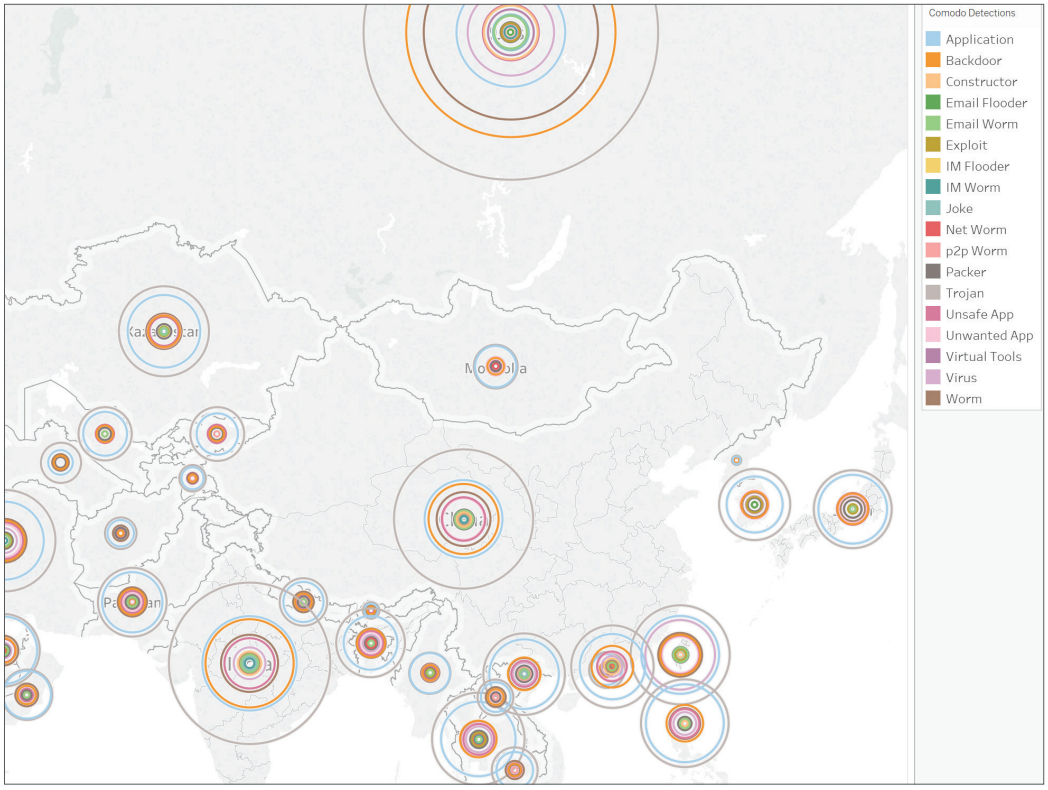

Figure 34: Malware Detections in Asia

China	Type: Trojan	Family: Hider
	Type: Application	Family: KuaiZip
	Type: Backdoor	Family: Hupigon
India	Type: Trojan	Family: Kryptik
	Type: Application	Family: DealPly
	Type: Backdoor	Family: Torr
Russia	Type: Trojan	Family: WannaCry
	Type: Backdoor	Family: Bladabindi
	Type: Worm	Family: Conficker

Potential Geopolitical Correlations

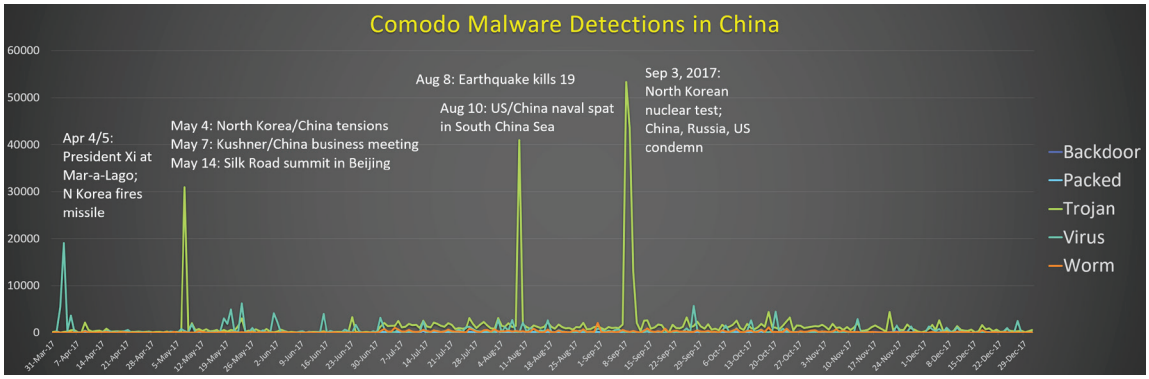

Figure 35: China

For at least the past 20 years, cyber espionage, and preparations for cyber war, have been a key part of international affairs in East Asia. While spikes in malware detection such as those seen above could be coincidental, it should no longer come as a surprise when significant events such as missile launches, nuclear threats, and other forms of international tension are reflected in cyberspace in the form of concurrent computer network operations.

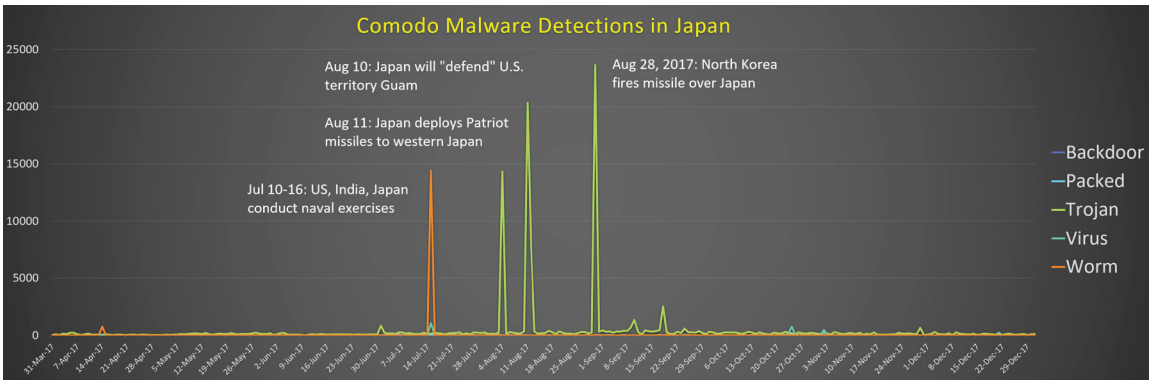

Figure 36: Japan

In Japan, Comodo detected a series of malware spikes at roughly the same time as numerous international military incidents in East Asia.

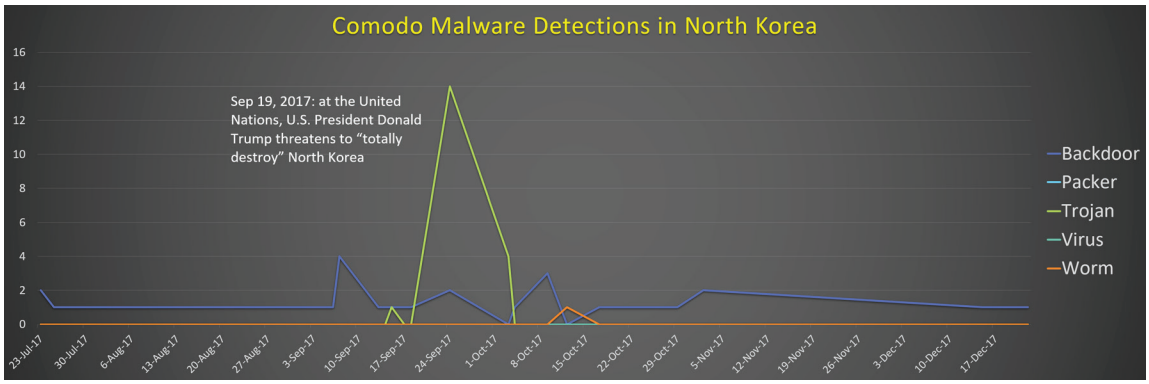

Figure 37: North Korea

Nuclear activity of any type draws worldwide attention, as nations scramble to gather intelligence and prepare for possible military operations. The startling spike seen above demanded the creation of the more detailed chart below — especially since Comodo is likely one of the few commercial cybersecurity companies with visibility inside North Korea.

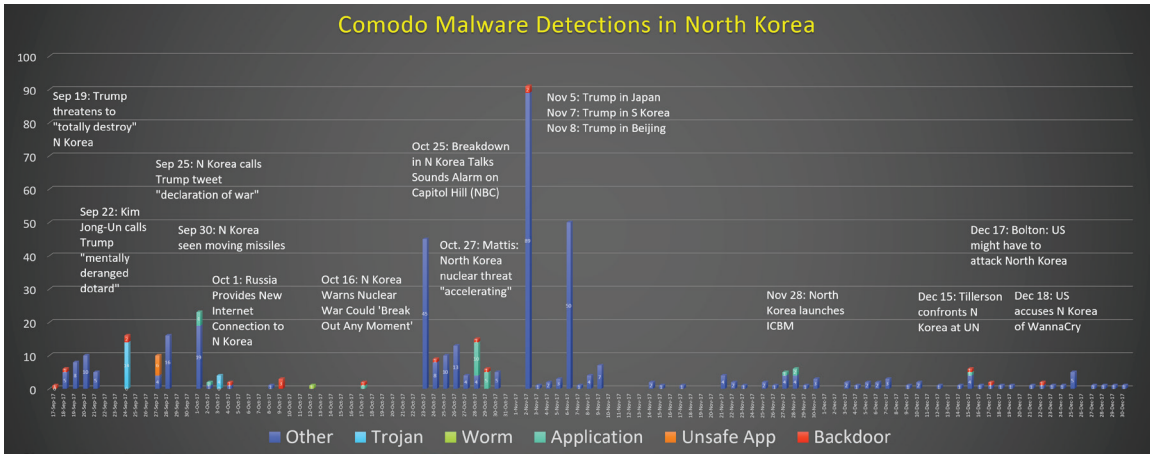

Figure 38: North Korea 2

Here, we can see not only the top malware types such as trojan and backdoor, but also a range of uncategorized "Other" malware that helps to provide a fuller picture. In-depth Comodo analysis of all of these malware detections suggests that North Korean network administrators are attempting to protect computer systems running unlicensed copies of Windows 7, using a variety of means including the use of remote access tools to monitor user activity and by trying to bypass Windows User Account Control (UAC).

4 | Middle East

This map shows the top malware types for the Middle East in 2017, as well as the top three malware families within each type from Q4 2017 for a sample set of nations.

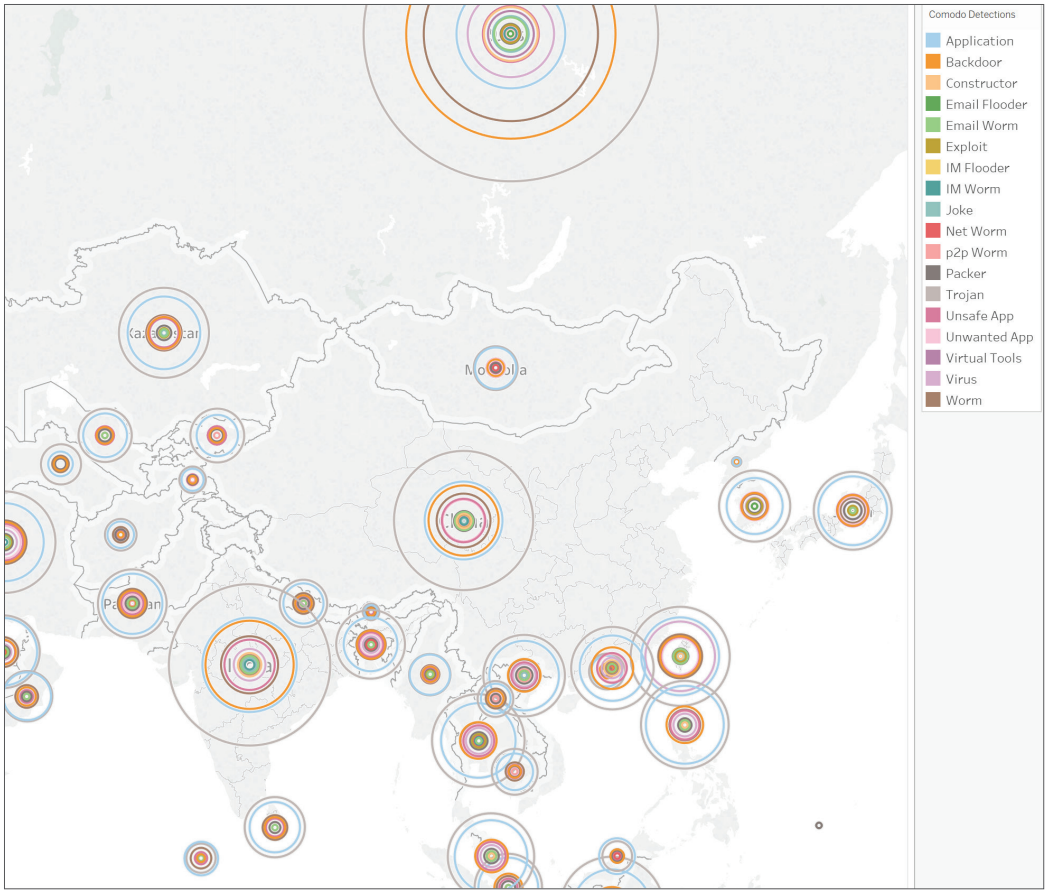

Figure 39: Malware Detections in the Middle East

Israel	Type: Trojan	Family: Yakes
	Type: Application	Family: MyWebSearch
	Type: Backdoor	Family: PCClient
Iran	Type: Trojan	Family: Dapato
	Type: Application	Family: CrossRider
	Type: Worm	Family: Autoit
Saudi Arabia	Type: Trojan	Family: Starter
	Type: Application	Family: MyWebSearch
	Type: Worm	Family: Delf

Potential Geopolitical Correlations

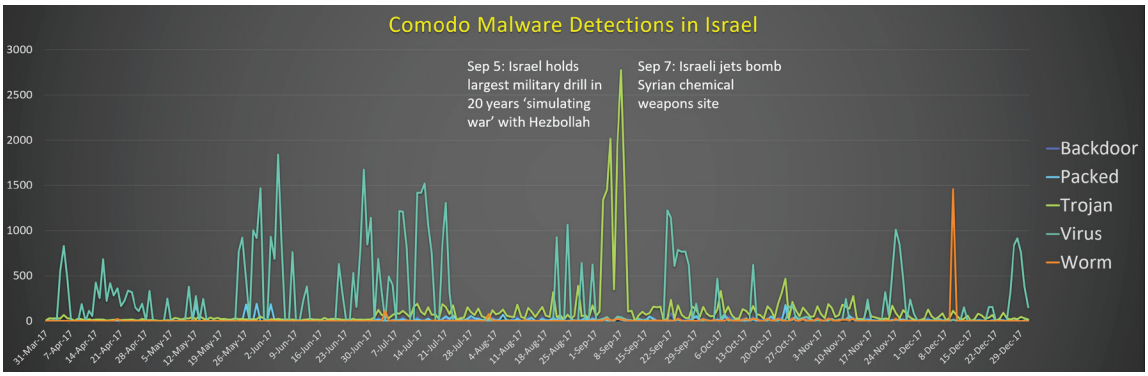

Figure 40: Israel

The largest malware spikes Comodo detected in Israel occurred concurrent to a major military exercise and an Israeli attack on Syria. Such events are of high political, intelligence, and military interest not only to regional nations, but also to governments around the world.

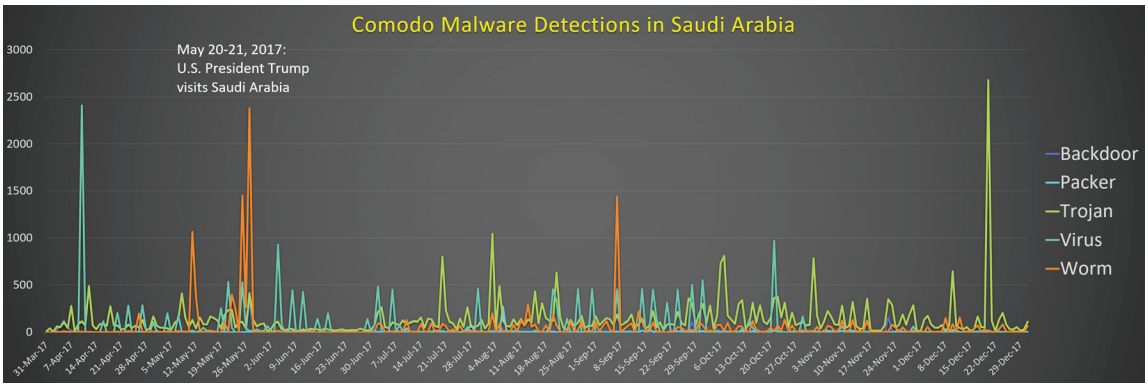

Figure 41: Saudi Arabia

In May 2017, U.S. President Trump took his first foreign trip visiting Saudi Arabia May 20-21 and Israel May 22-23. Comodo detected unusually high trojan activity in Saudi Arabia on May 11, 25, and 27.

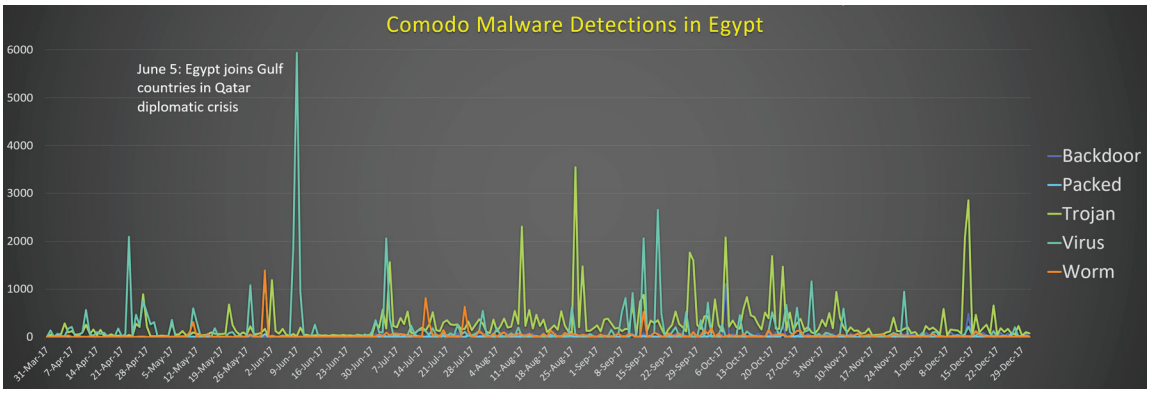

Figure 42: Egypt

In 2017, a major Middle East crisis erupted in June between Arab states including Egypt and Qatar concerning terrorism and relations with Iran. These events spilled over into cyberspace, with computer hacking and information operations in social media also playing a role.

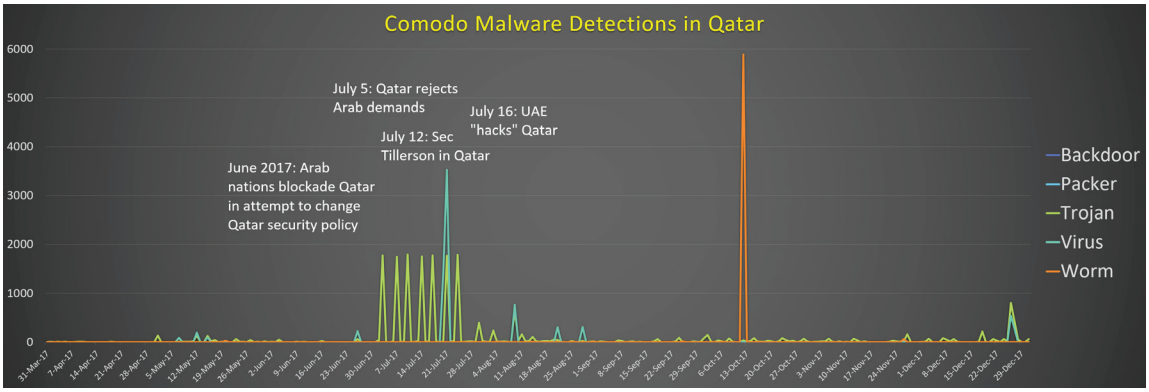

Figure 43: Qatar

In Qatar, Comodo detected a range of unusually high malware activity from July 3-24 that may have been associated with this international tension.

5 | South America

This map shows the top malware types for South America in 2017, as well as the top three malware families within each type from Q4 2017 for a sample set of nations.

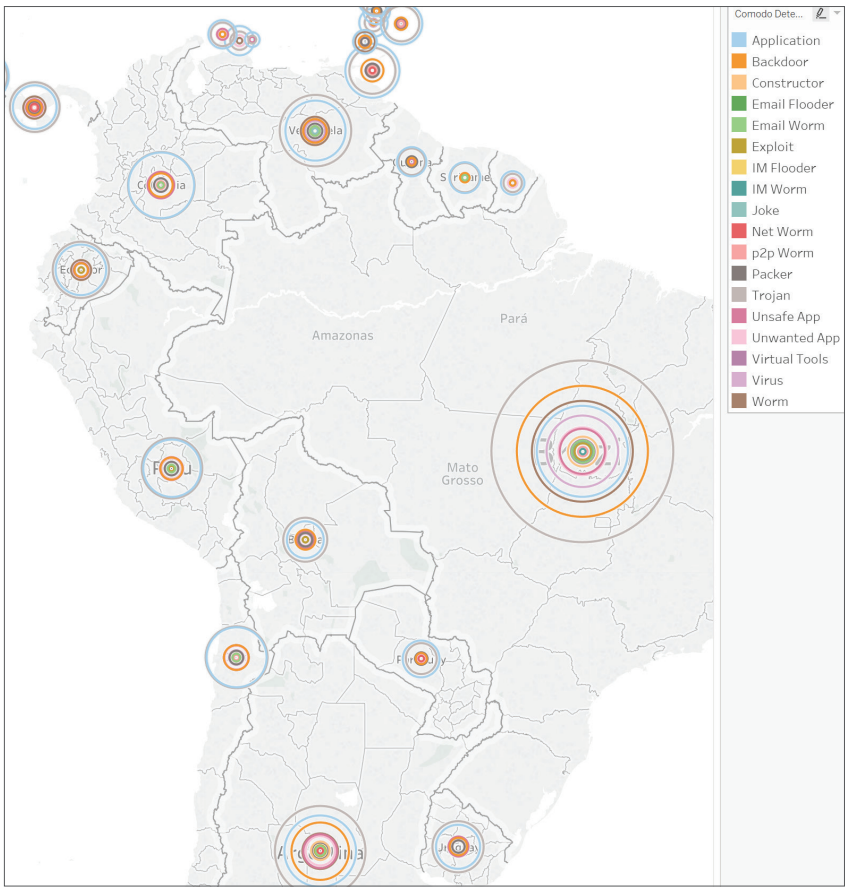

Figure 44: Malware Detections in South America

Argentina	Type: Trojan	Family: Zbot
	Type: Application	Family: MyWebSearch
	Type: Backdoor	Family: Rbot
Brazil	Type: Trojan	Family: Scar
	Type: Backdoor	Family: Bladabindi
	Type: Worm	Family: Mabezat
Chile	Type: Trojan	Family: Starter
	Type: Application	Family: MyWebSearch
	Type: Backdoor	Family: Androm

Potential Geopolitical Correlations

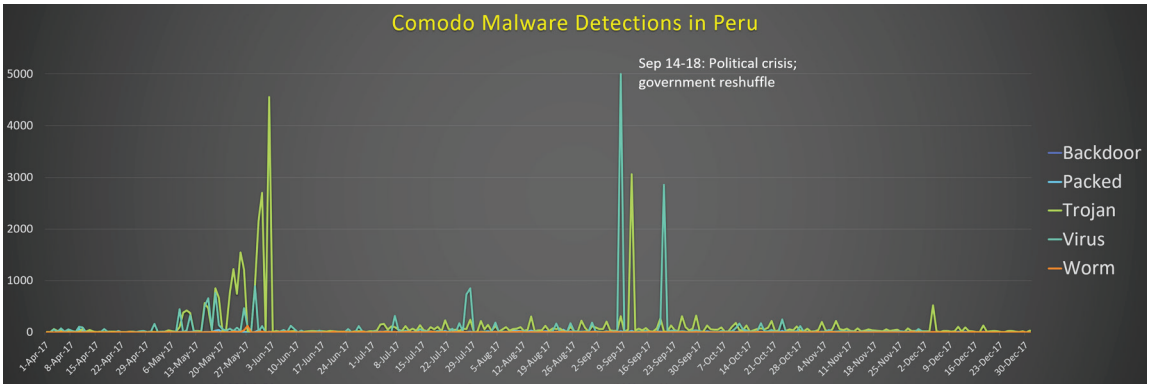

Figure 45: Peru

Comodo did not see a strong association between malware detection and geopolitics in South America in 2017. However, Peru may be an exception: between Sept. 14-18 there was a massive government shake-up, including a no-confidence vote in Congress, a resignation of the entire cabinet, and the appointment of a new Prime Minister. Comodo detected large virus and worm spikes on Sept. 8, 11, and 20.

6 | Africa

This map shows the top malware types for Africa in 2017, as well as the top three malware families within each type from Q4 2017 for a sample set of nations.

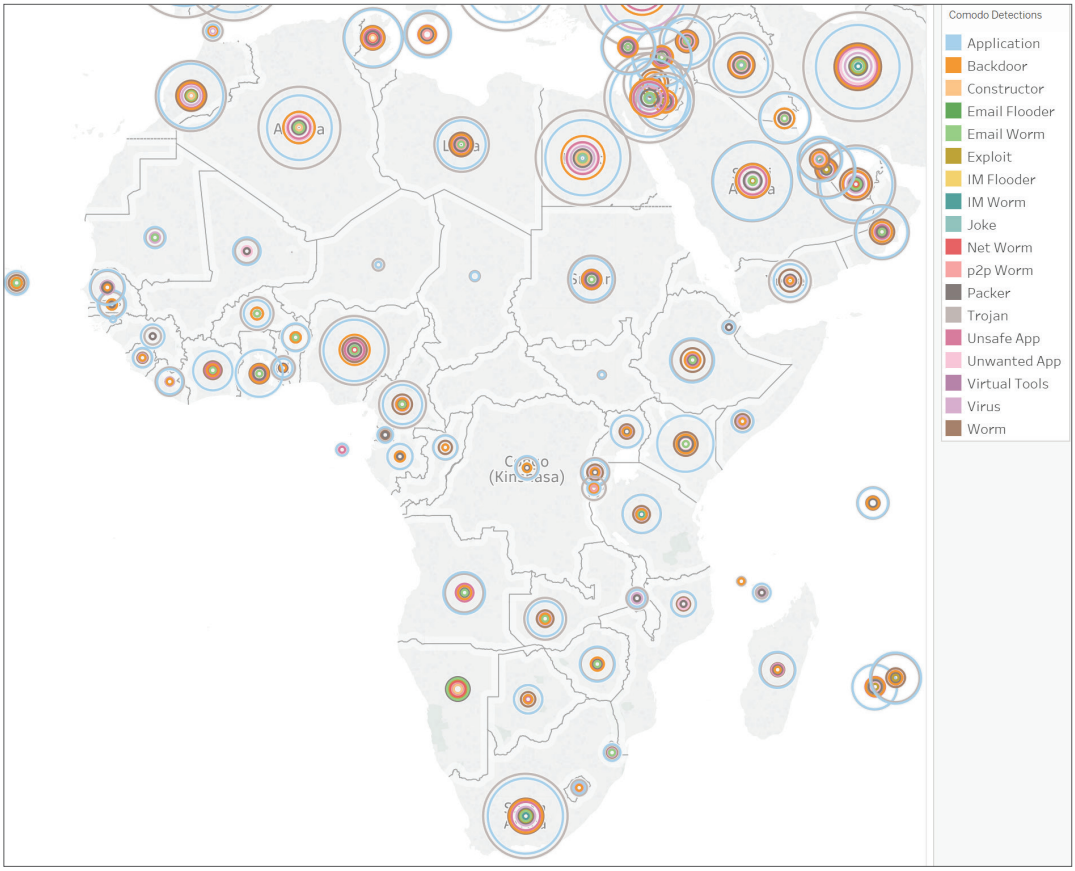

Figure 46: Malware Detections in Africa

Egypt	Type: Trojan	Family: Starter
	Type: Application	Family: HackKMS
	Type: Backdoor	Family: Shiz
Morocco	Type: Trojan	Family: Salrenmetie
	Type: Application	Family: CrossRider
	Type: Worm	Family: Mabezat
South Africa	Type: Trojan	Family: Fynloski
	Type: Application	Family: MyWebSearch
	Type: Worm	Family: Brontok

Potential Geopolitical Correlations

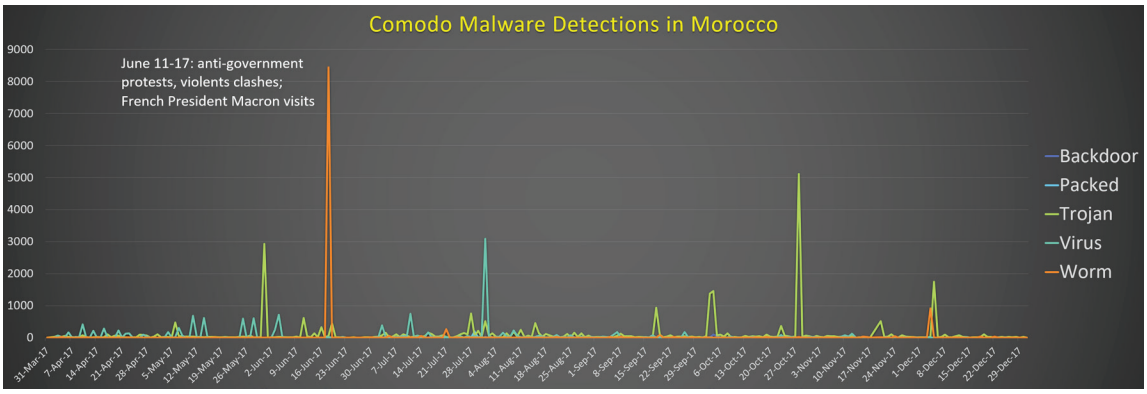

Figure 47: Morocco

The closest potential geopolitical correlation Comodo analyzed in Africa occurred during a time of extreme rioting in Morocco, in support of political and social reform during the middle of June 2017.

7 | Oceania

This map shows the top malware types for Oceania in 2017, as well as the top three malware families within each type from Q4 2017 for a sample set of nations.

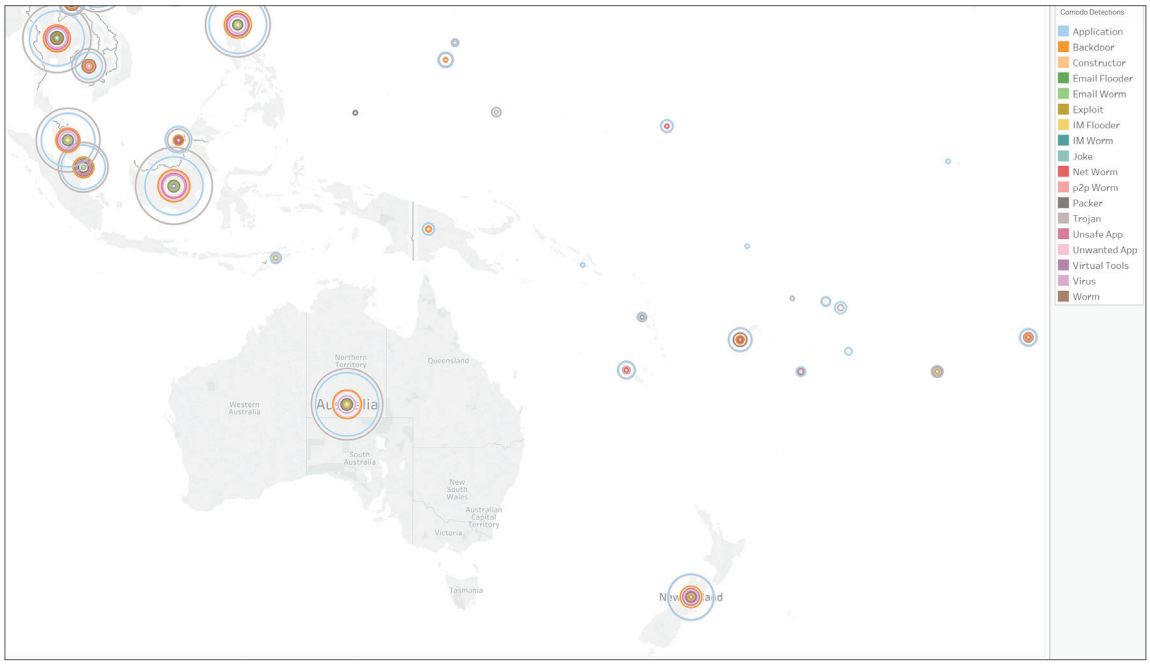

Figure 48: Malware Detections in Oceania

Australia	Type: Trojan	Family: Small
	Type: Application	Family: ELEX
	Type: Backdoor	Family: Xbot
Indonesia	Type: Trojan	Family: Ramnit
	Type: Application	Family: HackKMS
	Type: Backdoor	Family: Torr
Philippines	Type: Trojan	Family: Starter
	Type: Application	Family: Pirrit
	Type: Backdoor	Family: Shiz

Potential Geopolitical Correlations

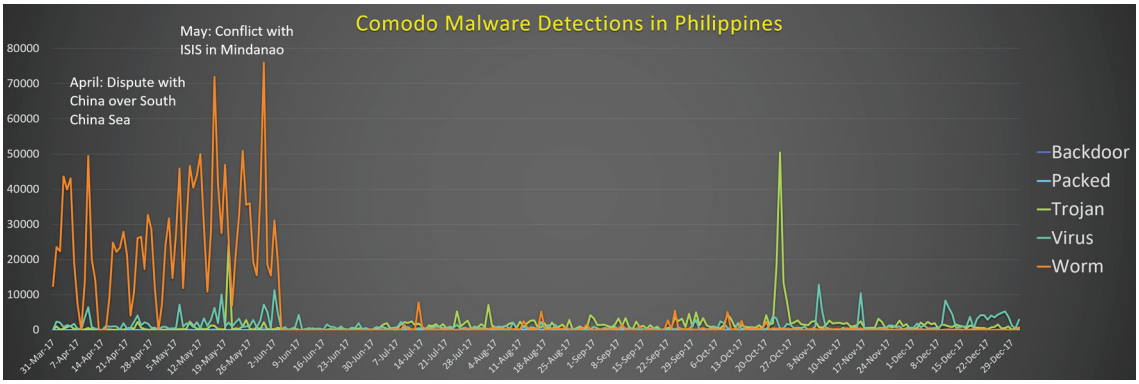

Figure 49: Philippines

This final chart is striking in its disparity between April/May and every other month. Therefore, it is possible that these changes are due primarily to unknown technical issues. However, in April the Philippine government was involved in a major international dispute with China, and during the month of May, there was an even more intense domestic conflict involving clashes with ISIS.

Vertical Analysis

It is often helpful to see how specific malware types and families may be found within particular verticals, as this can show the specific challenges that are inherent within any particular economic sector and which cyberthreat groups are targeting what type of data, which can also shed light on the thorny problem of attribution.

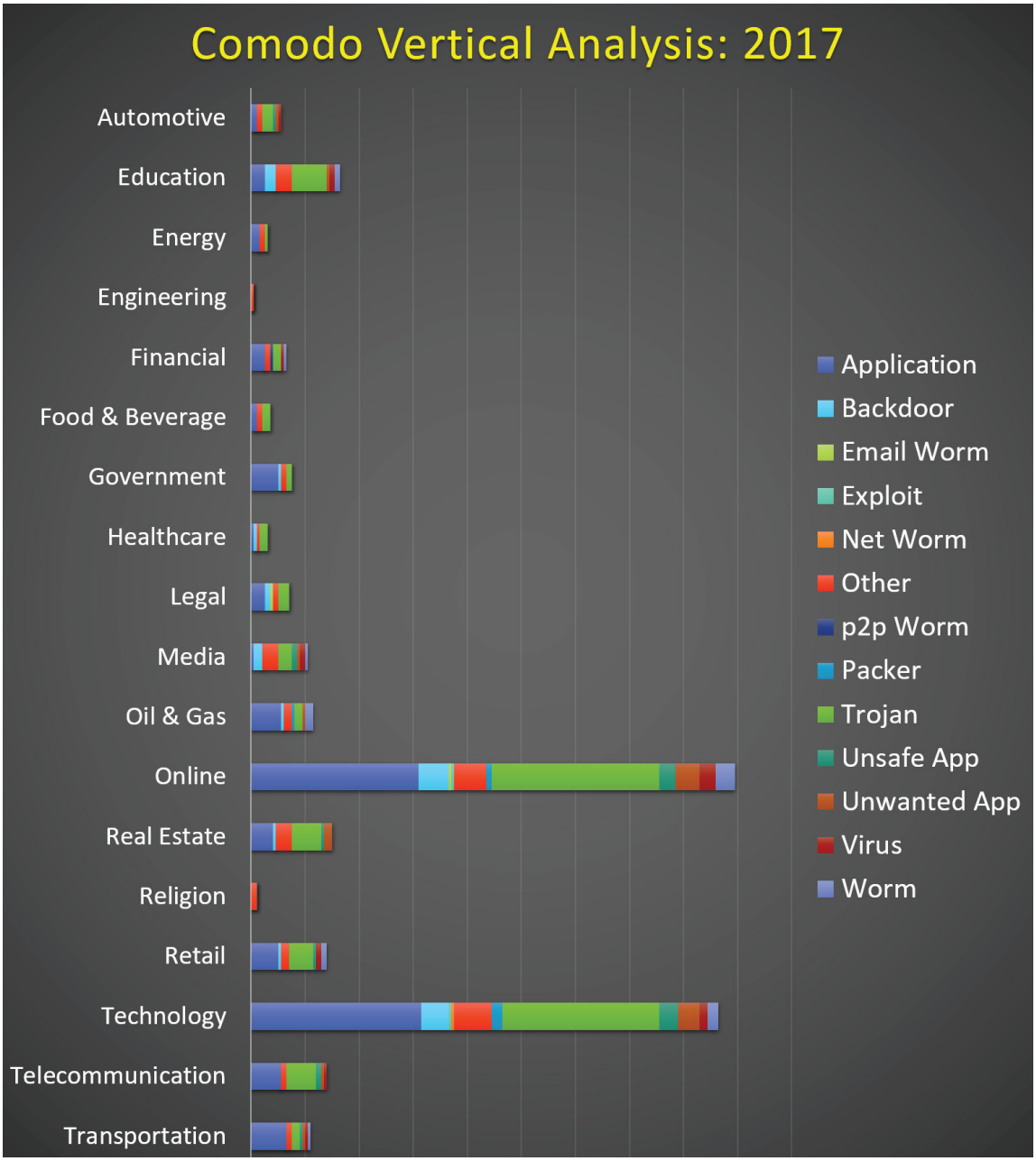

Figure 50: Comodo Vertical Analysis: 2017

In the chart above, we can see that online services and technology are commonly targeted. In part, this is due to the makeup of Comodo's clientele. However, it also speaks to another important dynamic: information technology producers and providers offer asymmetric keys to the virtual kingdom of cyberspace. In other words, if attackers can compromise a specific software or internet platform, they can also potentially target any user of that software or platform. Thus, they are the most sought-after targets for compromise by advanced cybercriminals and spies.

Top malware families within each vertical for Q4 2017:

Online	**Telecommunication**
1. BaiduWrapper 2. Injector 3. MailRu 4. Kryptik 5. MyWebSearch	1. Virut 2. Monder 3. IStartSurf 4. Bundledz 5. Spy
Technology	**Real Estate**
1. CompuTrace 2. WinVNC 3. Jeefo 4. DarkKomet 5. Monder	1. Cinmus 2. CompuTrace 3. MultiPlug 4. ArchSMS 5. AirAdInstaller
Oil & Gas	**Legal**
1. Krap 2. Ammyy 3. VB 4. Delf 5. Installcore	1. VB 2. TestFile.Eicar 3. FakeAlert 4. NetWiredRC 5. Obfuscated
Automotive	**Media**
1. Agent (generic) 2. Monder 3. Spector	1. OnLineGames 2. Parite 3. Jeefo 4. Hupigon 5. AutoRun
Education	**Transportation**
1. Jeefo 2. Hupigon 3. Parite 4. OnLineGames 5. VB	1. Teront 2. Amonetize 3. Renos
Retail	**Government**
1. MediaGet 2. InstallCore 3. Agent (generic)	1. SoftonicDownloader
	Healthcare
	1. Cossta

Recommendations

As the internet — and cyberspace — have matured around us, so have the quantity and quality of attacks on information security. In turn, we have created a professional discipline called “cybersecurity” that leverages best practices, technical certifications, user training, awareness campaigns, and more in order to limit the number of teenagers who can hack into the Pentagon. Nonetheless, cyberattacks persist because computer hacking has also become a professional discipline. Criminal syndicates and national three-letter agencies compete for top talent and devise increasingly powerful ways to leverage the power of computer network operations.

If you manage an important network, these historical dynamics mean at least three things. First, your computer network is vulnerable. Second, at some point it will be targeted by an advanced hacker. Third, due to the international architecture of the internet, law enforcement may not be able to help you very much. For the most part, when it comes to cybersecurity, we are all on our own. Fortunately, this is not rocket science, and there are many things you can do to protect your data, your customers, and your reputation, from keeping your software up-to-date to retaining off-line backups and teaching your employees how to spot social engineering.

Above and beyond the basics, you can research cutting-edge tactics and examine prevailing strategic trends. That’s where in-depth analyses such as this 2017 Comodo Global Malware Report are invaluable. For example, on the downside, Comodo detected and classified 19 unique malware types. But on the upside, trojans and applications constituted roughly 65% of all detections, so this can help you to focus limited resources and time on the most current points of attack.

When we plot these infections on a traditional world map, we see that the detections took place in an astonishing 225 country codes — and almost every nation-state on Earth. For network security, law enforcement, and counterintelligence personnel, this fact poses an overwhelming challenge. However, we also see that the clear majority of detections occurred in the U.S. and Russia. This bit of intelligence can help you to design your cybersecurity defenses, proactively through better traffic filtering and monitoring, and reactively by encouraging you to think now about future communications aimed at compromise mitigation.

In the world of geopolitics, this report offers significant evidence that computer network operations are regularly used to support political, intelligence, military, and business initiatives worldwide, from intelligence gathering via cyber espionage to preparations for war. In many individual countries, they also now play a tangible role in elections and any kind of political unrest. The takeaway for enterprises is that as political and/or military tension increases, so do the volume and sophistication of malware propagation and use.

Within specific verticals, we have also shown that each is plagued by a peculiar mix of malware types, families, and threat actors, which gives each person, business, nation, country, and even continent a unique malware profile. This insight is critical because it should encourage each enterprise to create a unique set of network defenses ideally constructed for the particular set of threat actors and operations it faces. And finally, the most sought-after compromises, from an attacker's perspective, are online services and technology as these are stepping stones that can be leveraged to compromise any number of future users of a given software or internet-based platform.

Looking toward 2018, our malware trendlines show that the detection rate for trojans, worms, unsafe applications, and malware packers is currently down. Holding steady are applications, unwanted applications, and viruses. Most importantly for Q1 2018, backdoors are now on the rise, which means that for the moment, enterprises should shift some of their focus to the detection and mitigation of backdoors. If you are interested in more specific information on certain malware types, malware families, or the countries in which Comodo has detected them, please send us an email at:
malwaresubmit@avlab.comodo.com

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.

Comodo and the Comodo brand are trademarks of the Comodo Group Inc. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. The current list of Comodo trademarks and patents is available at comodo.com/repository.

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

About The Comodo Threat Intelligence Lab

The Comodo Threat Intelligence Lab (the Lab) monitors, filters and contains, and analyzes malware, ransomware, viruses and other "unknown" potentially dangerous files 24x7x365 in over 190 countries around the world. With 5 offices spread across the Americas, Asia and Europe (and staff covering over 190 countries), the Lab is made up of more than 120 IT security professionals, ethical hackers, computer scientists and engineers (all full-time Comodo Lab employees) analyzing millions of potential pieces of malware, phishing, spam or other malicious/unwanted files and emails every day. The Lab also works with trusted partners in academia, government and industry to gain additional insights into known and potential threats.

The Lab is a key part of the Comodo Threat Research Labs (CTRL), whose mission is to use the best combination of cybersecurity technology and innovations, machine learning-powered analytics, artificial intelligence and human experts and insights to secure and protect Comodo customers, business and public sector partners and the public 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