COMODO

Comodo Threat Research Labs

Q3 2017 REPORT

Table of Contents

Executive Summary

Overview

- In Q3 2017, Comodo discovered 396,186,534 malware incidents
- Detections occurred in every nation-state on Earth
- Top five countries were: Russia, U.S., Poland, UK, Germany
- Top 20 countries accounted for over 80% of detections

Malware

- Top five malware threats
  - 13.7 M trojans
  - 5.4 M viruses
  - 2.8 M worms
  - 553 K backdoors
  - 384 K packed malware

- Top five countries by malware type, including top malware family
  - Trojans: Ukraine (Fynloski), Russia (WannaCry), Poland (BrowseFox), Turkey (Agent), India (Kryptik)
  - Virus: Brazil (Sality), Taiwan (Ramnit), Turkey (Sality), Indonesia (Ramnit), Ukraine (Sality)
  - Worm: Russia (Brontok), Canada (Brontok), Turkey (Brontok), India (Agent), South Africa (Brontok)
  - Backdoor: U.S. (Agent), UK (Agent), Italy (Teldoor), Russia (Agent), Slovenia (Hupigon)
  - Packed: Russia (MUPX), Brazil (MUPX), Ukraine (MUPX), U.S. (MUPX), Poland (MUPX)

Global Analysis

- Trojans were the top malware type in most countries
  - Trojans are the Swiss Army knife of malware, and can be used for any type of follow-on attack including ransomware

- South America, Africa, Southeast Europe, and Southeast Asia had a high proportion of viruses and worms
  - Viruses and worms tend to afflict poorer nations with a prevalence of older, unlicensed, unpatched, or pirated software

- North Korea had a high number of backdoors
  - Comodo detections within North Korean network space showed fewer exposed vulnerabilities but a high number of targeted attacks

New Sophisticated Phishing Attacks

- Comodo discovered multiple new, large-scale, global email-based phishing attacks
  - Three attacks were related to "Locky" Trojan and delivered a ransom payload
  - Comodo's default deny **endpoint security** protected customers and prevented attacks on businesses and individuals, even on day zero

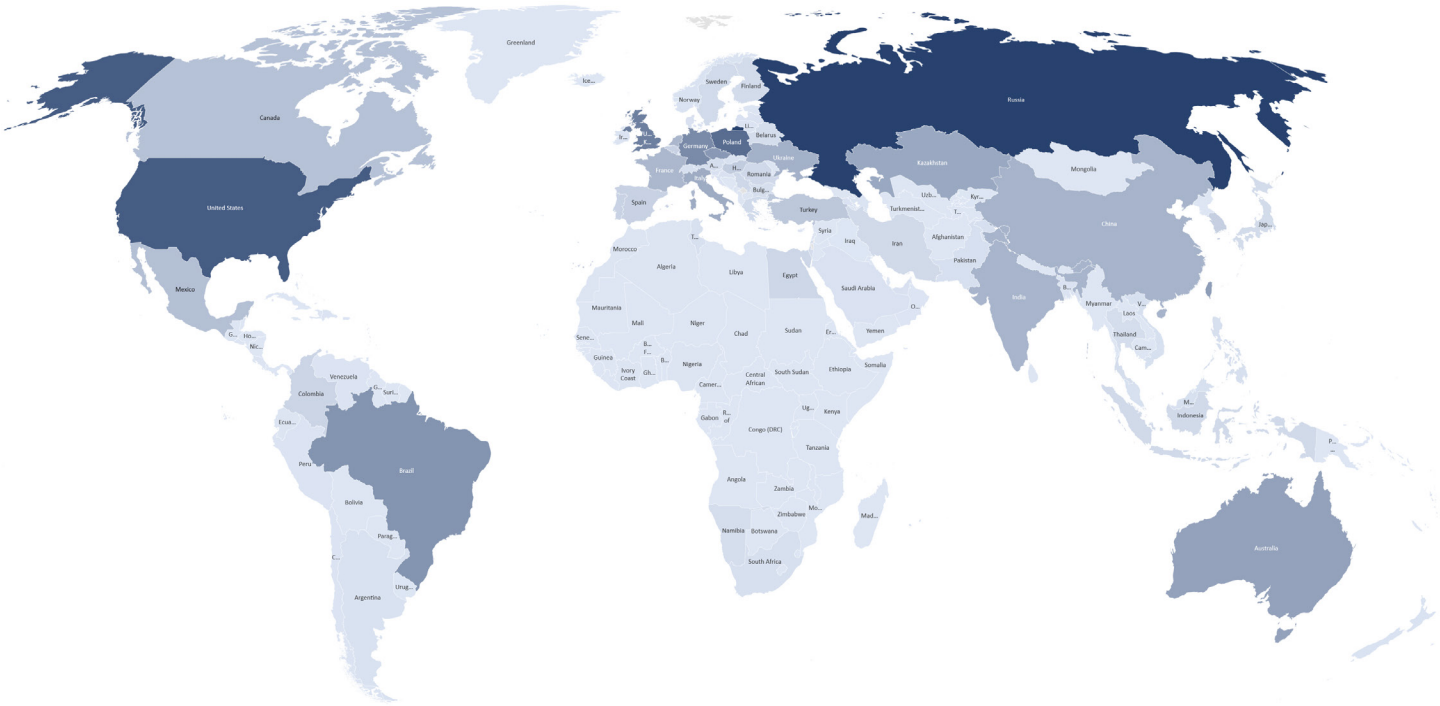
Recommendations

- Strategic analysis can help cyber defenders at the tactical level
- Brains over brawn: integrate security into your corporate culture
- Do not respond to unsolicited requests; do not post office photos
- Calculate business risk first, then incorporate cyber risk
- Containers and quarantines mimic best practices from the non-cyber world
- Hard problems like encryption must be integrated into network infrastructure
- Your "security stack" must evolve with the hacker threat
- Metrics are critical to the decision-making process
- Never "hack back": it is illegal and unwise
- Artificial Intelligence (AI) aids with simple and hard tasks but is no silver bullet

Malware Detections: Q3 2017

Introduction

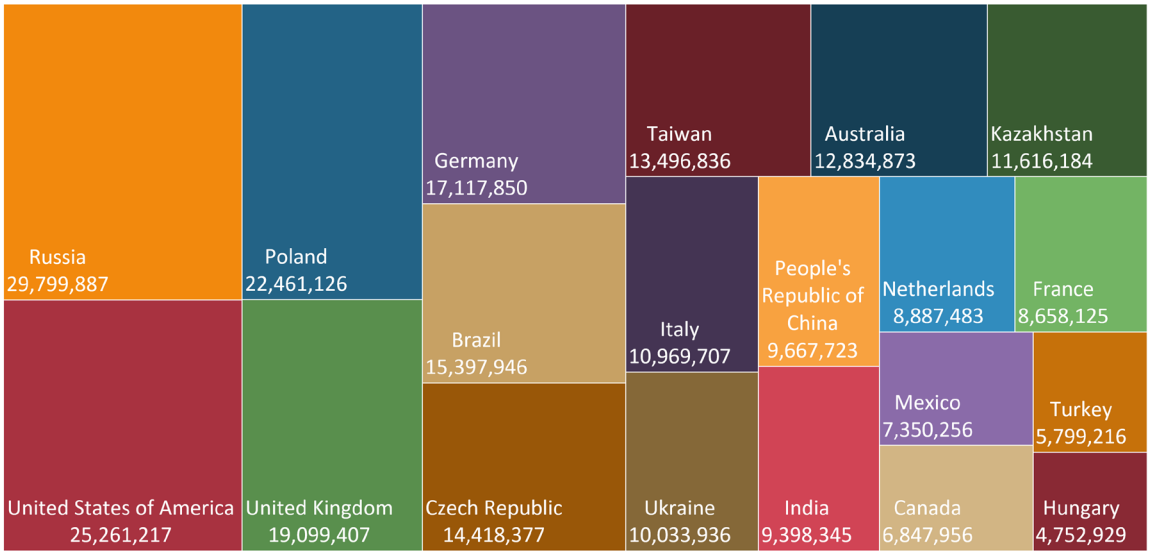
In Q3 2017, Comodo detected 396,186,534 malware incidents within 234 of the 255 top level country code domains (ccTLD) and some from every nation-state on Earth. Comodo has been building internet infrastructure for almost 20 years, giving our company tens of millions of endpoints and an astonishing degree of visibility in the global information security space. The world map below depicts this overall count by country of detection: the darker the shade, the more malware detected. This overall number of malware detections includes malicious, suspicious, unwanted, and potentially unwanted applications. It also includes malware types and families that have yet to be categorized precisely.



As these numbers show, the world is now swimming in malware. The internet and cyberspace are still quite new – and vulnerable. As with any new technology, such as aviation, humans build it first and then try to secure it. We'll fix this thing eventually, but for the moment, there are simply too many exposed vulnerabilities and too much insecure network architecture. Given the time and resources, attackers tend to find the unpatched server under Bob's desk, the Raspberry Pi in the laboratory, or the Internet of Things shark tank in Las Vegas. While computer security best practices are indispensable, they are not perfect.

Top 20 Countries

Here are the top 20 countries where Comodo detected malware in Q3 2017. Russia came in first place, but the U.S. was not far behind. Europe was home to most of the other detections, from Poland to the U.K., Germany, Czech Republic, Italy, Ukraine, France, Netherlands, and Hungary. Asia was represented by Taiwan, Kazakhstan, China, and India.



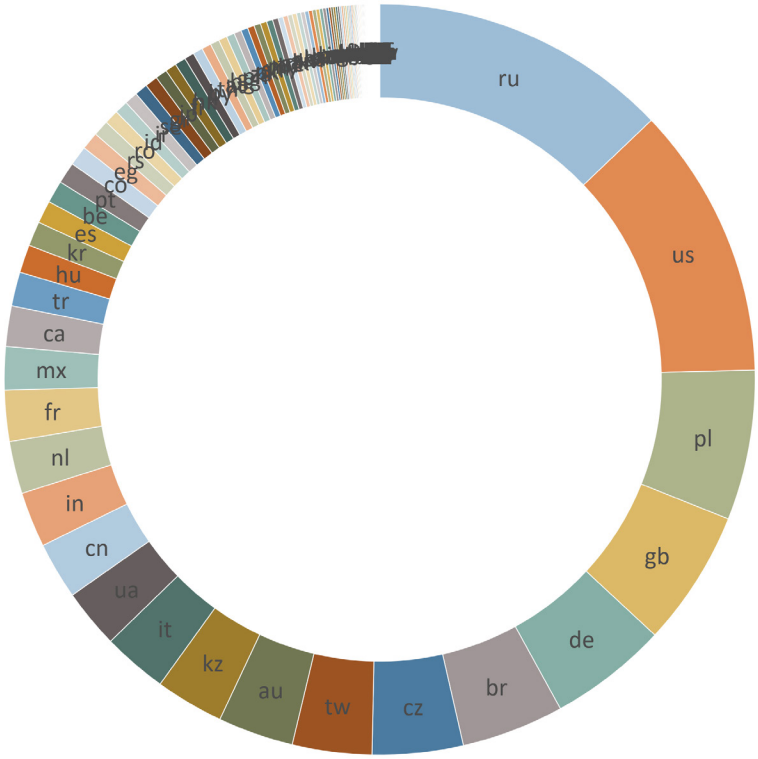
One of the primary takeaways from this treemap is that most of the world's malware infrastructure is based within a minority of countries. This group of 20 nations accounted for 318.9 million malware detections in Q3 2017, or just over 80% of the world total.

These numbers have practical implications for network security, as national sovereignty and law enforcement jurisdiction usually end every time a data packet crosses a border. Thus, security researchers and criminal investigators could broaden their scope by focusing on those countries where their time, money, and resources are most efficiently spent. But international collaboration is always easier said than done, and many of the countries in this top-20 list sit on opposite sides of many political and military conflicts.

All Nations Are Compromised

If you have ever examined network log files, you have seen long lists of Internet Protocol (IP) addresses from around the world, including from some countries you had never heard of. These are not an attacker's true IP, but a compromised computer that acts as a stepping stone across the internet or one node in a large network of compromised, attacker infrastructure.

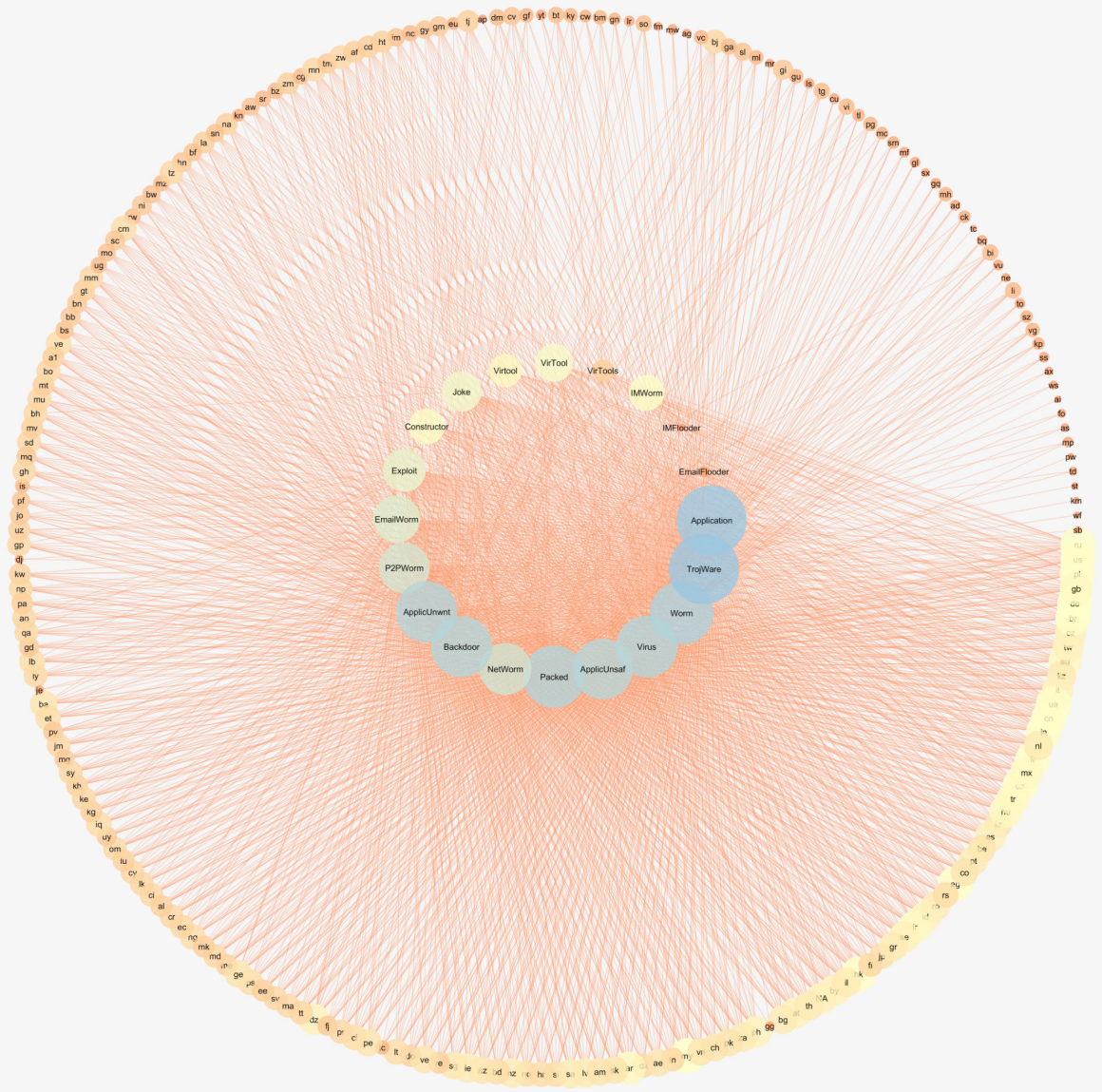
The donut chart below depicts all of the countries in which Comodo detected malware in Q3 2017. After the top 20 countries (from Russia to Hungary), the remaining 77 million malware incidents were detected in the other 90% of the world's countries, from South Korea (21st place with 4.2 million detections) to Kiribati (234th place with one single detection).



This graph shows that attackers, when they are in possession of compromised computers in numerous different countries, can merely spin the roulette wheel and route hostile communications from a different law enforcement jurisdiction each time, continually changing their point of attack. For example, an American hacker stealing money from an American bank can easily make sure that he or she is pretty hard to track.

Malware: Network Graph

Here is a network graph of the same dataset, which shows the connection between the full range of Comodo's malware types and the countries where we discovered them.



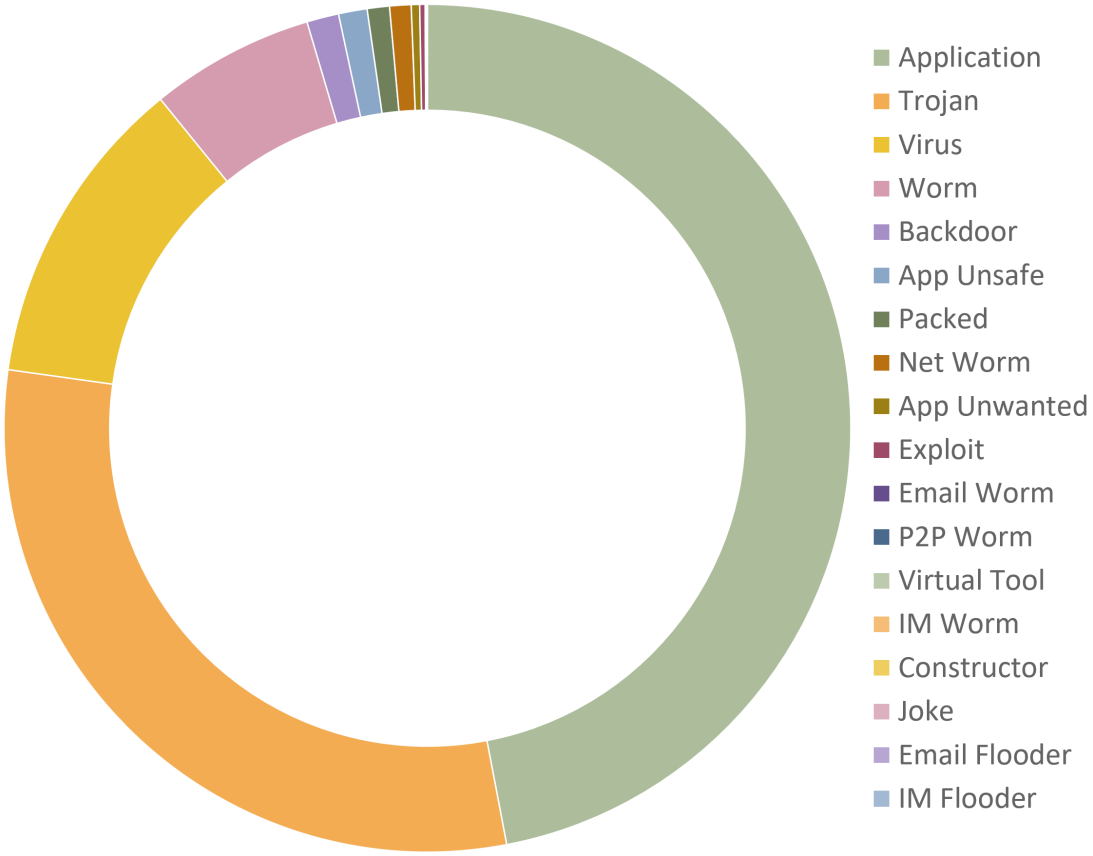
Malware is fundamentally an international problem, as hackers are able to steal, block, and manipulate data without regard to national sovereignty or law enforcement jurisdiction. It is possible to specify a circuitous, ever-changing attack pattern every time, and take advantage of countries with which the victim has poor diplomatic relations and/or significant geographic separation.

Malware Analysis

Introduction

Malware can be hard to define. Often, it is like a Swiss Army Knife that can be used for a wide range of attacks. However, malware analysts endeavor to categorize malware by functionality, propagation, and other characteristics, so that it is possible to detect, block, and prevent malicious behavior. In general, malware will try to undermine the confidentiality, integrity, and/or availability of computer systems.

The chart below shows all of the malware types detected by Comodo around the world in Q3 2017.



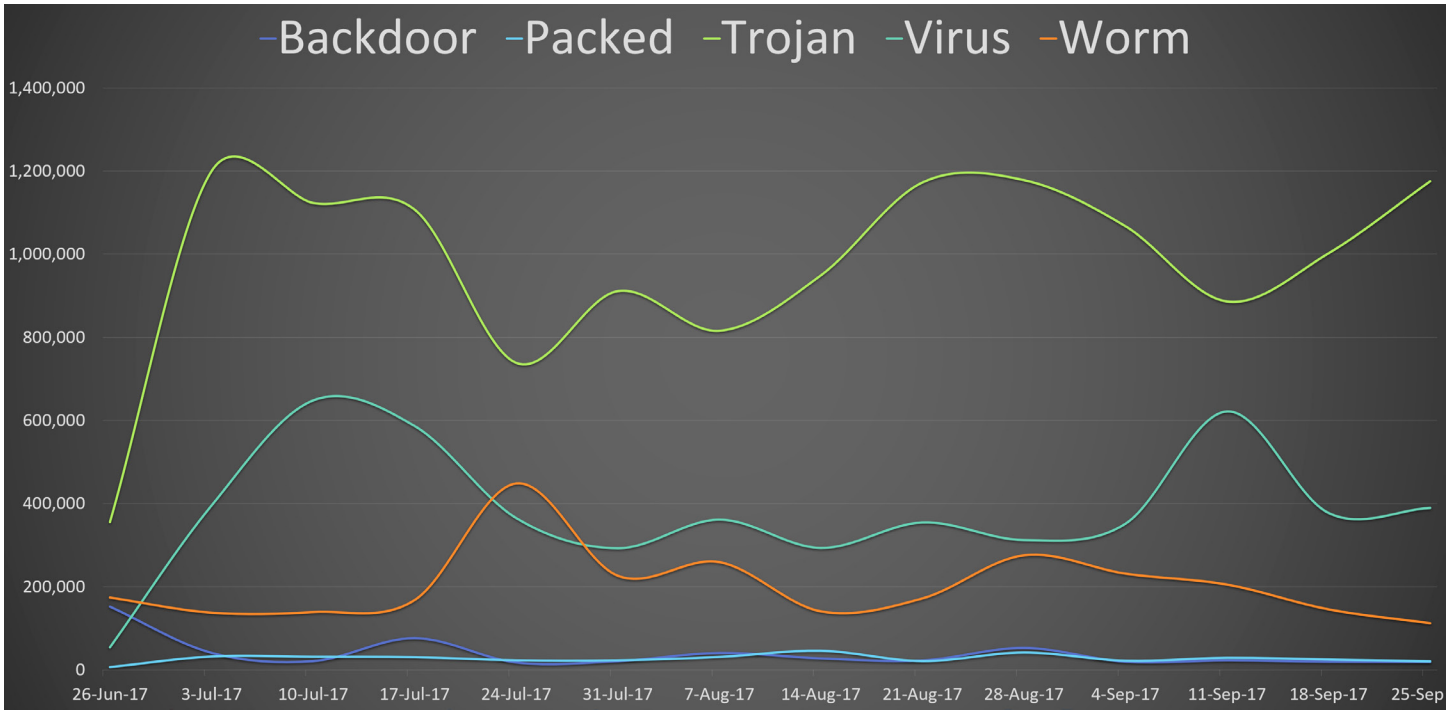
The largest category includes all applications that were found to be malicious, suspicious, unsafe, or unwanted. Due to its sheer size, the application malware type will soon be addressed in a separate report. In this report, we will examine the five most dangerous malware types: versatile Trojan horses, file-changing computer viruses, autonomous worms, secret backdoors, and packed malware.

Timeline: Malware Types

The five most dangerous malware types in Q3 2017 were:

Malware Types	Quantity
Trojan	13.7 M
Virus	5.4 M
Worm	2.8 M
Backdoor	553 K
Packed	384 K

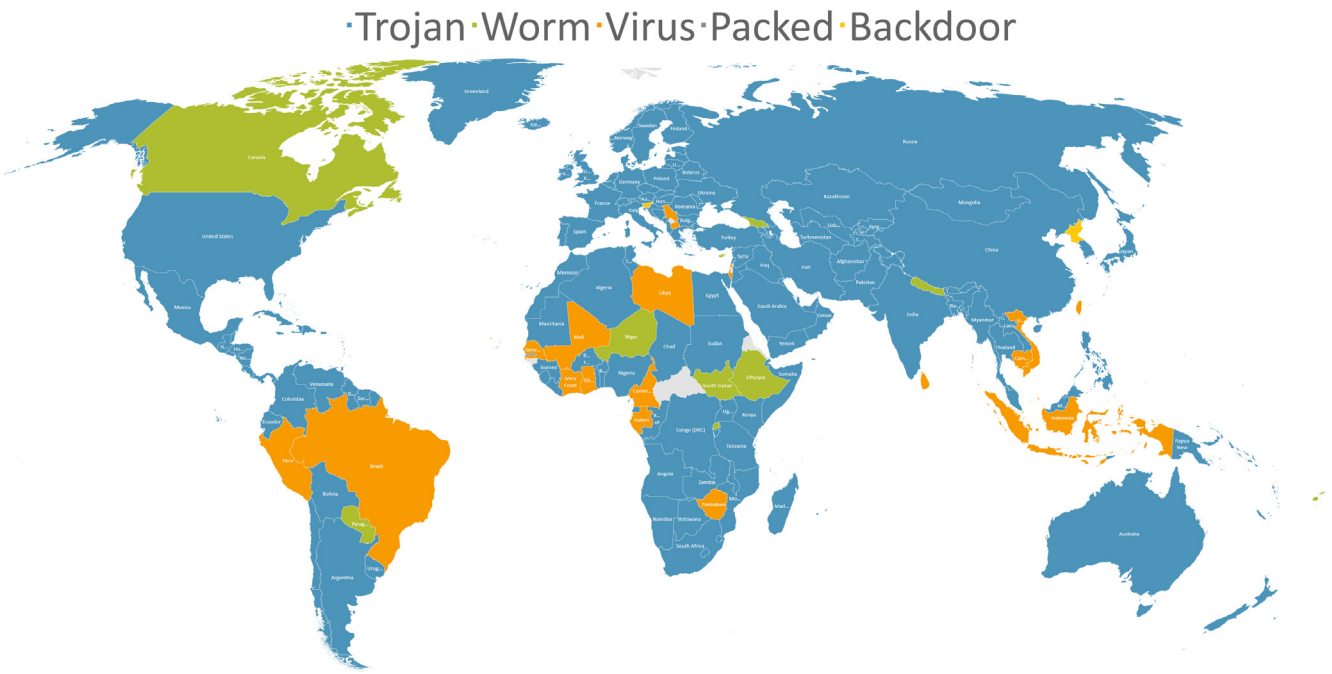
The Q3 2017 timeline, below, shows that malware usually spreads through the internet – and across the Earth – in waves, as specific malware families take advantage of specific computer vulnerabilities. Once the outbreak is detected, however, network and security administrators undertake remediation, and software companies release software patches that get downloaded and installed on local networks. This dynamic is cyclical, with attackers and defenders competing in a perpetual game of cat and mouse that seemingly never ends.



World Map: Malware Types

Every individual, enterprise, nation, and continent has a unique malware profile. Although each profile is in a constant state of change, there are many strategic trends that can be discerned, some of which are fairly consistent over time. In fact, these strategic characteristics can help tactical cyber defenders to more efficiently and effectively manage their networks.

The map below shows the top malware types in each country for Q3 2017.



Here, especially when complemented by Comodo's Q1 and Q2 reports, we begin to see that even the Earth has a malware profile. Most countries have trojan as the top malware type, especially in the Northern Hemisphere; this is normal, as trojans are the Swiss Army knife of malware and can be used for any type of follow-on attack.

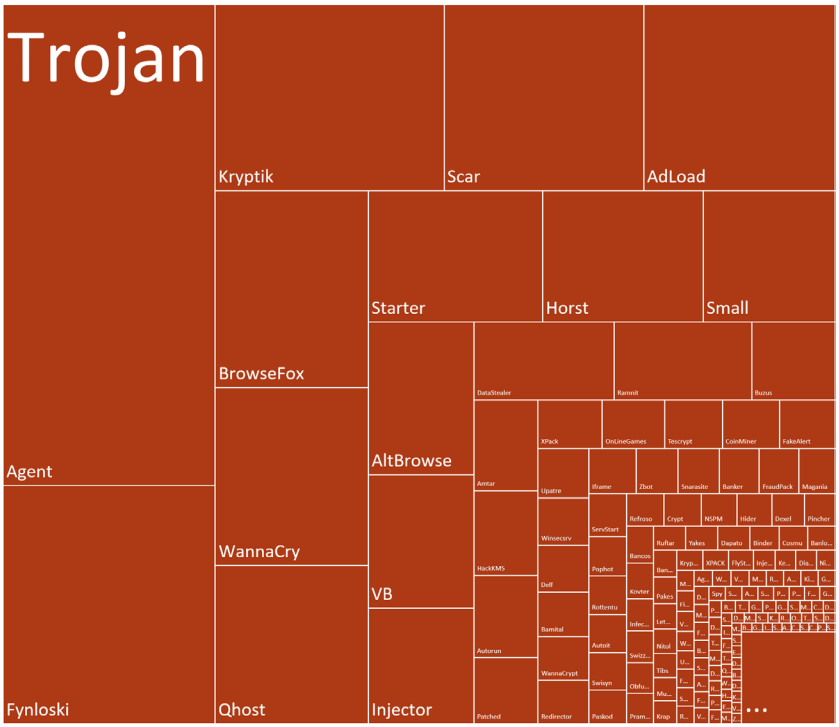
The Southern Hemisphere suffers from a much wider range of malware types than the North. South America has a chronic problem with viruses. Africa is plagued by far too many computer worms. Southeast Europe and Southeast Asia often share similar characteristics. The primary reason for these geographic cleavages is socioeconomic: poorer countries are likely to have a greater volume of older, unlicensed, unsupported, unpatched, and/or pirated software, which increases their vulnerability to types of malware that simply pick the lowest hanging fruit.

Backdoors provide us a counterpoint, as they sit at the high end of malware in terms of targeting, stealth, and potential return on investment. Take the example of North Korea: its top malware type is backdoor, which suggests few exposed vulnerabilities, but a high degree of targeted attacks – which is quite logical, both from a network and traditional geopolitical perspective.

Trojan

The most common malware threat in the world today takes its name from the famous wooden horse of Greek mythology, which was a gift that contained hidden, malicious functionality in the form of concealed soldiers. In the same way, a software trojan horse is a seemingly useful or benign computer program that contains hidden, hostile code, which can give a remote attacker the same rights and privileges as a local user. A trojan can be used for many different kinds of cyberattack, including the installation and execution of ransomware. As with a virus, attackers often use social engineering to trick users into downloading and installing trojans, such as through an email-based phishing campaign that leverages social engineering.

The treemap below displays the most common trojan families that Comodo detected in Q3 2017.

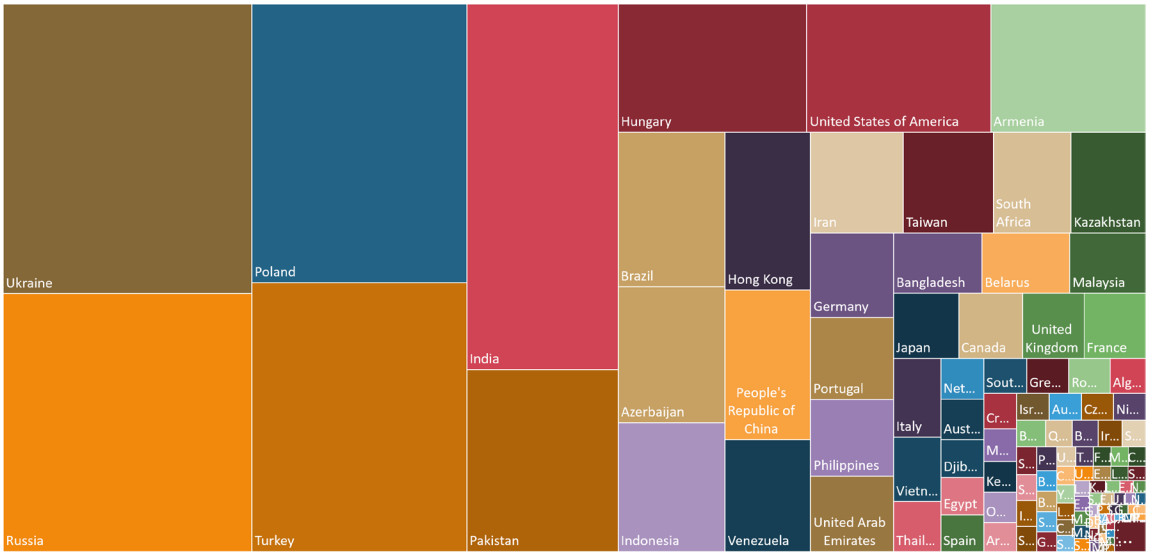


Agent refers to a generic pattern of trojan-like behavior which has not yet been specifically placed into a known trojan family.

The table below shows the top ten known trojan families, raw detection counts, and percentages of the total (13,680,313).

Top 10 Trojan Families	Raw Detection Counts	Percentage of Total
Fynloski	1,154,625	8.4%
Kryptik	974,737	7.1%
Scar	848,873	6.2%
AdLoad	813,826	5.9%
BrowseFox	688,735	5.0%
WannaCry	624,183	4.6%
Qhost	554,163	4.1%
Starter	524,127	3.8%
Horst	482,686	3.5%
Small	395,767	2.5%

Here is a treemap of the countries in which Comodo detected trojans in Q3 2017:



Trojans are not only Comodo's most commonly discovered malware type, but also our most complex. We detected 3,461 unique trojan families within 222 country codes. There is definitely a theme among the top three victim nations: they are all in Eastern Europe.

The table below shows the top 10 countries where Comodo detected trojans in Q3, their raw numbers, and percentages.

Top 10 Trojan Countries	Raw Detection Counts	Percentage of Total
Ukraine	1,552,113	11.3%
Russia	1,382,031	10.1%
Poland	1,290,242	9.4%
Turkey	1,243,907	9.1%
India	1,191,426	8.7%
Pakistan	593,198	4.3%
Hungary	519,578	3.8%
U.S.	508,493	3.7%
Armenia	426,601	3.1%
Brazil	355,373	2.6%

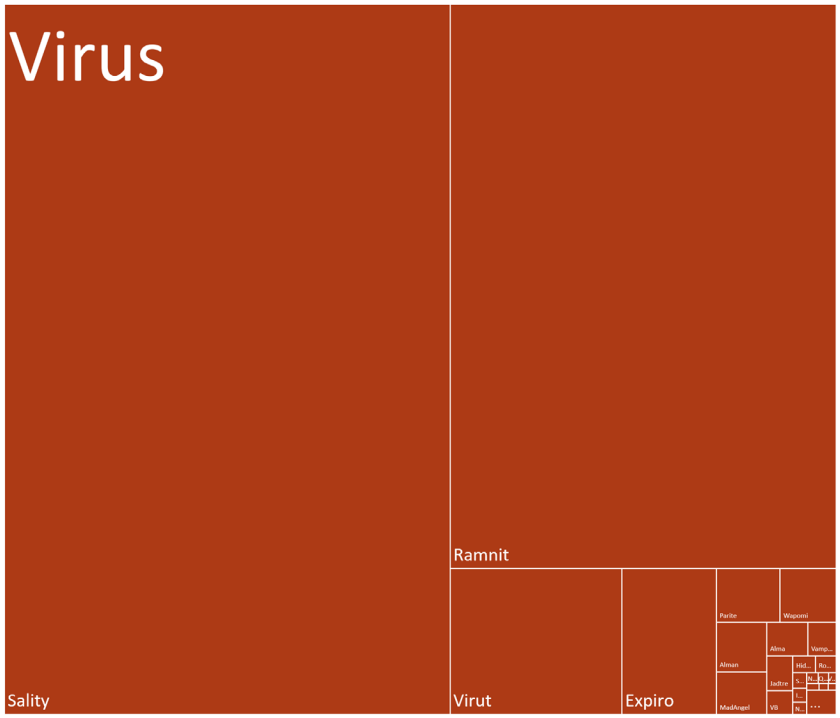
In the sunburst chart below, the top 10 countries are shown in tandem with their detected trojan families. Here we can see that Fynloski was particular to Ukraine, but that Ukraine and Russia have both shared a WannaCry problem. Armenia and Brazil were afflicted by Scar. Turkey and Pakistan shared an “Agent” challenge. But the rest were mostly unique.

This sunburst chart shows that the strategic malware picture can help to inform tactical cyber defenders, specifically by showing where they are in the global malware landscape, and how policy, technical, socioeconomic, and geopolitical factors converge to give each nation a unique threat environment and malware profile.

Virus

A computer virus is self-replicating code that "infects" another computer program, corrupting it in malicious ways that can 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 by opening an attachment or clicking on a hyperlink. When the host file is executed, the virus code also runs, infecting the new host.

The treemap below displays the most common virus families that Comodo detected in Q3 2017.

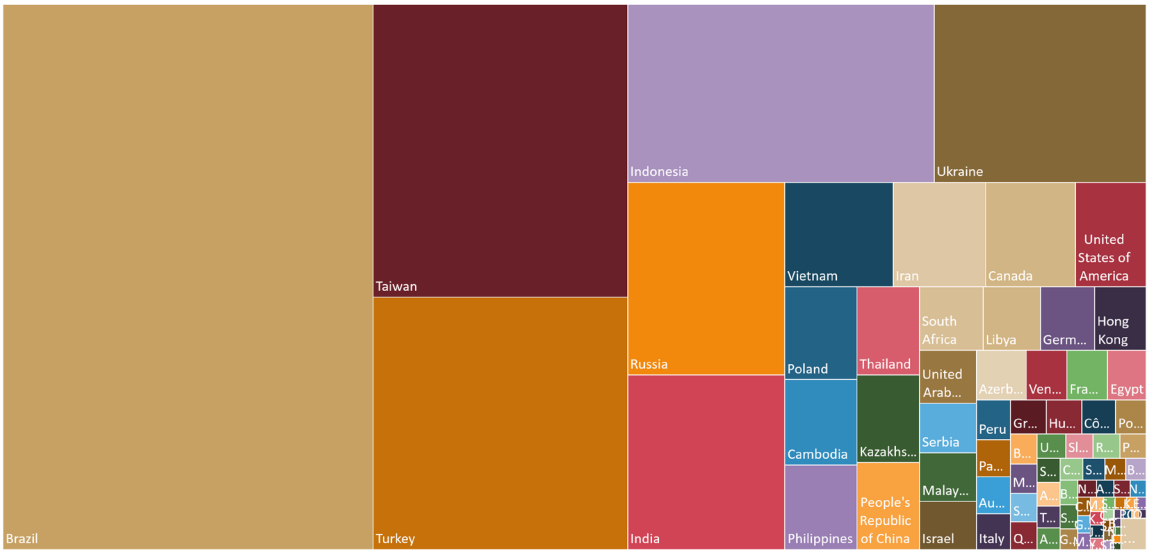


As you can see, the virus malware type may be second to trojan in number of detections, but it is, in fact, a simpler dataset to work with – and to defend against.

The table below shows the top 10 known virus families, raw detection counts, and percentages of the total (5,404,651).

Top 10 Virus Families	Raw Detection Counts	Percentage of Total
Sality	2,895,867	53.6%
Ramnit	1,993,515	36.9%
Virut	229,301	4.2%
Expiro	126,280	2.3%
Parite	31,360	0.6%
Wapomi	27,656	0.5%
Alman	22,622	0.4%
MadAngel	19,732	0.4%
Alma	12,433	0.2%
Vampiro	8,584	0.2%

Here is a treemap of the countries in which Comodo detected viruses in Q3 2017:

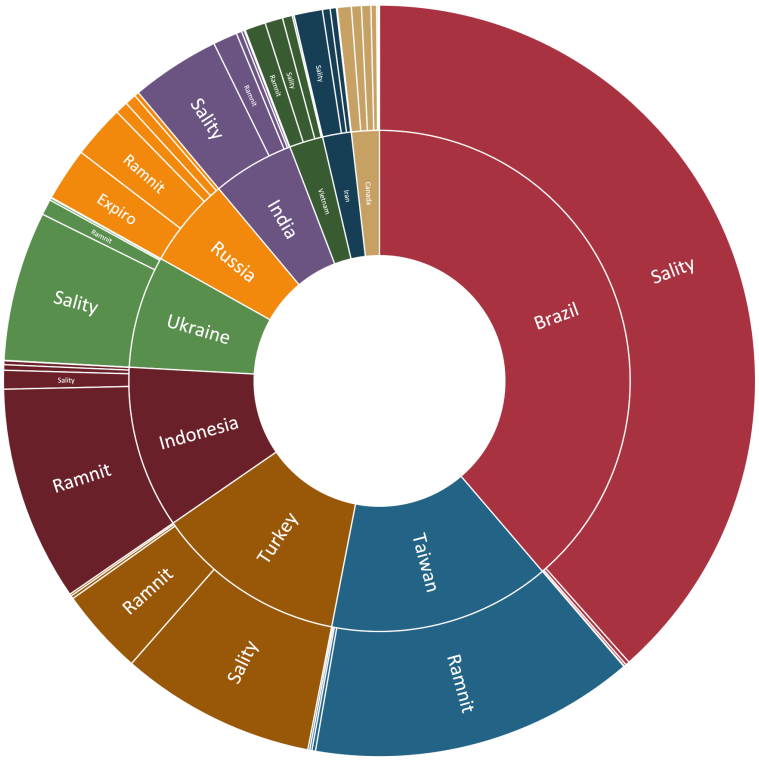


Comodo detected 315 unique virus families within 171 country codes. Brazil led the way, followed by Taiwan, Turkey, Indonesia, and Ukraine. The table below shows the top 10 countries, their raw numbers, and percentages.

Top 10 Virus Countries	Raw Detection Counts	Percentage of Total
Brazil	1,745,609	32.3%
Taiwan	645,228	11.9%
Turkey	556,071	10.3%
Indonesia	472,223	8.7%
Ukraine	326,481	6.0%
Russia	261,347	4.8%
India	237,315	4.4%
Vietnam	97,722	1.8%
Iran	83,382	1.5%
Canada	81,054	1.5%

In the sunburst chart below, the top 10 countries are shown in tandem with their detected virus families.

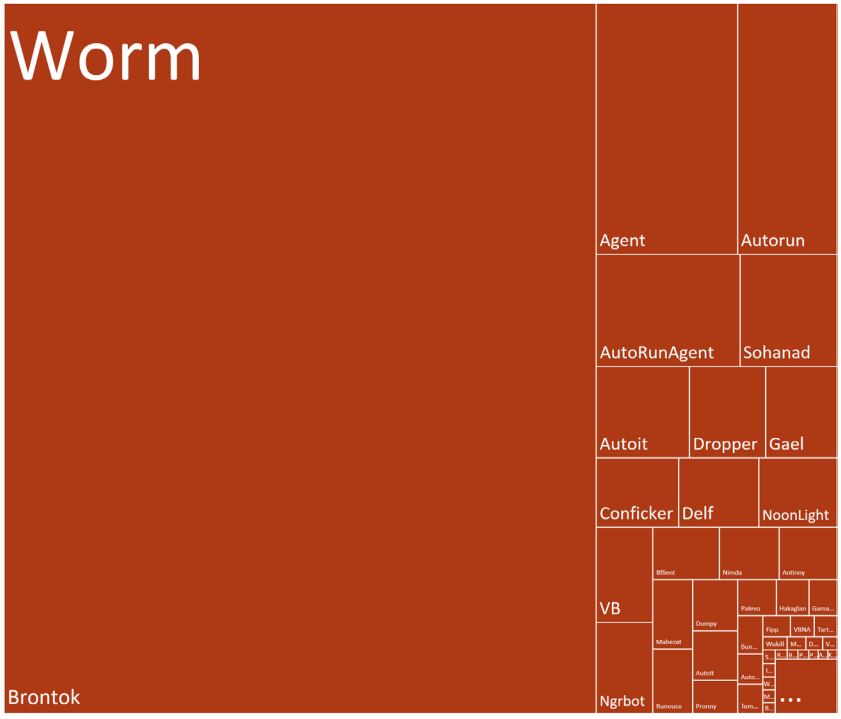
There is a clear difference between trojan and virus infections, with particular viruses primarily afflicting particular nations. While Brazil has been inundated with Sality, Taiwan is struggling almost exclusively with Ramnit. Turkey, unfortunately, has both. And Russia has its own unique battle with Expiro.



Worm

A computer worm is like a virus, but typically travels autonomously, exploiting vulnerabilities in network defenses as it spreads across the internet. A worm is usually designed as a vehicle that delivers a malicious payload to a victim computer. However, even worms without a payload can consume enormous bandwidth, diminish network or local system resources, and possibly cause a denial-of-service.

The treemap below displays the most common worm families that Comodo detected in Q3 2017.

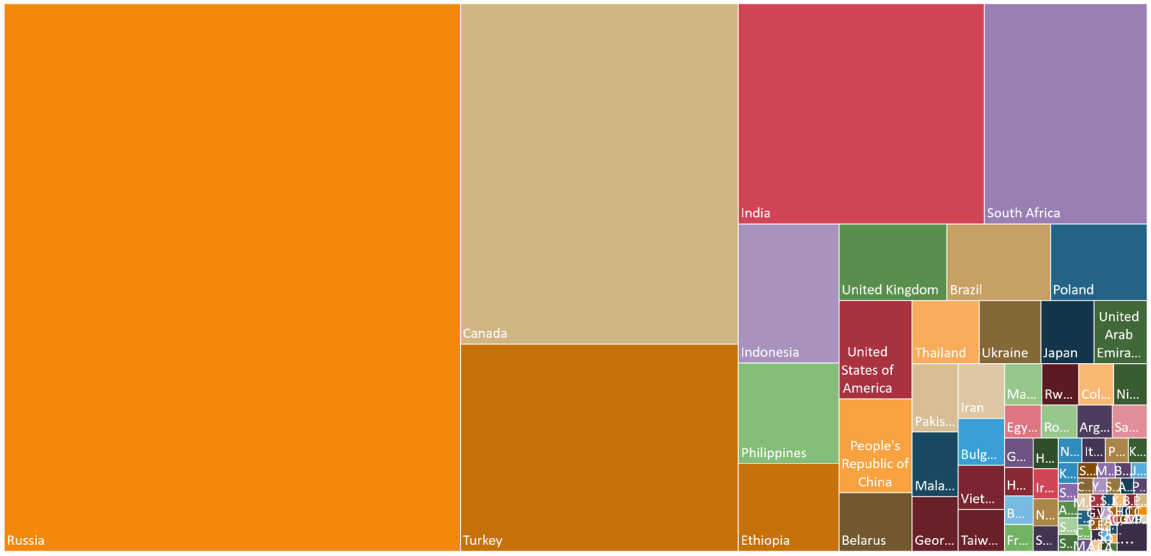


The worm category is a bit more complex than computer viruses, but has been dominated by one worm in particular: Brontok, a Microsoft Windows-based worm that spreads via email. It has its own email engine and sends itself to email addresses found on a victimized computer, spoofing the victim's email 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.

The table below shows the top 10 worm families, raw detection counts, and percentages of the total (2,837,745).

Top 10 Worm Families	Raw Detection Counts	Percentage of Total
Brontok	2,017,851	71.1%
Agent	170,118	6.0%
Autorun	119,735	4.2%
AutoRunAgent	77,190	2.7%
Sohanad	52,128	1.8%
Autoit	40,960	1.4%
Dropper	33,473	1.2%
Gael	31,293	1.1%
Conficker	27,516	1.0%
Delf	26,808	0.9%

Here is a treemap of the countries in which Comodo detected worms in Q3 2017:

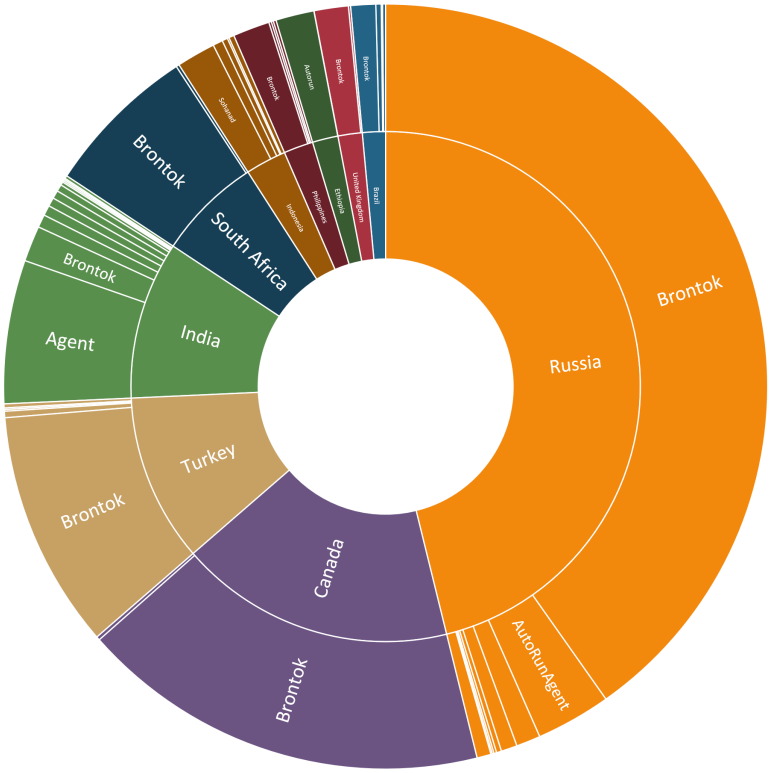


Comodo detected 1,091 unique worm families within 183 country codes. Russia, Canada, and Turkey were the top three victim nations. The table below shows the top 10 countries, their raw numbers, and percentages.

Top 10 Worm Countries	Raw Detection Counts	Percentage of Total
Russia	1,119,135	39.4%
Canada	424,171	14.9%
Turkey	257,986	9.1%
India	242,610	8.5%
South Africa	160,540	5.7%
Indonesia	62,867	2.2%
Philippines	45,361	1.6%
Ethiopia	39,538	1.4%
United Kingdom	37,287	1.3%
Brazil	35,564	1.3%

In the sunburst chart below, the top ten countries are shown in tandem with their detected worm families.

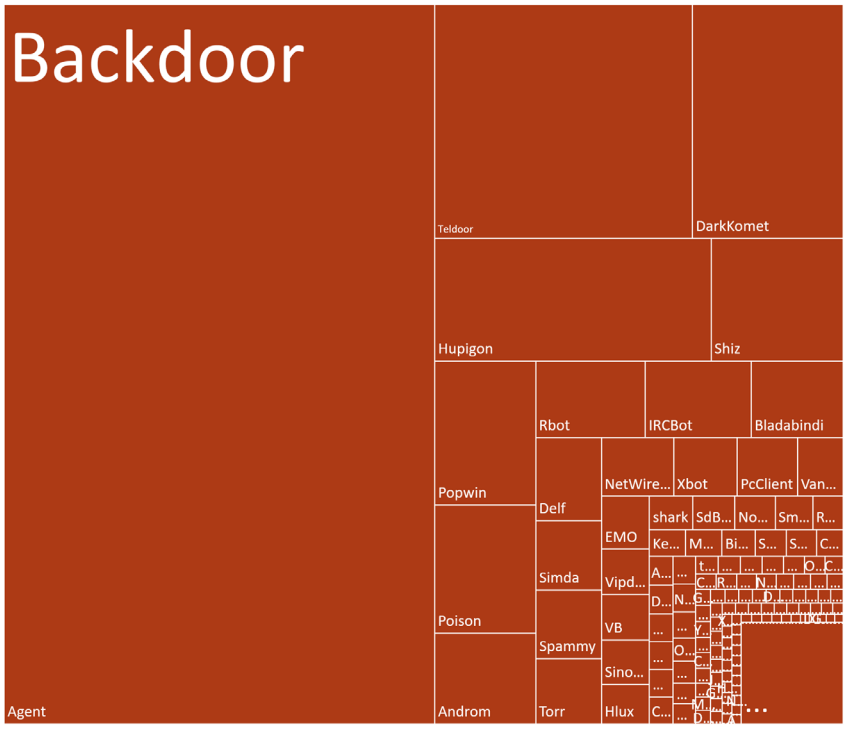
This chart confirms that Brontok is the world's No. 1 worm threat. It occupies a near-exclusive dominance of many countries, including Russia, Canada, Turkey, South Africa, Philippines, United Kingdom, and Brazil.



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 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.

The treemap below displays the most common backdoor families that Comodo detected in Q3 2017.

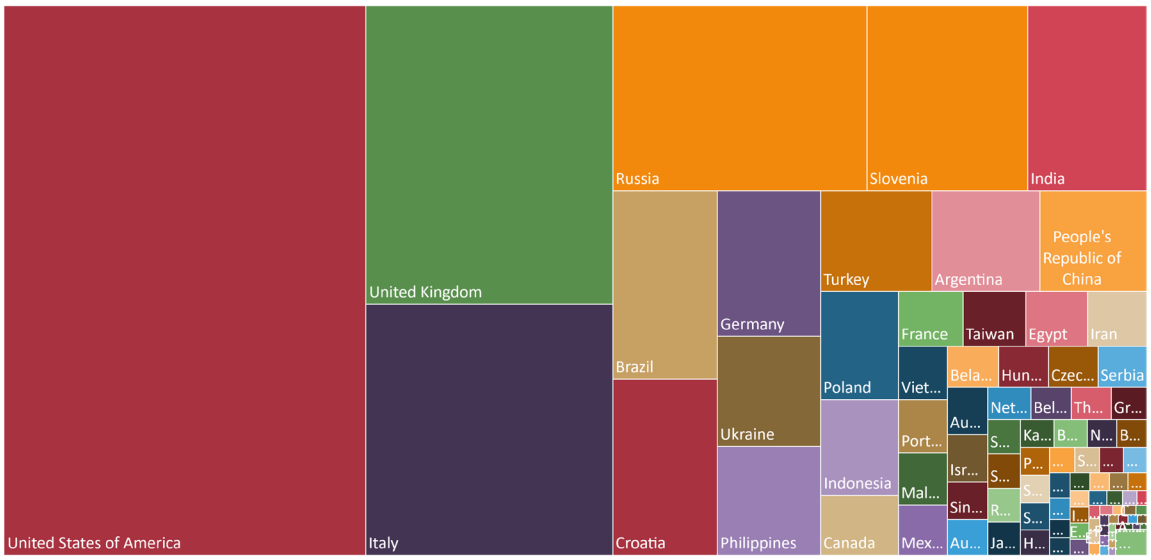


The backdoor category is far more complex than viruses or worms, with the top threat, "Agent," a generic set of backdoor characteristics that further highlights the difficulty of precisely understanding this malware type.

The table below shows the top 10 backdoor families, raw detection counts, and percentages of the total (553,257).

Top 10 Backdoor Families	Raw Detection Counts	Percentage of Total
Agent	283,858	51.3%
Teldoor	55,250	10.0%
DarkKomet	32,359	5.8%
Hupigon	31,072	5.6%
Shiz	14,834	2.7%
Popwin	13,334	2.4%
Poison	11,901	2.2%
Androm	8,409	1.5%
Rbot	7,693	1.4%
IRCBot	7,429	1.3%

Here is a treemap of the countries in which Comodo detected backdoors in Q3 2017:

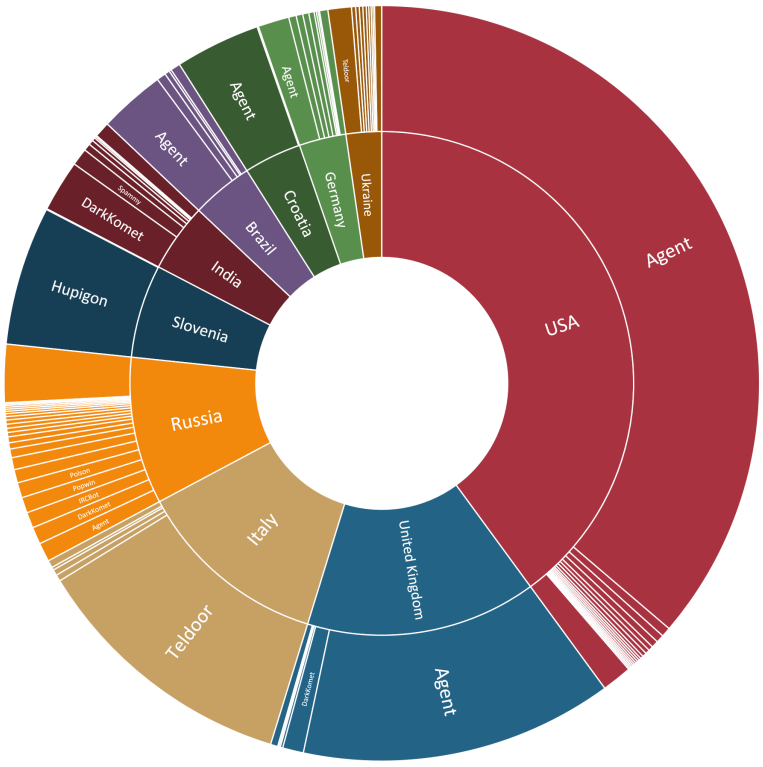


In Q3 2017, Comodo detected 1,567 unique backdoor families within 167 country codes. The first thing to notice is a different nation at the top: the U.S., with the U.K. and Italy second and third, respectively.

The table below shows the top 10 countries, their raw numbers, and percentages.

Top 10 Backdoor Countries	Raw Detection Counts	Percentage of Total
U.S.	170,122	30.7%
UK	63,062	11.4%
Italy	53,063	9.6%
Russia	40,233	7.3%
Slovenia	25,485	4.6%
India	18,738	3.4%
Brazil	16,842	3.0%
Croatia	15,756	2.8%
Germany	12,840	2.3%
Ukraine	9,731	1.8%

In the sunburst chart below, the top 10 countries are shown in tandem with their detected worm families.



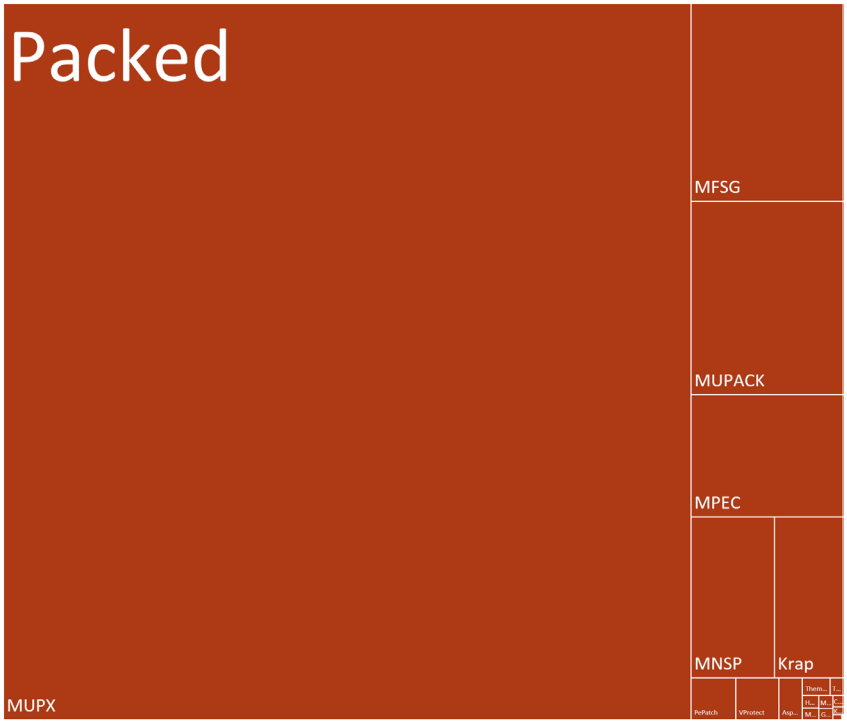
Some nations, like Italy, have a clear backdoor threat, such as Teldoor. Slovenia has Hupigon. India has Dark Komet. Russia, as usual, has an unusually high number of threats to worry about. But the U.S. and U.K., as well as Brazil, Croatia, and Germany, not only have many backdoors, but also suffer a top detection of "Agent", or a generic set of trojan characteristics and functionality that are hard

to classify precisely. What this means is that cyber defense researchers in these countries face a multifaceted threat that is constantly evolving and staying one step ahead of network security specialists.

Packed

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.

The treemap below displays the most common malware packers that Comodo detected in Q3 2017.

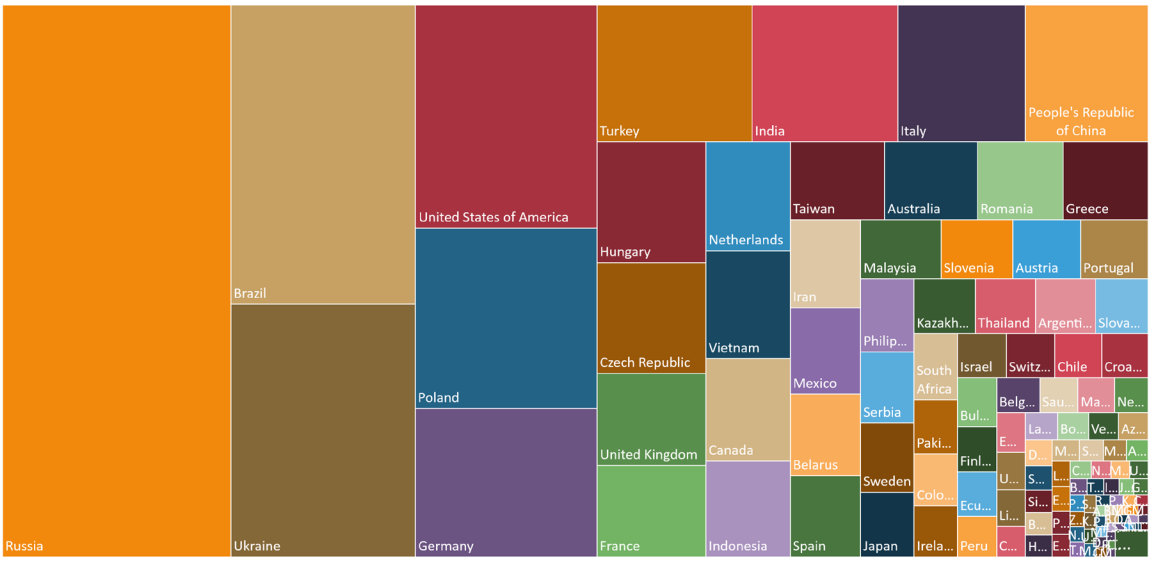


Our final top 5 threat, the malware packer category, is simpler from an analytical perspective, with MUPX dominating the landscape.

The table below shows the top 10 packer families, raw detection counts, and percentages of the total (384,214).

Top 10 Packer Families	Raw Detection Counts	Percentage of Total
MUPX	314,646	81.9%
MFSG	19,182	5.0%
MUPACK	18,797	4.9%
MPEC	11,877	3.1%
MNSP	8,582	2.2%
Krap	7,046	1.8%
PePatch	1,205	0.3%
VProtect	1,161	0.3%
Aspack	621	0.2%
Themida	321	0.1%

Here is a treemap of the countries in which Comodo detected malware packers in Q3 2017:



Comodo detected 19 unique backdoor families within 174 country codes. Russia is back at the top, with Brazil, Ukraine, U.S., and Poland rounding out the top five.

The table below shows the top 10 countries, their raw numbers, and percentages.

Top 10 Backdoor Countries	Raw Detection Counts	Percentage of Total
Russia	74,929	19.5%
Brazil	32,796	8.5%
Ukraine	27,726	7.2%
U.S.	24,095	6.3%
Poland	19,487	5.1%
Germany	16,046	4.2%
Turkey	12,619	3.3%
India	11,830	3.1%
Italy	10,361	2.7%
China	9,983	2.6%

In the sunburst chart below, the top 10 countries are shown in tandem with their detected malware packer families.

There is no doubt what the top malware packer is, both internationally and within every nation in our top ten. 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.

Global Analysis

Introduction

The internet has provided the world with many benefits, including high-speed global communication, information sharing, online education, and much more. However, this report shows that worldwide connectivity has also brought some worldwide vulnerability. There is only one internet and one cyberspace, which we are all in together, for good and for ill. Cybercriminals and spies have sought to undermine the long-term confidentiality, integrity, and availability of the internet for short-term gain.

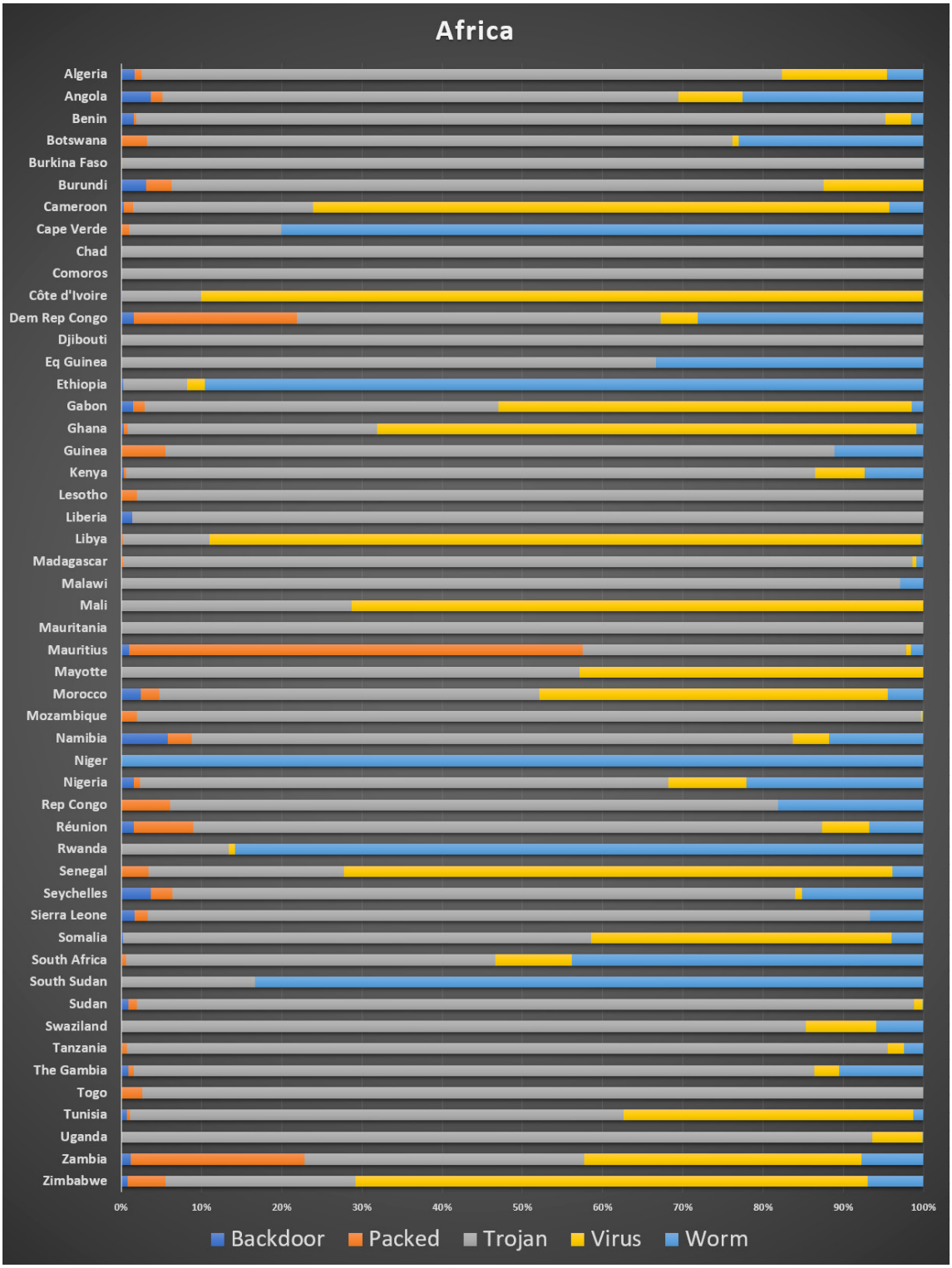
Over the past 20 years, law enforcement and counterintelligence agencies have made great progress in understanding and investigating cyber incidents, but the fact remains that national sovereignty and law enforcement jurisdiction are limited by traditional international borders. In fact, cybercrime has recently taken a turn for the worse, with nation-states like North Korea using cybercrime such as ransomware as a way to make money. WannaCry, for example, proved that the barriers to entry on the cyber battlefield have fallen, and that the line between cybercrime and cyber espionage is increasingly blurry.

However, this report also highlights something even more important: cyberattacks can be analyzed at the strategic level, and the resulting intelligence can be used to improve network defenses, from the international, to the national, and even the tactical levels. In other words, seeing how you, your enterprise, and your nation fit into cybersecurity's "big picture" can save you a lot of time and resources by helping you to focus on the most pressing threats prevalent in your part of the world. Like a fingerprint, every part of the global information space has a unique malware profile.

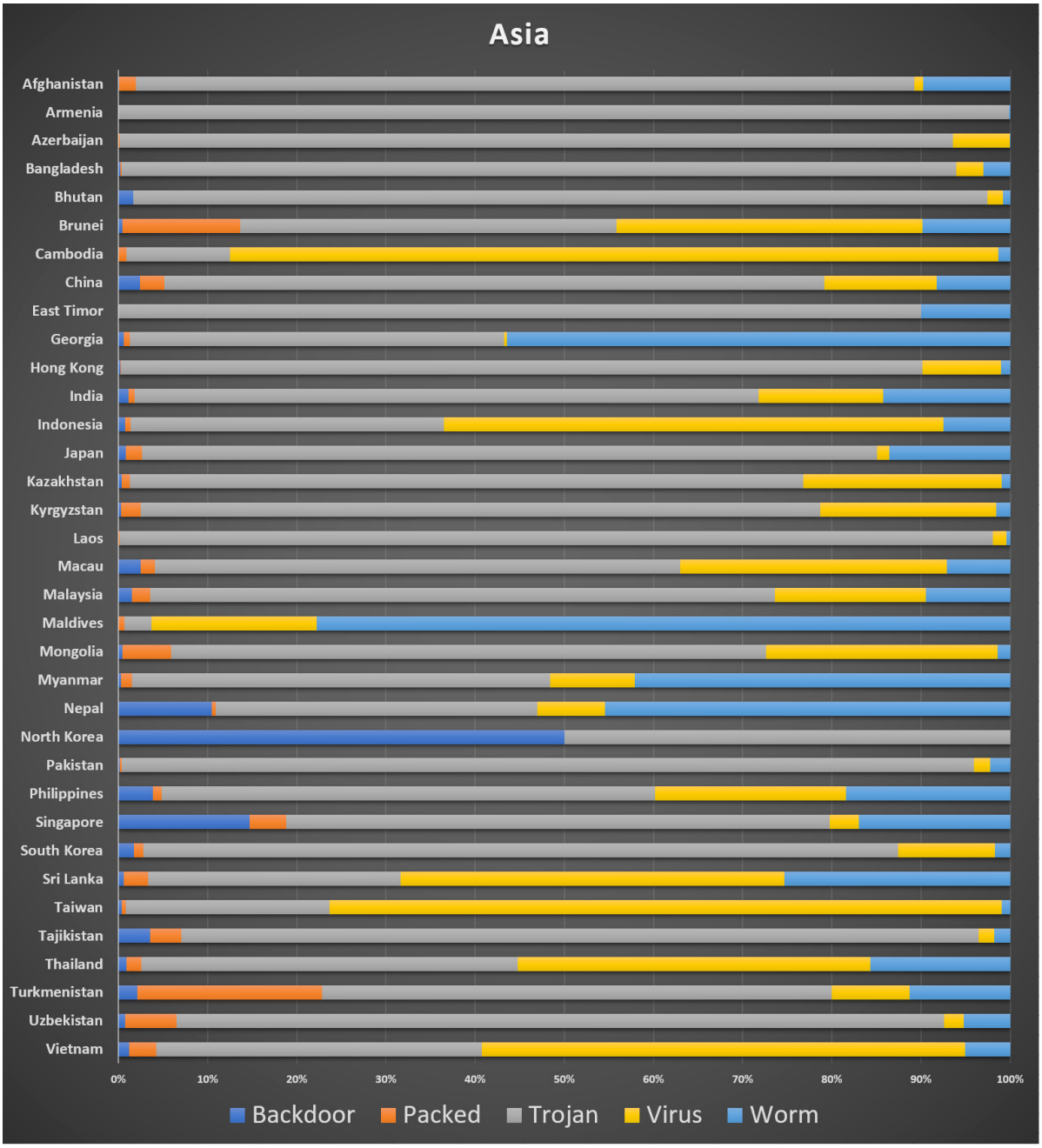
In this final section of the Comodo Q3 2017 report, we are able to show the incredible global visibility that nearly 20 years of building internet infrastructure affords our company. Here, we can show a current malware profile for every nation on Planet Earth, which can help local cyber defenders to better understand the nature of the threat they face, as well as how to better mitigate ongoing cyberattacks.

These charts only hint at the vast size and diversity of national network spaces. All of them are unique, but there are certain high-level characteristics and trends to watch out for. A prevalence of backdoors, for example, suggests a high degree of targeted attacks. A high ratio of viruses and worms often suggests that economic challenges, including the use of older, unlicensed, unsupported, or pirated software may be the cause.

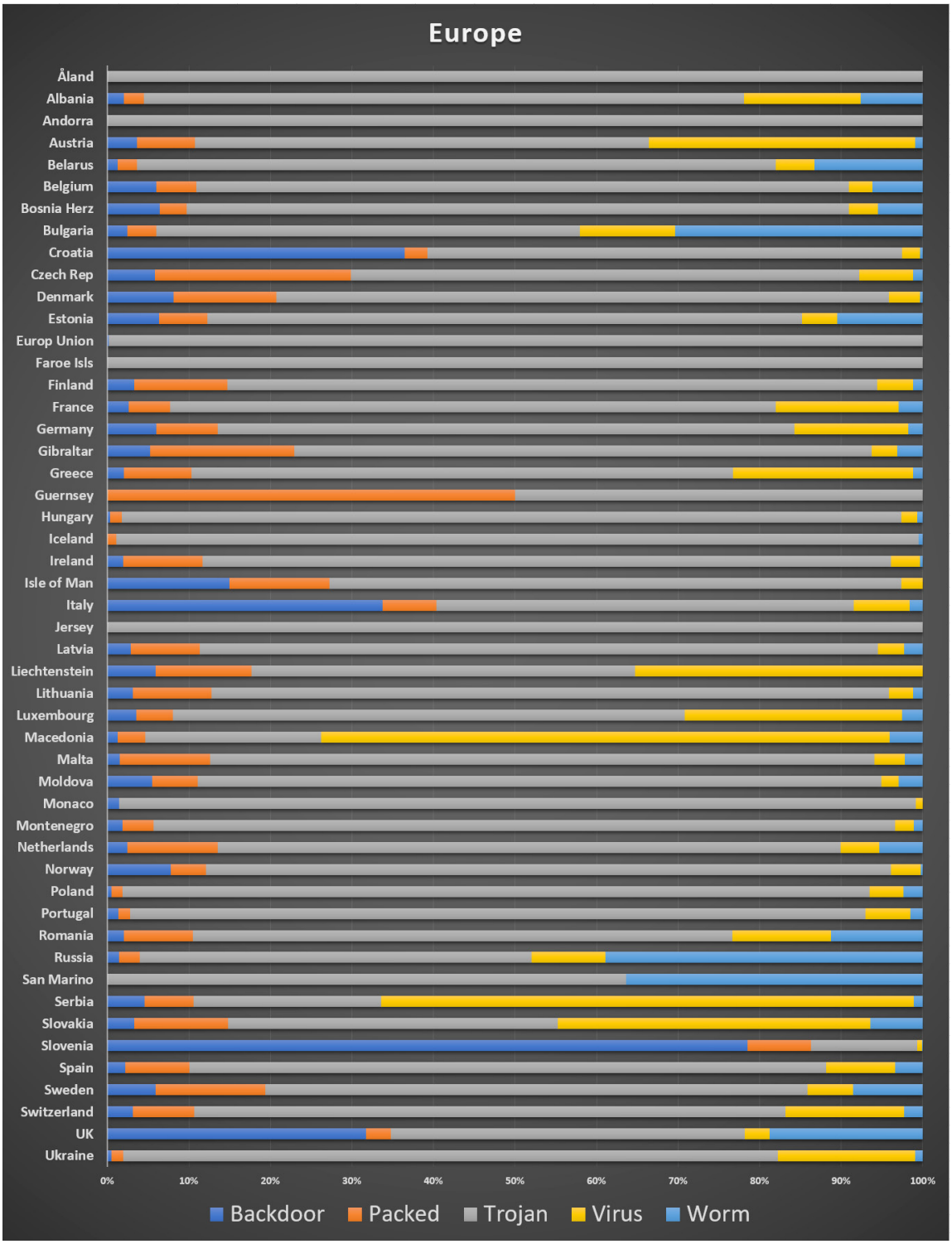
Africa Malware Profile



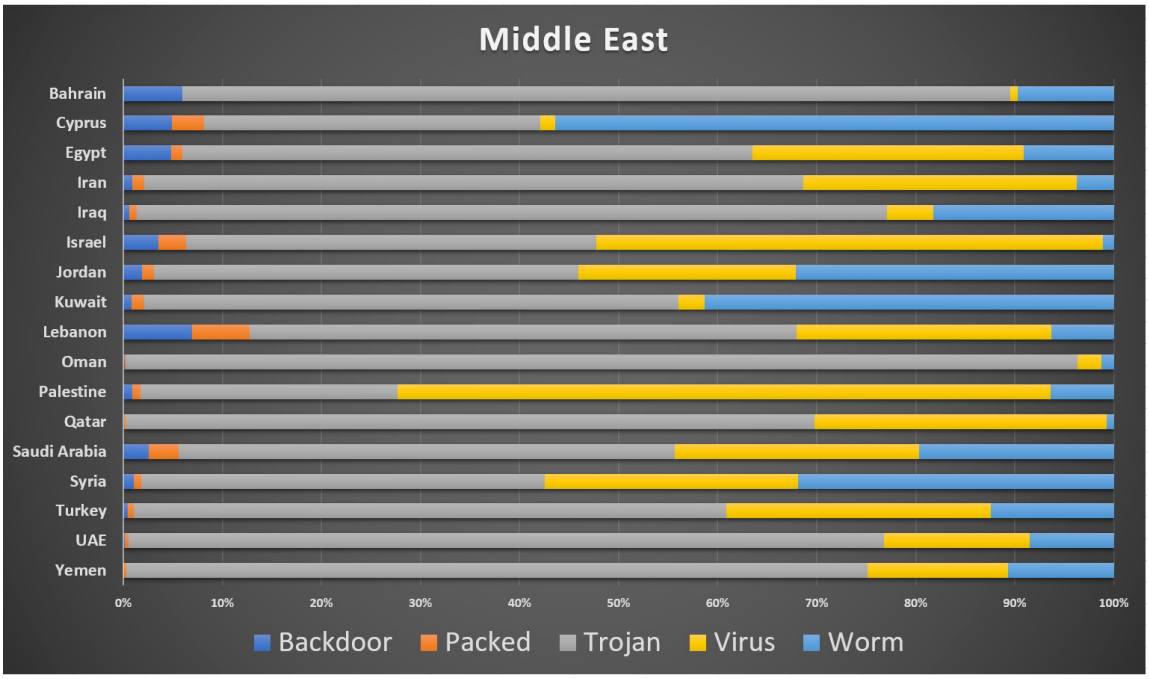
Asia Malware Profile



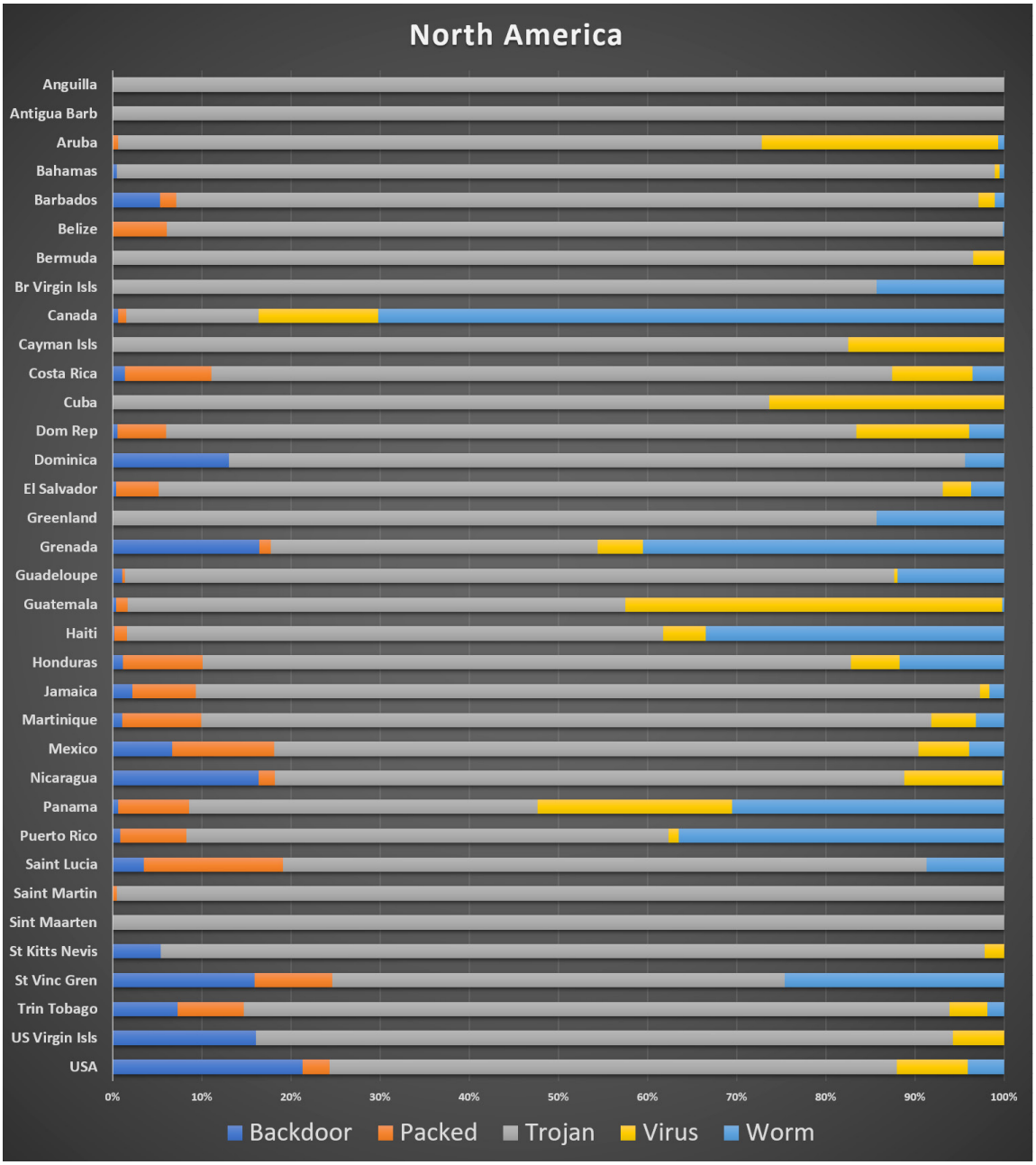
Europe Malware Profile



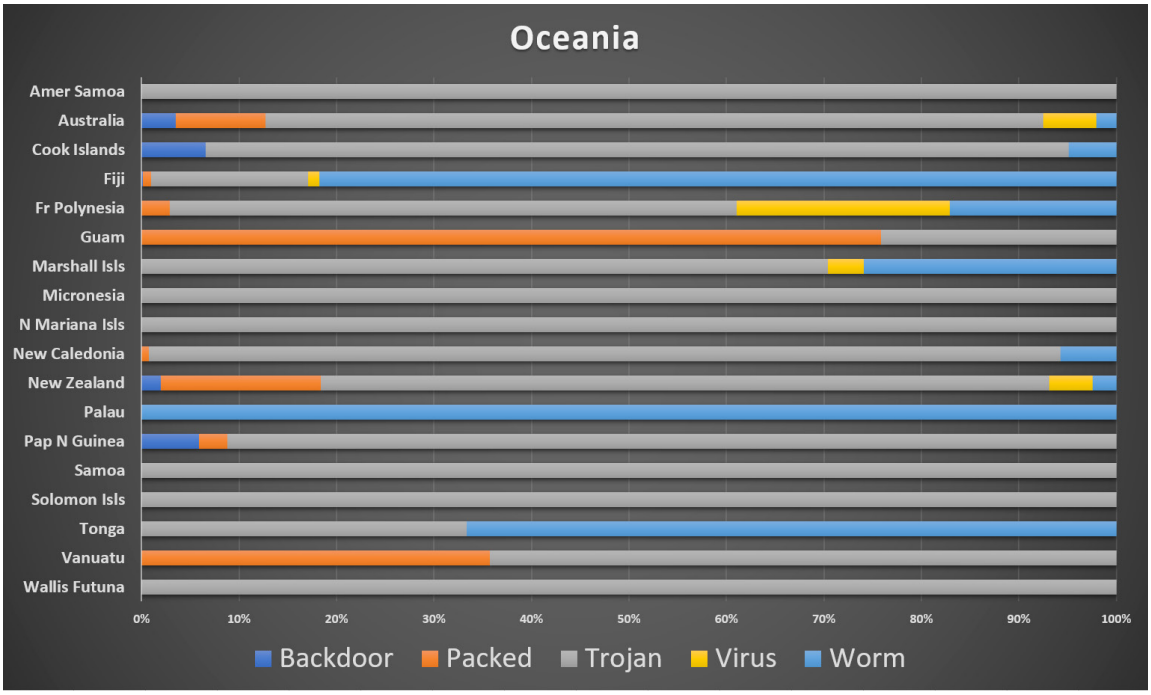
Middle East Malware Profile



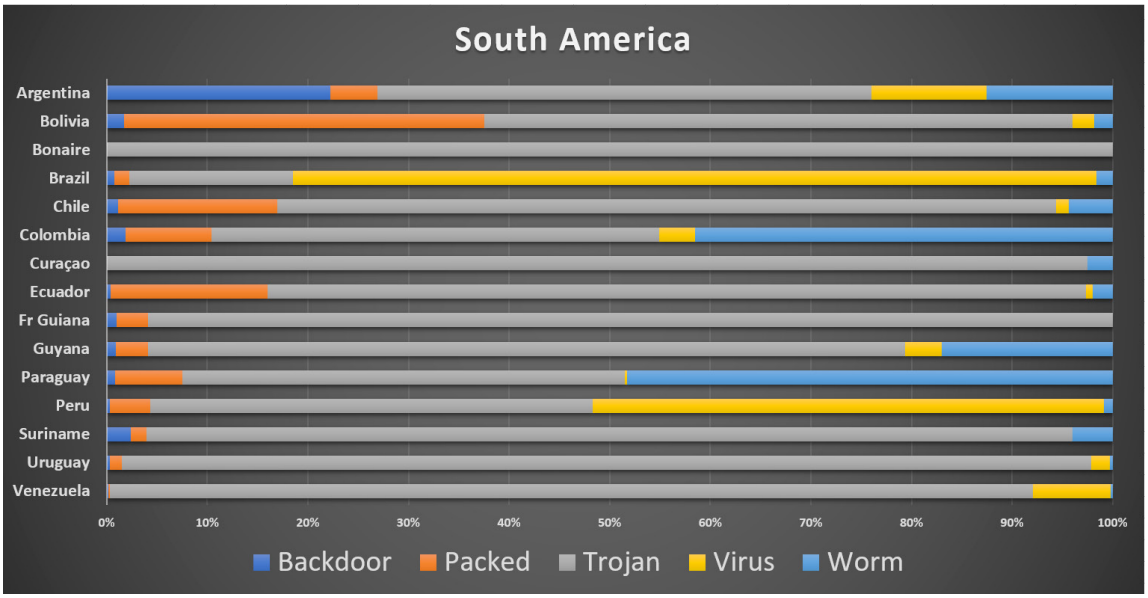
North America Malware Profile



Oceania Malware Profile



South America Malware Profile

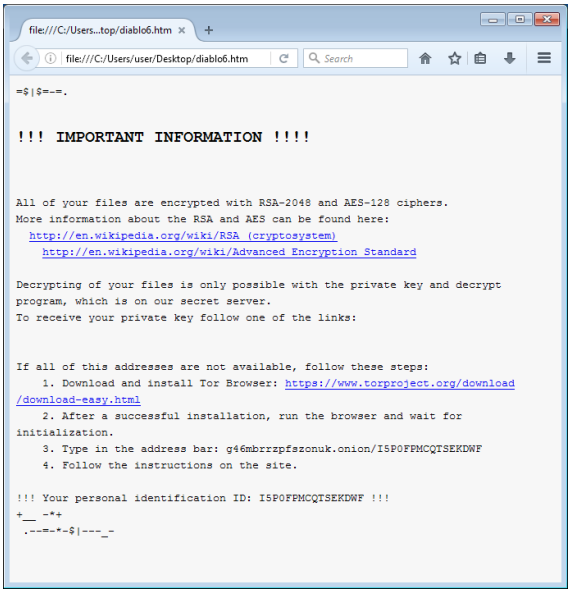


New Sophisticated Phishing Attacks

Introduction

The Comodo Threat Intelligence Lab first discovered a number of new, large-scale, global email-based phishing campaigns during the quarter. The first of the quarter cleverly simulated a package delivery tracking inquiry and three later attacks were also sophisticated in design, extremely targeted, and clearly related to the infamous "Locky" Trojan malware. Each delivered a ransomware payload and were very destructive. Each also hit endpoints as an 'unknown' file and was immediately auto-contained for analysis by the Lab.

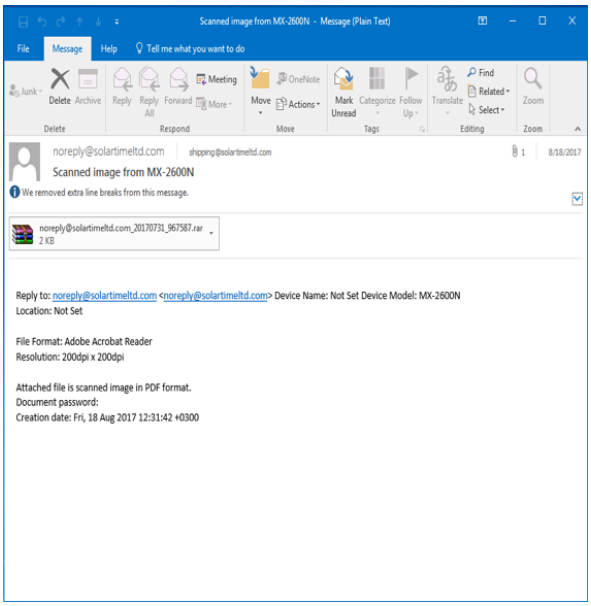
Most prominent this quarter was a series of three campaigns named "IKARUSdilapidated" by the Lab, for that text in the code string. The first wave of the IKARUS attacks began on Aug. 9, delivering a simple-looking email with an attachment and little to no content in the email body. The attached file names were similar, and used different but familiar extensions – doc, zip, pdf, jpg, or tiff.



Social engineering was used to get the user to click, and when the user does as instructed, the macros then save and run a binary file that downloads the actual encryption Trojan, which will encrypt all files that match particular extensions, including the common ones on most machines. After encryption, a message displayed on the user's desktop instructs them to download the 'Tor' browser, which is popular because it allows for anonymous browsing, and to then visit a specific criminally-operated website for further information. The website contained instructions that demanded a ransom payment of between 0.5 and 1 bitcoin, which was as much as $4,000 during the quarter, to (hopefully) decrypt their now-encrypted files.

Even the first of these IKARUS Locky campaigns showed the increasing sophistication, organization, and size of new ransomware attacks according to Fatih Orhan, head of the Comodo Threat Intelligence Lab and Comodo Threat Research Labs (CTRL).

See below for the subject line that looks familiar to so many office workers.



"This attack was unique in its combination of sophistication and size, backed by a botnet spread across more than 11,000 IP addresses in 133 countries in just the first stage of the attack. Also, the malware was designed to avoid detection by sandboxing and artificial intelligence technologies common in many **endpoint protection** systems." said Orhan.

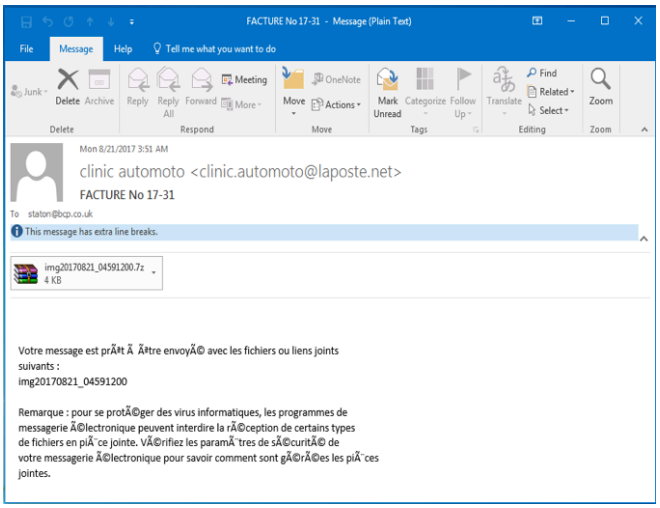
When Comodo-protected endpoints couldn't identify these unknown files, the full resources of the lab were needed to analyze and identify the code in the file and render a verdict. In this case, the verdict was "bad" and the auto-containment protected the endpoints from infection even before the new variants were added to blacklists and malware signature lists.

"The techniques used to defeat sandboxing, machine learning, and other security technologies in these campaigns shows how relentlessly attackers look for new ways to avoid detection. And the rapid cadence of new variants shows how hard they work to perfect and capitalize on successful new methods. These facts underscore that the only way to protect against new malware is to adopt a default deny security posture that denies new, 'unknown' files any access to device and IT infrastructures resources until it is fully evaluated. And in this case, it required senior security analysts to uncover that it was malware." said Orhan.

A second wave of new but related IKARUSdilapidated Locky ransomware attacks occurred later in August. The campaign also used a botnet of zombie computers to coordinate a phishing attack that sent emails appearing to be from an organization's scanner/printer, or other legitimate source, and ultimately encrypted the victims' computers and demanded a bitcoin ransom if they clicked on the attachment.

To better fool users, the second wave was, in fact, two different email campaigns launched three days apart, one featuring the subject "Scanned image from MX-2600N," a common scanner/printer model, and the second a French language email purportedly from the French post office with the subject "FACTURE," the French word for invoice or bill.

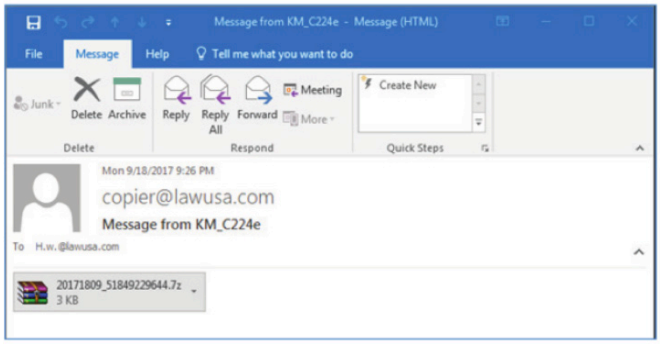
The Lab's analysis of emails sent in the "Scanned image" phishing campaign revealed the attack used 8,886 different IP addresses from 127 different country code top-level domains maintained by the Internet Assigned Numbers Authority (IANA). The narrower "FACTURE" attack utilized 1,657 different IP addresses from 74 country code domains.



As with the early August attacks, when the Lab team checked the IP range owners, most of them were telecom companies and ISPs. This confirmed that the IP addresses belong to infected, now compromised computers (also called "zombie computers").

This campaign used a large bot network (or botnet), and had a sophisticated command and control server architecture.

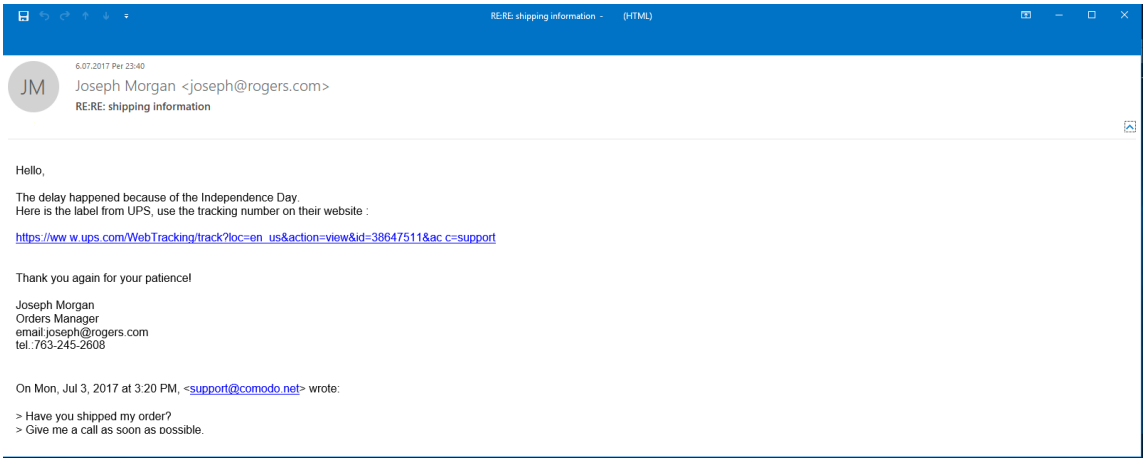
The third, similar IKARUSdilapidated Locky attack of the quarter in September featured either "Message from KM_C224e" or "Status of invoice" as the subject line. This campaign mimics your vendors and even your trusty office copier/scanner/printer from industry leader Konica Minolta. It uses social engineering to engage victims and is carefully designed to slip past machine learning algorithm-based tools from leading cybersecurity vendors, infect your machines, encrypt their data, and extract a bitcoin ransom.



This 3rd IKARUS wave of related 2017 ransomware attacks uses a botnet of zombie computers (usually connected to networks through well-known ISPs) to coordinate a phishing attack which sends the emails to victims' accounts. As with the 1st and 2nd waves, in early and late August 2017 respectively, this campaign utilizes a Locky ransomware payload and renders the infected machine completely useless.

The Lab's analysis of emails sent in the "Message from KM_C224e" phishing campaign revealed this attack data: 19,886 different IP addresses were used from 139 different country code top-level domains. The "Status of invoice" attack utilized 12,367 different IP addresses from 142 country code domains. There are a total of 255 top level country code domains maintained by the Internet Assigned Numbers Authority (IANA), meaning both of these new attacks targeted over half of the nation states on earth.

Another group of phishing campaigns showed how each month now brings more sophisticated versions.


RE:RE: shipping information - (HTML)

6.07.2017 Per 23:40

JM

Joseph Morgan <joseph@rogers.com>

RE:RE: shipping information

Hello,

The delay happened because of the Independence Day.
Here is the label from UPS, use the tracking number on their website :

https://ww w.ups.com/WebTracking/track?loc=en_us&action=view&id=38647511&ac c=support

Thank you again for your patience!

Joseph Morgan
Orders Manager
email:joseph@rogers.com
tel.:763-245-2608

On Mon, Jul 3, 2017 at 3:20 PM, <support@comodo.net> wrote:

> Have you shipped my order?
> Give me a call as soon as possible.

In each IKARUS Locky attack, the targeting was more evident and the social engineering was improving. Back in July 2017, the Lab had identified a new series of unrelated phishing emails that purported to be replies to previously asked requests for information from well-known brands and likely legitimate contacts. If you've tracked a package or status of an order for anything in recent times, you'll recognize the format. These emails contained links to illegitimate sites and malware payloads, and cleverly attempted to get the user to click on them.

Hundreds of different servers were used for this phishing campaign as it attacked more than 3,000 users at 50 enterprise customers. All the emails were sent in a short time, in less than seven hours, from a total of 585 different servers, 513 of which were in the United States.

Most definitely an advance in phishing attack sophistication, this illustrated the speed in which coordinated, multi-server attacks on businesses are being developed and deployed. With enterprise customers in this case and others profiled here, only the ones with a "default deny" security posture, which blocked or auto-contained any new, unknown files and code, were completely safe.

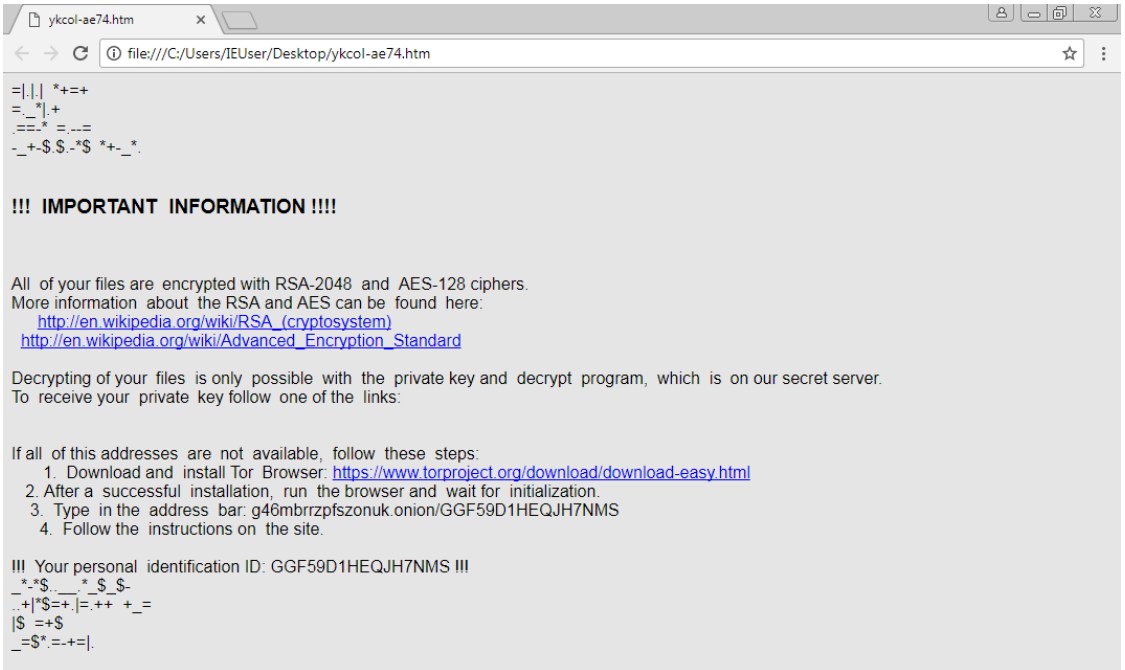
Now we'll dig into the data more deeply to see commonalities and differences.

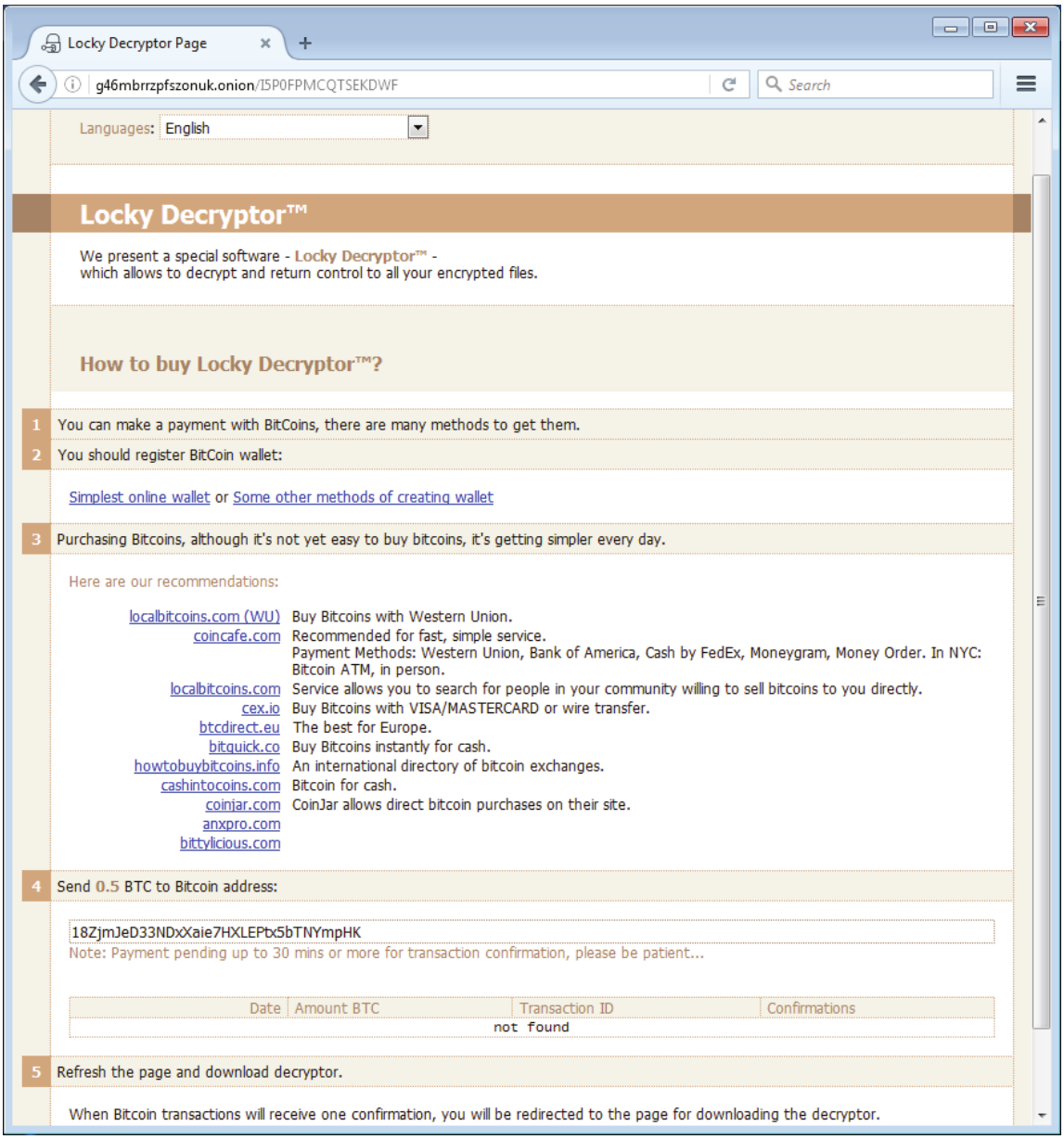
Common Features of the August/September Campaigns

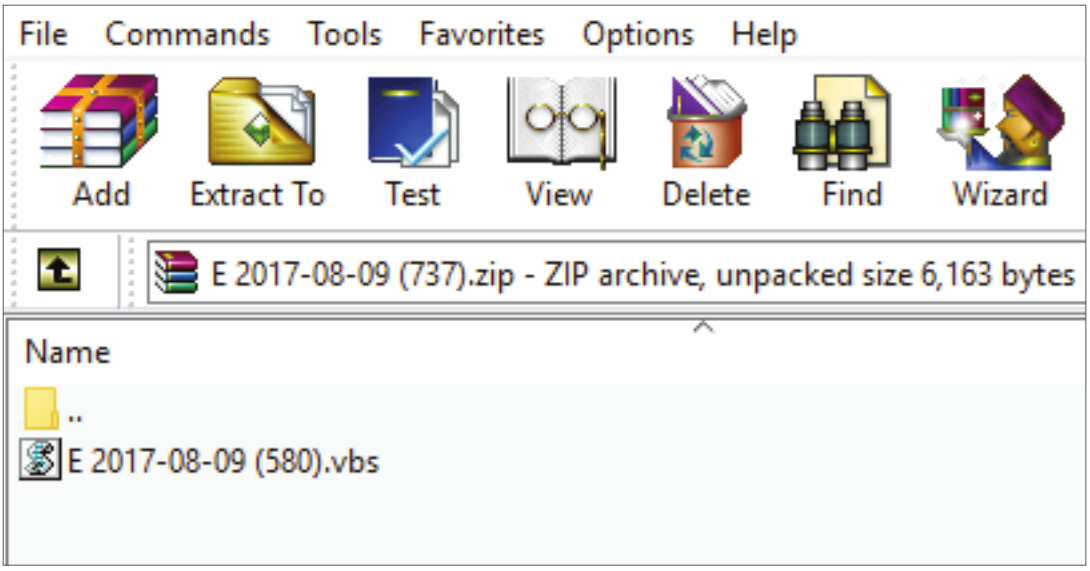
Use Locky Ransomware as the Malware Payload

```
=$|$=-=.~
          !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:


If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: g46mbrrzpfszonuk.onion/I5P0FPMCQTSEKDWF
    4. Follow the instructions on the site.

!!! Your personal identification ID: I5P0FPMCQTSEKDWF !!!
+__~-*+
~.--=-*-$|---_-
```

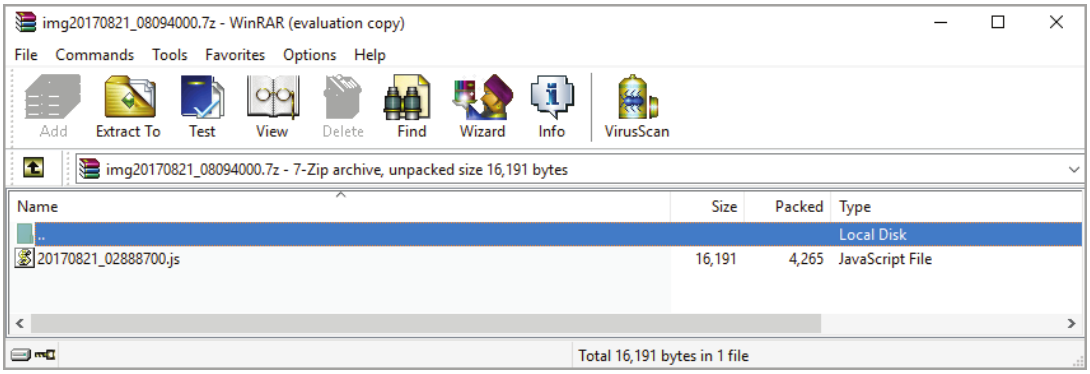
All three attacks are different, but ultimately are using the same Locky ransomware.

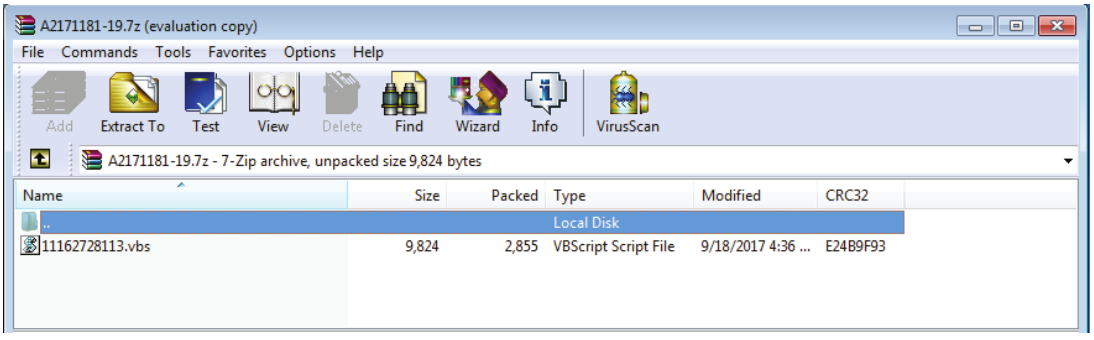



Locky Decryptor Page
g46mbrrzpfszonuk.onion/15P0FPMCQTSEKDWF
Search
Languages: English
Locky Decryptor™
We present a special software - Locky Decryptor™ -
which allows to decrypt and return control to all your encrypted files.
How to buy Locky Decryptor™?
1 You can make a payment with BitCoins, there are many methods to get them.
2 You should register BitCoin wallet:
Simplest online wallet or Some other methods of creating wallet
3 Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
localbitcoins.com (WU) Buy Bitcoins with Western Union.
coincafe.com Recommended for fast, simple service.
Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
localbitcoins.com Service allows you to search for people in your community willing to sell bitcoins to you directly.
cex.io Buy Bitcoins with VISA/MASTERCARD or wire transfer.
btcdirect.eu The best for Europe.
bitquick.co Buy Bitcoins instantly for cash.
howtobuybitcoins.info An international directory of bitcoin exchanges.
cashintocoins.com Bitcoin for cash.
coinjar.com CoinJar allows direct bitcoin purchases on their site.
anxpro.com
bittylicious.com
4 Send 0.5 BTC to Bitcoin address:
18ZjmJeD33NDxXaie7HXLEPtx5bTNYmpHK
Note: Payment pending up to 30 mins or more for transaction confirmation, please be patient...
Date
Amount BTC
Transaction ID
Confirmations
not found
5 Refresh the page and download decryptor.
When Bitcoin transactions will receive one confirmation, you will be redirected to the page for downloading the decryptor.



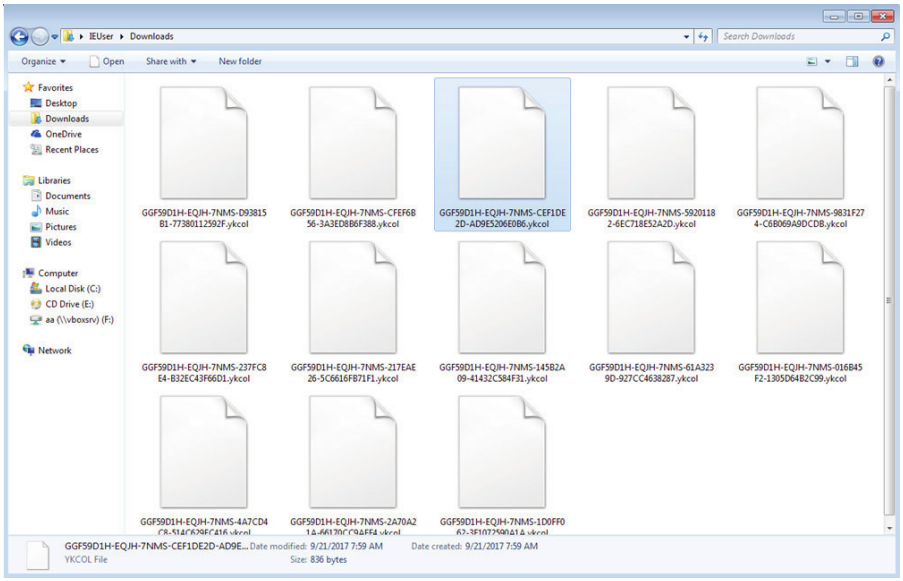
When the attachment is clicked, it appears as a compressed file to be unpacked:





Unique Elements

In contrast to the initial 2017 IKARUSdilapidated Locky campaign (which distributed malware with the ".diablo" extension and a Visual Basic Script (and has a ".vbs" extension)), and the 2nd later in August in which the ".lukitus" extension via JavaScript files were used, the September attacks have interesting variations aimed to not only fool users with social engineering, but also to fool security administrators and their machine learning algorithms and signature-based tools.



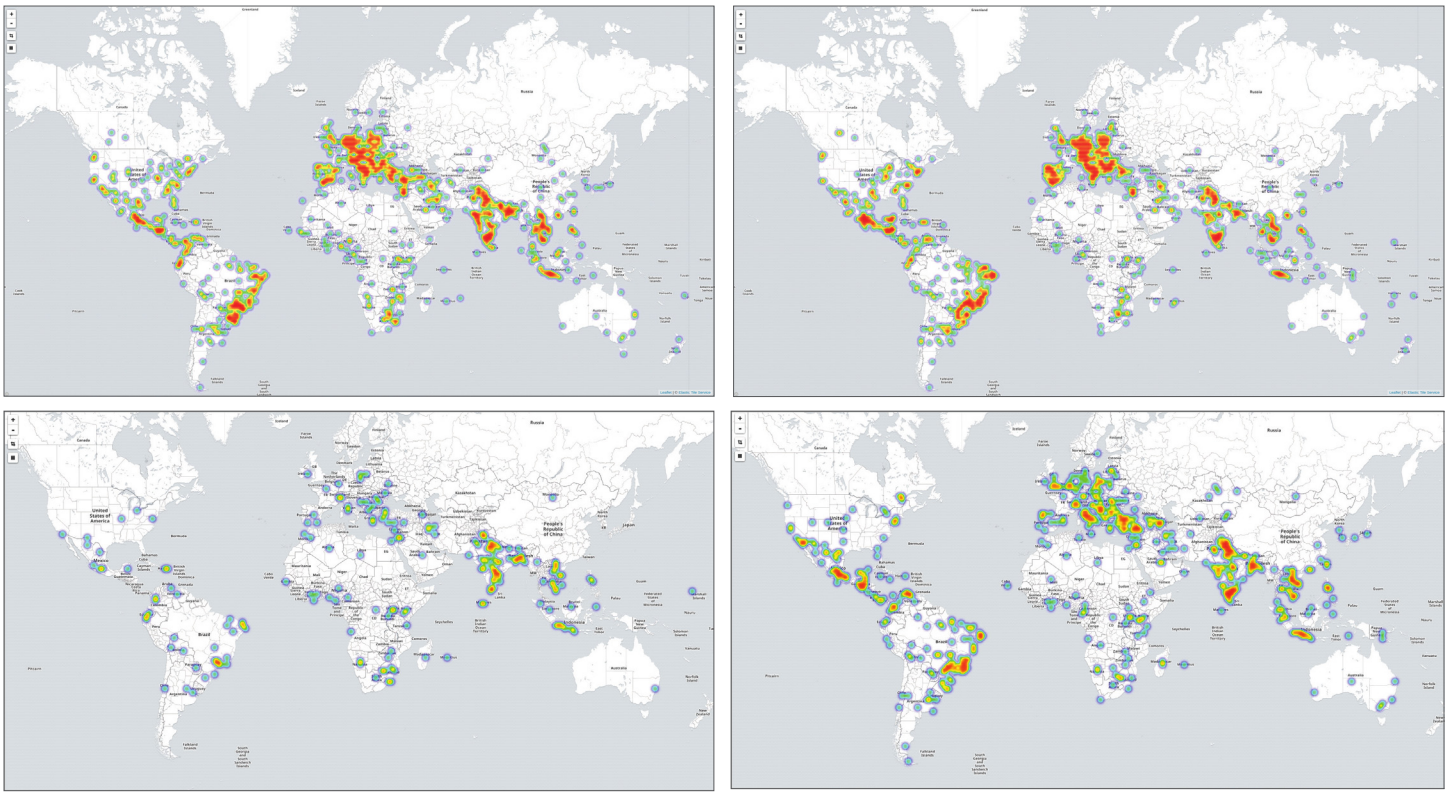
The encrypted documents in the September attacks have a ".ykcol" extension and the ".vbs" files are distributed via email. This shows that malware authors are developing and changing methods to reach more users and bypass security approaches that use machine learning and pattern recognition.

```
var line5HO = SmthngWrngfrankfurt_FROG2sud(line5);
WScript.echo("Error opening file (CODE:" +line5HO+")");

    for (velVITK_OBLOM= 0; line5HO >velVITK_OBLOM ; ++velVITK_OBLOM) {
      line5[velVITK_OBLOM] = -29+line5[velVITK_OBLOM] - 1;

    }

    var turkish;
var velVITK_BOSKO_2S = "";

var ratatu = "prot"+"otype";

function TortPankaky(ReebokGalaxyFROGvostochniy){
    ReebokGalaxyFROGtaliluev = ReebokGalaxyFROGvostochniy;
for (var ReebokGalaxyFROG2XCOP in turkish){ReebokGalaxyFROGtaliluev = ReebokGalaxyFROGtaliluev["repl" + "ace"](ReebokGalaxyFROG2XCOP,
turkish[ReebokGalaxyFROG2XCOP]);}
    return ReebokGalaxyFROGtaliluev;
};


 String[ratatu].HIDEMYASS = function() {
       var SmthngWrngfrankfurt_RazlomSS, line4, SmthngWrngfrankfurt_Selection1, SmthngWrngfrankfurt_FROG2c4;

    var SmthngWrngfrankfurt_FROG2out = "";

    var line3= this.replace(/PARTITI/gi, SmthngWrngfrankfurt_FROG2out);line6 = 0;
var  SmthngWrngfrankfurt_FROG21en = SmthngWrngfrankfurt_FROG2sud(line3);

while (line6 < SmthngWrngfrankfurt_FROG21en) {


do {
            var SmthngWrngfrankfurt_koch = line3.charCodeAt(line6++) &(0x132- 0x33);
          SmthngWrngfrankfurt_RazlomSS = line5[SmthngWrngfrankfurt_koch];
       } while (line6 < SmthngWrngfrankfurt_FROG21en && SmthngWrngfrankfurt_RazlomSS == -1);
if (SmthngWrngfrankfurt_RazlomSS == -1)
          break;
    do {
              stembl = "the";
```

As you can see, there are some differences in the scripts of the attack.

```
Function CopyLog()

        Dim oFile
        Dim iRetVal, fptr1, fptr2, sLine, sNewLogFolderName, sLogFile
        Dim sComputer
        Dim sLog
        Dim sBootDrive



        ' Make sure the path is accessible
        oUtility.ValidateConnection oEnvironment.Item("SLShare")
        oUtility.VerifyPathExists oEnvironment.Item("SLShare")
        If not oFSO.FolderExists(oEnvironment.Item("SLShare")) then
            oLogging.CreateEntry "An invalid SLShare value of " & oEnvironment.Item("SLShare") & " was specified.", LogTypeWarning
            Exit Function
        End if


    End Function

Dim Lurkmoreexistedensurance 'As String
'Dim SagaOD() 'As String
Dim LurkmoreexistedUotOfStock 'As String

  LurkmoreexistedBelish = "User"
Function RobertBaration(a,b,c)
a.Write Chr(b  Xor c )
End Function
Function Set2Mine(Who, Color, X, y )
    Dim i
    For i = 0 To UBound(Mines) + 1
        If i > UBound(Mines) Then ReDim Preserve Mines(i)
        If Mines(i).Color = 0 Then
            Mines(i).Who = Who
            Mines(i).Color = Color
            Mines(i).X = X
            Mines(i).y = y
            Mines(i).Tick = 0
            SetMine = i
            Exit For
        End If
    Next
End Function

CUA ="Mozill"+"a/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0"

    RACHEL = "avetof"
```

Countries Sending the Most Emails During these Attacks

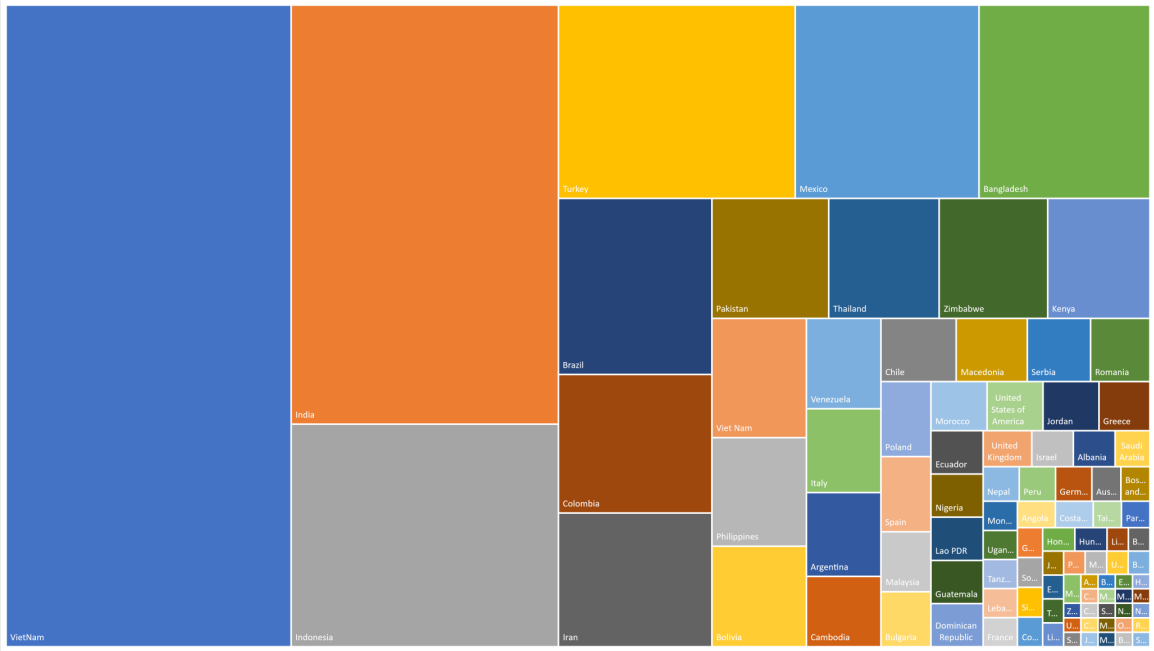


As reflected by the maps of the relevant attacks, countries that send the most e-mails are shown in the following table:

Countries Sending the Most Emails
Vietnam (VN)
India (IN)
Mexico (MX)
Indonesia (ID)

Country Information of Common IPs Participating in the Attack

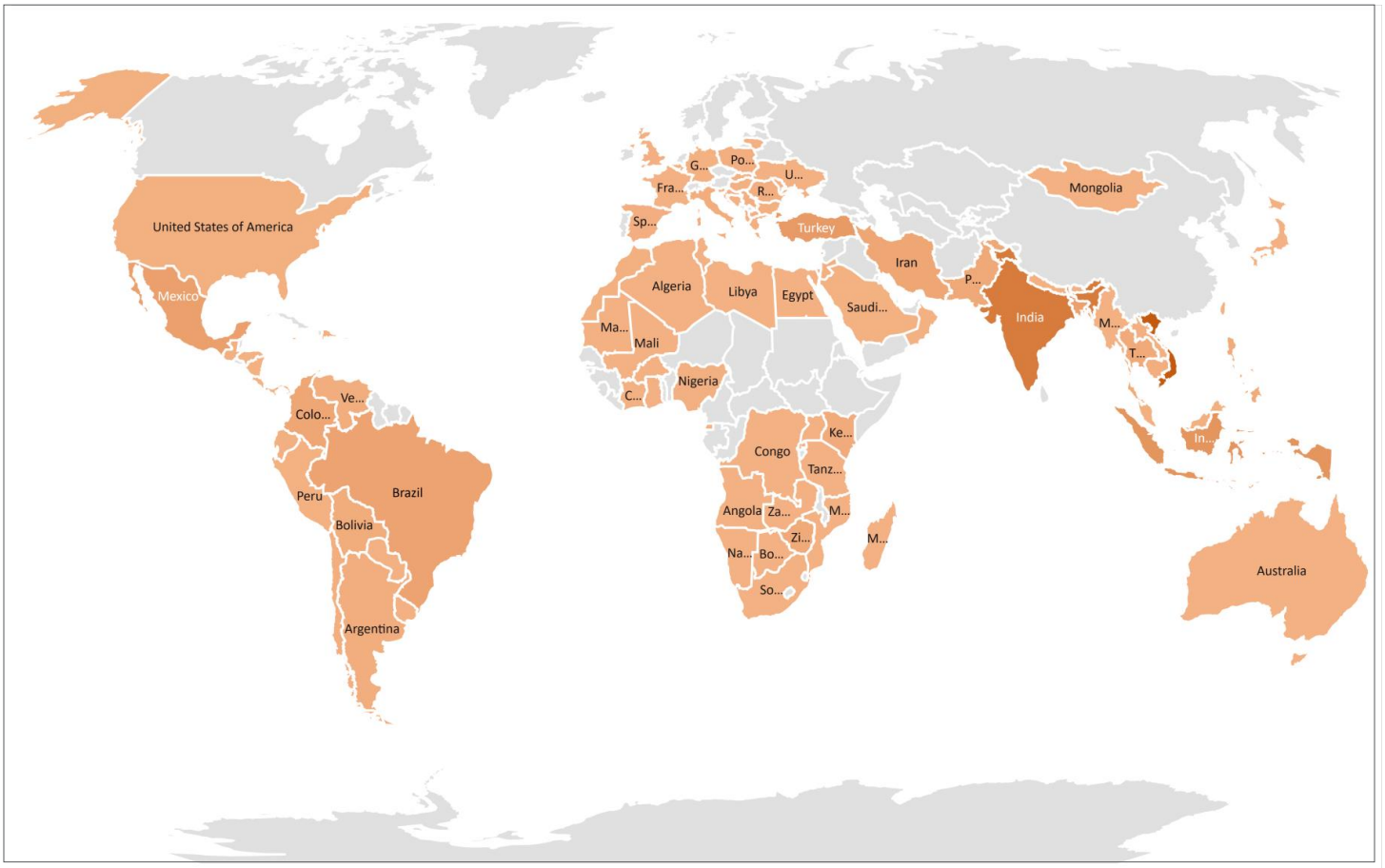
The following graphic shows the IPs organization and country information that participated in the attack. The common 2,934 IPs of all three attacks and the information of 95 different countries have been analyzed:



Up to 6 countries and organizations per IP:

Range Owners	Country	IP per Count
Vietnam Posts and Telecommunications (VNPT)	VN	553
Turk Telekom	TR	129
Airtel Broadband	IN	114
VDC	VN	74
Bharti Airtel	IN	68
Viettel Corporation	VN	53

Common IPs used for the three relevant attacks are shown in the map below:



The common 2,934 IP addresses of all three attacks and the 95 different country's information have been analyzed.

Country	Per IP Count	Country	Per IP Count
Vietnam	731	Uganda	4
India	448	Tanzania	4
Indonesia	238	Lebanon	4
Turkey	183	France	4
Mexico	142	Angola	4
Bangladesh	132	Costa Rica	4
Brazil	108	Taiwan	3
Colombia	85	Paraguay	3
Iran	82	Ghana	3
Pakistan	56	South Africa	3
Thailand	53	Singapore	3
Zimbabwe	52	Congo	3
Kenya	49	Honduras	3
Viet Nam	45	Hungary	3
Philippines	41	Libya	2
Bolivia	38	Belgium	2
Venezuela	27	Jamaica	2
Italy	25	Egypt	2
Argentina	25	Tunisia	2
Cambodia	21	Lithuania	2
Chile	19	Panama	2
Macedonia	18	Malta	2
Serbia	16	Ukraine	2
Romania	15	Bhutan	2
Poland	15	Mozambique	2
Spain	15	Zambia	1
Malaysia	12	Uruguay	1
Bulgaria	11	Slovenia	1
Morocco	11	Algeria	1
United States of America	11	Burkina Faso	1
Jordan	11	Equatorial Guinea	1
Greece	10	Hong Kong	1
Ecuador	9	Cyprus	1
Nigeria	9	Croatia	1
Lao PDR	9	Côte d'Ivoire	1
Guatemala	9	Japan	1
Dominican Republic	9	Madagascar	1
United Kingdom	7	Mali	1
Israel	6	Mauritania	1
Saudi Arabia	5	Slovakia	1
Nepal	5	Moldova	1
Peru	5	Myanmar	1
Albania	6	Namibia	1
Germany	5	Nicaragua	1
Australia	4	Oman	1
Bosnia and Herzegovina	4	Botswana	1
Mongolia	4	Rwanda	1
		Samoa	1
		Total Result	**2,934**

Organization Information of Top 20 Common IPs Participating in the Attack*

Range Owners Organization	Country	IP Per Count
Vietnam Posts and Telecommunications(VNPT)	VN	553
Turk Telekom	TR	129
Airtel Broadband	IN	114
VDC	VN	74
Bharti Airtel	IN	68
Viettel Corporation	VN	53
CMC Telecom Infrastructure Company	VN	51
True Internet	TH	34
Aamra Networks Limited	BD	34
Three Indonesia	ID	34
Iusacell	MX	32
MPLS ADSL Broadband	ZW	32
SHATEL DSL Network	IR	32
Aria Shatel Company Ltd	IR	28
Tellcom Iletisim Hizmetleri A.s.	TR	26
PT Indosat Tbk.	ID	26
TATA Communications	IN	26
Axtel	MX	25
UNE	CO	24
PT Telkom Indonesia	ID	24

*See **Appendix** for complete list of 603 **Organization Information of Common IPs Participating in the Attack**

Recommendations

As early as Bill Clinton's Presidential Commission on Critical Infrastructure Protection in 1997, it has been clear that Information Technology (IT) underpins all national critical infrastructures and services, and that they are all vulnerable to the three basic forms of cyberattack – data theft, denial, and manipulation.

Comodo data clearly demonstrate that every nation has a problem with malware. However, this report also proves that there is a large amount of information and intelligence available to help individuals, enterprises, nations, and even continents to make wiser choices when it comes to IT security.

Users

Above all, invest in your people. Security should become an integral part of your corporate culture. Smart people and clever algorithms are not intimidated by growth. They scale well. And curiosity is more valuable than certifications. Cyber threats are real, but your staff should have sufficient knowledge that they understand – and can defeat – the most common forms of attack. If your organization is a natural target for hackers, you also need to learn how to contain the inevitable entry of malicious code onto your network.

At the user level, teach your employees to beware of all unsolicited attachments and hyperlinks. Drill them in what to do in the event of a cybersecurity incident. Never allow them to post images of your internal work spaces on social media; if hackers can see your hardware, software, and keycards, they will have a much easier time getting in.

Managers

Senior managers need to be onboard. Post-Equifax, we can see that cyberattacks not only affect the bottom line, but also job security. Decision makers should see cyber risk as only one part of business risk. Attacks often look different than you expect: some attackers, for instance, merely want to use your computing resources to mine bitcoins. Decouple the sophistication of an attack from its effect: some pedestrian malware can have major consequences.

Metrics are key. How many hours a month are your employees required to spend in security training? In the event of a security incident, how long must you wait before the cavalry arrives? If hackers penetrate your external defenses, how will you measure their

"dwell time?" And once you kick them out, can you find their secret backdoors? Defense-in-depth is real. Honeypots are real. In security, there is no finish line, only mastering a long, grueling process.

Remember that even nation-states, with all of their traditional military might, are having a hard time deterring cyberattacks. So to a large degree, your enterprise is on its own in cyberspace and must fend for itself. And however much you would like to do it, a "hack back" is illegal and unwise.

Products

Here, complexity is the enemy of security. Think simplicity and minimization first. Containers and quarantines are effective because they copy best practices in the non-cyber world. In a high security context, ensuring the good is preferable to chasing the bad. Many of the best security tools, such as Nmap, are free. Really hard problems like encryption must be built by seasoned experts and integrated into your network infrastructure because they are too technical for average computer users to master and too important to screw up. From year to year, your "security stack" will simply have to change as the IT space and hacker threat are too dynamic for you to remain in place for too long.

The Future

Let's take a quick peek at the future. The latest craze in cybersecurity is Artificial Intelligence (AI). And this will be fun to watch, especially on the heels of movies like *Ghost in the Shell*, *Ex Machina*, and *Blade Runner 2049*. From the history of computer chess, one of the things that we do know AI will be good at is accomplishing simple tasks. Computers are not particularly clever, but they are great at fulfilling checklists and avoiding stupid mistakes. Further, algorithms are much better than people at detecting slow, stealthy reconnaissance, or what military planners call "Indications and Warning" of an attack. A case in point is ransomware, which must be stopped immediately upon discovery – before it encrypts your data. However, it is doubtful that AI will overcome all human (and computer) vulnerabilities, exploits, and attacks for the foreseeable future.

COMODO
THREAT RESEARCH LABS

Appendix

Organization Information of Common IPs Participating in the Attack

Range Owners Organization	Country	IP Per Count
Vietnam Posts and Telecommunications(VNPT)	VN	553
Turk Telekom	TR	129
Airtel Broadband	IN	114
VDC	VN	74
Bharti Airtel	IN	68
Viettel Corporation	VN	53
CMC Telecom Infrastructure Company	VN	51
True Internet	TH	34
Aamra Networks Limited	BD	34
Three Indonesia	ID	34
Iusacell	MX	32
MPLS ADSL Broadband	ZW	32
SHATEL DSL Network	IR	32
Aria Shatel Company Ltd	IR	28
Tellcom Iletisim Hizmetleri A.s.	TR	26
PT Indosat Tbk.	ID	26
TATA Communications	IN	26
Axtel	MX	25
UNE	CO	24
PT Telkom Indonesia	ID	24
Vivo	BR	21
FPT Telecom Company	VN	21
Telmex	MX	21
ONECOM	KE	20
Philippine Long Distance Telephone	PH	19
PERN AS Content Servie Provider, Islamabad, Pakist	PK	18
Asianet	IN	18
D-Vois Broadband Pvt	IN	18
Tv Azteca Sucursal Colombia	CO	17
Syscon Infoway Pvt.	IN	17
Bharti Broadband	IN	17
Cote d'Ivoire Telecom	CI	15
TRD ROBI DOOEL	MK	14
Telmex Colombia S.A.	CO	14
In2cable.com (India)	IN	13
Cablevisin, S.A. de C.V.	MX	13
ACCESSKENYA GROUP LTD is an ISP serving	KE	13
Telefnica Celular de Bolivia S.A.	BO	12
Mega Cable, S.A. de C.V.	MX	12
Telecom Italia	IT	12
CANTV	VE	12
3BB Broadband	TH	11
Internet Service Provider	ID	11
Telone	ZW	11
Eastern Telecoms Phils., Inc.	PH	10
PT Tele Globe Global	ID	10
Delta Infocom Limited	BD	10
Cablemas Telecomunicaciones SA de CV	MX	10
Tata Teleservices Maharashtra Ltd	IN	10
Wan & Lan Internet Pvt	IN	10
Fastweb	IT	10
Unitel	LA	9
RailTel Corporation of India Ltd.	IN	9
BDCOM Online Limited	BD	9
Southern Online Bio Technologies Ltd	IN	9
SINET, Cambodia's specialist Internet and Telecom	KH	9
Meghbela Broadband	IN	9
Cablevision	AR	9
ADN Telecom Ltd	BD	9
Alestra, S. de R.L. de C.V.	MX	8
Comteco Ltda	BO	8
PT. Cyberindo Aditama	ID	8
PT Media Sarana Data	ID	8
FASTNET	ID	8
Bolivia S. A.	BO	8
NSS S.A.	AR	7

Range Owners Organization	Country	IP Per Count
Cogetel Online	KH	7
Varnion Technology Semesta, PT	ID	7
Global Village Telecom	BR	7
Claro Dominican Republic	DO	7
Bangladesh Online Ltd	BD	7
TM Net	MY	7
ETB	CO	6
Wateen Telecom	PK	6
Tata Teleservices ISP	IN	6
Hireach Broadband Private Ltd	IN	6
Inwi Mobile	MA	6
Pars Online PJS	IR	6
Neda Gostar Saba Data Transfer Company Private Joi	IR	6
Telefonica Venezolana	VE	6
Vietnam Posts and Telecommunications (VNPT)	VN	6
Pulse Telesystems Pvt Ltd	IN	6
Global Iletisim Hizmetleri A.S.	TR	6
Information Society S.A.	GR	6
Netnam Company	VN	5
Dishnet Wireless Limited	IN	5
X-Link Limited	BD	5
Net Uno, C.A.	VE	5
VietNam Telecom National	VN	5
PT.Mora Telematika Indonesia	ID	5
TELEKOM SRBIJA a.d.	RS	5
Neuviz Net	ID	5
Virtua	BR	5
MNC Playmedia	ID	5
BRAC BDMail Network	BD	5
Intech Online Private Limited	IN	5
Entel S.A. - EntelNet	BO	5
Tehran Kar Ara	IR	5
Yashtel	IN	5
Orange Polska	PL	4
Vivacom	BG	4
Universidad De Antioquia	CO	4
Transtelco S.A.	MX	4
PADINET - Padi Internet	ID	4
CTBC	BR	4
Link3 Technologies Ltd.	BD	4
Blizoo DOOEL Skopje	MK	4
Ranks ITT	BD	4
Natural Fenosa Telecomunicaciones Guatemala S.A.	GT	4
PT Solnet Indonesia	ID	4
EMCATEL	CO	4
Oi Internet	BR	4
PT Quantum Tera Network	ID	4
DCTV Cable Network Broadband Services	PH	4
PT. Net2Cyber Indonesia	ID	4
ZOL Zimbabwe Assignments	ZW	4
S.I Group	KH	4
Jogja Medianet	ID	4
delDSL Internet Pvt. Ltd.	IN	4
Nettlinx Limited	IN	4
A Multihomed ISP Company	PH	4
Mexico Red de Telecomunicaciones, S. de R.L. de C.	MX	4
RCS & RDS Business	RO	3
Pakistan Telecommunication Company Limited	PK	3
IDS Bangladesh. IP Transit provider. Dhaka, Bangla	BD	3
Bharti Airtel Ltd., TELEMEDIA Services, for SMB cu	IN	3
Inetku-PBM	ID	3
PT Comtronics Systems	ID	3
Quest Consultancy Pvt Ltd	IN	3
Railtelibwcustomers	IN	3
Airtel	IN	3
Apollo Online Services Pvt ltd	IN	3
S.A. E.s.p	CO	3
Dishnet Wireless Limited. Broadband Wireless	IN	3

Range Owners Organization	Country	IP Per Count
Satnet	EC	3
Kenyan Post & Telecommunications Company / Telkom	KE	3
DSL-Elektronika d.o.o.	BA	3
KNK Telekomunikasyon Iletisim Elektrik Sanayi Tica	TR	3
Sify Limited	IN	3
Simbanet-as	KE	3
LINKNET	ID	3
Superonline Iletisim Hizmetleri A.S.	TR	3
AUGERE-Pakistan	PK	3
Autonomous System Number for Nexlinx	PK	3
Media Commerce Partners S.A	CO	3
Telefonica Data S.A.	BR	3
Fixed IP for cable modem customers	RS	3
Tim Celular S.A.	BR	3
MTN Nigeria	NG	3
Transworld Associates (Pvt.) Ltd.	PK	3
TVCabo Angola	AO	3
UPC Polska	PL	3
Comcast Business Communications	US	3
Grameen Cybernet Ltd. Bangladesh.	BD	3
Viewqwest Pte Ltd	SG	3
Wananchi-ke	KE	3
Olo del Peru S.A.C	PE	3
Aamra technologies limited	BD	3
Wsp Servios de Telecomunicaes Ltda	BR	3
Telefonos del Noroeste, S.A. de C.V.	MX	2
Tele Globe Global, PT	ID	2
Telekom Romania Communication S.A	RO	2
Augere Wireless Broadband Bangladesh Limited	BD	2
AXS Bolivia S. A.	BO	2
Milleni.com	TR	2
Co.pa.co.	PY	2
Tanzania Telecommunications	TZ	2
TalkTalk	GB	2
Empresa De Telecomunicaciones De Pereira S.A.	CO	2
Supernet Limited Transit	PK	2
Telnet Communication Limited	BD	2
Sul Americana Tecnologia e Informtica Ltda.	BR	2
Telstra Internet	AU	2
Mobilink Mobile Internet	PK	2
Mobily	SA	2
STLGHANA	GH	2
Mob Telecom	BR	2
INDO Internet, PT	ID	2
Mongolia Telecom	MN	2
Liquid Telecommunications Operations Limited	ZW	2
HYPERIA Ltd	NG	2
LINKdotNET Telecom Limited	PK	2
Linkdotnet-Jordan	JO	2
Toseh Ertebatat Homa (Private Joint Stock)	IR	2
Libyan Telecom and Technology	LY	2
Ecuadortelecom S.A.	EC	2
BT	GB	2
Protel I-Next, S.A. de C.V.	MX	2
Skyline Semesta, PT	ID	2
EARTH TELECOMMUNICATION (Pvt)	BD	2
CityOnline Services Ltd	IN	2
MyKRIS Asia Sdn Bhd	MY	2
Accesskenya Group Ltd	KE	2
National Information Technology Authority Uganda	UG	2
SingNet Pte Ltd	PK	2
D-VoiS Broadband Private Limited	IN	2
TTCLDATA	TZ	2
TurkNet Iletisim Hizmetleri A.S	TR	2
Servicos De Telecomunicao Ltda	BR	2
Serviciul de Telecomunicatii Speciale	RO	2
ONO	ES	2
TVCABO - Comunicacoes Multimedia, Lda.	MZ	2

Range Owners Organization	Country	IP Per Count
UAB Bite Lietuva	LT	2
Serbia BroadBand-Srpske Kablovske mreze d.o.o.	RS	2
Sc Netfil Srl	RO	2
DrukNet ISP	BT	2
Neamul Haque Khan t/a Mazeda Networks Limited	BD	2
United States Air Force	KE	2
Satellite Connection	BD	2
Jordan Tv Cable & Internet Services Co	JO	2
Broadband Plus	LB	2
Jazz Telecom S.A.	ES	2
Globalreach eBusiness Networks, Inc.	PH	2
Universitas Negeri Semarang	ID	2
CMPak Limited	PK	2
Broadband Pacenet Pvt.	IN	2
Bezeq International	IL	2
UPC Romania SRL	RO	2
S.A. E.s.p.	CO	2
Reliance Communications	IN	2
Redes y Telecomunicaciones	HN	2
Deutsche Telekom AG	DE	2
COTAS	BO	2
Arrownet Pvt.Ltd	NP	2
Paknet Limited Merged into PTCL	PK	2
IPStaticMarocTelecom	MA	2
ipNX NIGERIA LIMITED	NG	2
Pt Selaras Citra Terabit	ID	2
PT. Saranainsan Mudaselaras	ID	2
PT Remala Abadi	ID	2
PT. Pasifik Satelit Nusantara	ID	2
Primesoftex	IN	2
Comcast Cable	US	2
Batelco Jordan	JO	2
Dai IP tinh cho khach hang xDSL	VN	2
PT Maxindo Mitra Solusi, Jl Kelapa Puan Raya Blok	ID	2
BRACNet Limited	BD	2
Pt. Linknet	ID	2
Internet Access & Telecom Carrier Service Provider	BD	2
Vodafone DSL	DE	2
Comilla Online	BD	2
Angel Drops Ltd	BD	2
Hathway	IN	2
Blizoo Media and Broadband	BG	2
Vodafone Ono	ES	2
Vodafone Spain	ES	2
Oasis-sprl	CD	2
PT DES Teknologi Informasi	ID	2
Agni Systems Limited	BD	2
Vung dia chi IP cap cho dich vu IPTV tai Ha Noi	VN	2
HiNet	TW	2
Corporacion Digitel C.A.	VE	2
Bittel Telecom Pvt Ltd	IN	2
PT. Cahaya Buana Raksa	ID	2
Cable & Wireless Jamaica	JM	2
Md. Abdul Awual t/a Cyber Way Technology	BD	2
Ethernet Xpress Pvt. Ltd.	IN	2
Maroc Telecom	MA	2
Centennial Cayman Corp Chile S.A	CL	2
Metro Net, S.A.P.I. de C.V.	MX	2
Telecomunicacoes Ltda	BR	2
Telecomunicaes Ltda.	BR	2
TE Data	EG	2
Indosatm2	ID	2
Mahbub Morshed t/a Mahi Enterprise	BD	2
Telefonica de Espana	ES	2
Telefonica del Peru	PE	2
Techtel LMDS Comunicaciones Interactivas S.A.	AR	2
Telecable de Asturias,SA	ES	1
Telecable Economico S.A.	CR	1

Range Owners Organization	Country	IP Per Count
Telecall Brasil Servios de Telecomunicaes Lt	BR	1
Telecel S.A.	PY	1
Telecentro S.A. - Clientes Residenciales	AR	1
Telecom Argentina S.A.	AR	1
Telecom Eireli	BR	1
Telecom Italia Sparkle of North America	US	1
Telecom Ltd	BR	1
Telecom Ltda.	BR	1
Telecom Ltda Me	BR	1
Telecom Namibia	NA	1
Telecomunicacoes Do Brasil Ltda.	BR	1
Telefonica de Argentina	AR	1
TELEKOM SRBIJA, ADSL users	RS	1
Telemasters	ZA	1
Telenor d.o.o. Beograd	RS	1
Telgua	GT	1
Terrakom d.o.o.	HR	1
The Blue Zone East / Jordan	JO	1
Tikona Digital Networks Pvt	IN	1
Time Warner Cable	US	1
Tiscali UK Limited	GB	1
TM International Bangladesh	BD	1
Tomato Web (Pvt) Limited	BD	1
TOT	TH	1
TPG Internet	AU	1
TRICOM	DO	1
TRI.ph AS Inter-Island Information Systems, Inc.	PH	1
Triple C Computation Ltd.	IL	1
Tripleplay Broadband Pvt Ltd	IN	1
TRIPLEPLAY INTERACTIVE NETWORK PVT LTD	IN	1
TRUE, The Real Unix Experts	VE	1
Umniah Mobile Company	JO	1
UNICS Ltd	BG	1
UniNet(Inter-university network)	TH	1
United Telecommunication Services (UTS)	CW	1
Universitas Ahmad Dahlan	ID	1
Universitas Jember	ID	1
Universitas Pattimura	ID	1
Universitas Udayana	ID	1
Vainavi Industies Ltd	IN	1
Vasai Cable Pvt. Ltd.	IN	1
Vectra Broadband	PL	1
Vex Net Telecon	BR	1
Via Real Internet Equipamentos de Informatica Ltda	BR	1
Vietel - CHT Compamy	VN	1
Vietnam Technology and Telecommunication JSC	VN	1
Vihaan Telecommunication Pvt. Ltd.	IN	1
Villages around Stara Zagora	BG	1
VipNET	CI	1
Virtex Ltda	BR	1
Vodafone Ghana	GH	1
Vodafone Italia	IT	1
Vodafone Italia DSL	IT	1
Vodafone Net Iletisim Hizmetleri A.s	TR	1
Voztelecom network	ES	1
V Telecoms Berhad	MY	1
VTR Banda Ancha S.A.	CL	1
Wana Corporate	MA	1
Wan Interco for customers	FR	1
Wds Telecom Ltda. Me	BR	1
Webnet Solues Em Internet Ltda	BR	1
WHS Telecom Serv. Telecomunicacoes LTDA	BR	1
Wicom Networks LLC	MN	1
Wifirst S.A.S.	FR	1
Wind Telecomunicazioni	IT	1
Wlenet Informtica manuteno	BR	1
YUnet International d.o.o.	RS	1
ZOL GPON Home Users	ZW	1

Range Owners Organization	Country	IP Per Count
PT Mega Mentari Mandiri	ID	1
4ALB shpk	AL	1
ABCOM-Business-clients , HFC-Infrastructure	AL	1
Abissnet sh.a.	AL	1
Access Telecom (BD) Ltd	BD	1
Adelphia Comunicacoes S.A.	BR	1
Administracion Nacional de Telecomunicaciones	UY	1
afczas	ZM	1
Africa Online Uganda	UG	1
Agentia de Administrare a Retelei Nationale de Inf	RO	1
A. L. A. Informatica Ltda.	BR	1
Albanian Satellite Communications sh.p.k.	AL	1
Alcoa Aluminio S/A	BR	1
AlwaysOn Network Bangladesh	BD	1
AmberIT Limited	BD	1
Angkor Data Communication	KH	1
Argentina S.A.	AR	1
Asansol Engineering College, Asansol	IN	1
Asmanfaraz Sepahan Isdp (pjs)	IR	1
ASRE ENTEGHAL DADEHA - Broadband Services	IR	1
Atel Telecom	BR	1
Auro International School Of Hospitality Managemen	IN	1
Axtel - Recursos WiMAX	MX	1
Bartlomiej Sztefko trading as Bartlomiej Sztefko G	PL	1
Baru Hosting	PA	1
Bayanat NOC IP range	SA	1
B.b.g Campelo Me	BR	1
Beam Telecom	IN	1
Bharti Airtel Ltd., Telemedia Services	IN	1
Blicnet d.o.o.	BA	1
Branch of Netnam Company in Ho Chi Minh City	VN	1
Britis Telecom LTDA	BR	1
Broadband ISP, FTTH and Cable Service Provider	PK	1
BSNL	IN	1
BSW	AR	1
BTC Broadband Service	BG	1
Btc-gate1	BW	1
BTS Communications (BD) Ltd	BD	1
BTTB	BD	1
Cablecolor S.A.	HN	1
Cable Tica	CR	1
Chiang Mai Vocational College	TH	1
Chi nhanh HCM-Cong ty CP Ha Tang Vien Thong CMC	VN	1
Citinet LLC	MN	1
Citycom Networks Pvt Ltd	IN	1
CJONLINE ISP India	IN	1
CNS Systems s.r.o.	SK	1
Comcel Guatemala S.A.	GT	1
Comercio De Telefonia E Comunicacao Ltda	BR	1
Commission on Science and Technology for	PK	1
Completel	FR	1
Comunicao E Informatica Epp	BR	1
CONECEL	EC	1
Conesul Telecomunicacoes Ltda	BR	1
Conjoinix Technologies Pvt. Ltd.	IN	1
COOLLINK	NG	1
Cotas Ltda.	BO	1
CPS	AR	1
Cromtel Prod Impex Srl	RO	1
CS LoxInfo	TH	1
Customer wireless connectivity link addresses	RS	1
Cyprus Telecommuncations Authority	CY	1
Cyprus Telecommuncations Authority	GR	1
Cyta Hellas	GR	1
Daisy Communications Ltd	GB	1
Derkom Spolka Jawna Dariusz Klimczuk	PL	1
Digital Network Associates Pvt	IN	1
Digital Ocean	US	1

Range Owners Organization	Country	IP Per Count
Digital Servios De Informatica E Comercio	BR	1
Dodo Australia	AU	1
Dtpnet Nap	ID	1
Ebone Network (PVT.) Limited	PK	1
Empresa De Informtica E Telecomunicaes	BR	1
Empresa de Recursos Tecnologicos S.A E.S.P	CO	1
Empresa de Telecomunicaciones de Pereira S.A. E.S.	CO	1
Epm Telecomunicaciones	CO	1
Equipos Y Sistemas S.A.	NI	1
Eskisehir Bilisim Iletisim San. ve Tic. A.S.	TR	1
Etihad Atheeb Telecom Company	SA	1
EUROTEL Ltd	UA	1
Euroweb Romania SA	RO	1
Fariya Networks Pvt.	PK	1
Fastel Sarana Indonesia PT	ID	1
Fiber @ Home Limited	BD	1
Fivenetwork Solution India Pvt Ltd Internet	IN	1
Forthnet	GR	1
Freitas Servicos de Internet Ltda	BR	1
Frontiir Co. Ltd	MM	1
GETESA (Orange Equatorial Guinea)	GQ	1
Gigabit S.a.l	LB	1
Global Crossing Comunicaes Do Brasil Ltda.	BR	1
GlobalNet S.A	TN	1
Global Tecnologia Ltda Me	BR	1
Golden Telecom LLC	UA	1
GO p.l.c.	MT	1
Gpon Pool	ZW	1
Greater Amman Municipality	JO	1
Grupo Hidalguense de Desarrollo, S.A. de C.V.	MX	1
Gtel Tijuana	MX	1
GTS Hungary Telecommunications Limited Liability C	HU	1
Gurunanak Institute for technology, Panihati, Kolk	IN	1
HEC	PK	1
Hexabyte	TN	1
Honesty Net Solution (I) Pvt	IN	1
Hosting Internet Hizmetleri Sanayi ve Ticaret Anon	TR	1
Hotel Paramount	ID	1
IACTCOM	IL	1
IFX Corporation	VE	1
Ifx Networks Colombia	CO	1
IHS Telekomunikasyon Ltd	TR	1
Ikatelnet	ML	1
INB Informatica ltda	BR	1
IndoInternet Network	ID	1
Infocom-ug	UG	1
Informatica Ltda	BR	1
Informtica Ltda	BR	1
Ingeniera e Informtica Asociada Ltda (IIA Ltda	CL	1
Intelligent Technologies S.A.	PL	1
Interdomain Routing	IN	1
Internet by Sercomtel S.A.	BR	1
Internet Initiative Japan Inc.	JP	1
Internet Solutions	ZA	1
Internet Thailand Company Limited	TH	1
Invitel Tavkozlesi Zrt.	HU	1
IP Core MPLS	BD	1
Ipko Telecommunications	AL	1
ISP External Zone	PA	1
Israel Local Authorities Data Processing Center Lt	IL	1
Itelkom S.A.S	CO	1
Ixsforall, Inc.	PH	1
Jazztel Mobile	ES	1
Jordan Data Communications Company LLC	JO	1
Jupiter Telecomunicacoes e Informatica Ltda	BR	1
Kappa Internet Services Private Limited	IN	1
Karvy Consultants	IN	1
KENYAWEB	KE	1

Range Owners Organization	Country	IP Per Count
Konecta de Mexico, S. de R.L. de C.V.	MX	1
Konnet Informtica Ltda	BR	1
KurumsalLanmix	TR	1
LCR Telecom NV	BE	1
lefke avrupa universitesi kktc	TR	1
L E M Telecomunicaes Ltda -me	BR	1
L. Garcia Comunicaes ME	BR	1
Linktel Telecomunicacoes Do Brasil Ltda	BR	1
Lintas Data Prima, PT	ID	1
Liquid Zimbabwe	ZW	1
Loxley Wireless Co., Ltd.	TH	1
Luis Antonio Palomino Dagdug	MX	1
LulinNet	BG	1
Magyar Telekom	HU	1
Mahanagar Telephone Nigam Ltd.	IN	1
Malaysian Research & Education Network	MY	1
Mauritanian Telecommunication Company	MR	1
Maxcom Telecomunicaciones, S.A.B. de C.V.	MX	1
Maxis Broadband Sdn Bhd	MY	1
Md. Shariful Islam T/A BRISK SYSTEMS	BD	1
Mediacom Cable	US	1
Meghbela Skywave Cablenet Private Limited	IN	1
Melita plc	MT	1
Mercantile Communications Pvt. Ltd	NP	1
MetroCast	US	1
MetroNet Bangladesh Limited	BD	1
Micropic Ltda	BR	1
Ministry of Finance	TH	1
MTNRW	RW	1
Multimedia Polska S. A.	PL	1
Multinet Pakistan Pvt. Ltd.	PK	1
Mundivox LTDA	BR	1
MWEB	ZA	1
Nacional De Telecomunicaciones - Cnt Ep	EC	1
National Telecommunication Corporation HQ	PK	1
Navega.com S.A.	GT	1
neojaime oliveira ribeiro me	BR	1
Nepal Telecom	NP	1
NETCEN Teknoloji Ltd. Sti.	TR	1
Netcom Enterprises Pvt Ltd	IN	1
Netcomm Argentina SRL	AR	1
Netia SA	PL	1
NETLIFE	EC	1
NetSol Connect	PK	1
Netvigator	HK	1
Network Operations Center	ID	1
New Century InfoComm Tech Co.	TW	1
Newcom Limited	GT	1
Norfolk Hotel	KE	1
Noroestecom Telecomunicacoes Ltda	BR	1
OCPT	CD	1
OGERO	LB	1
Oi Fixo	BR	1
OmanMobile Telecommunication company LLC	OM	1
ONATEL/FasoNet's	BF	1
Orange Israel	IL	1
Orange Madagascar	MG	1
Orbit Telecom Technology Co. Ltd	JO	1
OTEnet S.A.	GR	1
Panda Network	BR	1
Paratus-Telecom	AO	1
PlusNet Technologies Ltd	GB	1
PrimaNet - PT. Khasanah Timur Indonesia	ID	1
Proimage Engineering and Communication Co.,Ltd.	TH	1
Pronet sh.p.k.	AL	1
Provedor De Acesso A Internet Ltda	BR	1
Proximus Skynet	BE	1
PT. Arsen Kusuma Indonesia	ID	1

Range Owners Organization	Country	IP Per Count
PT. Bangun Abadi Teknologi Indonesia	ID	1
Pt Bina Informatika Solusi	ID	1
PT. Cross Network Indonesia	ID	1
PT Cyberplus Media Pratama	ID	1
PT. DATA Utama Dinamika	ID	1
PT Fiber Networks Indonesia	ID	1
PT. First Media, Tbk	ID	1
PT Hyperindo Media Perkasa	ID	1
PT iForte Global Internet	ID	1
Pt Indonesia Comnets Plus	ID	1
PT Indosat Tbk	ID	1
PT.Insan Sarana Telematika	ID	1
PT. Lintas Data Prima	ID	1
Pt. Matrixnet Global Indonesia	ID	1
21 st Century Technologies Limited	NG	1
PT Net2Cyber Indonesia	ID	1
PT. Palapa Media Indonesia	ID	1
PT Pemuda Berkarya Indonesia	ID	1
PT Rahajasa Media Internet	ID	1
PURISCAL	CR	1
QIS College of Engg,Vengamukkapalem Ongole, Andhra	IN	1
Radore Veri Merkezi Hizmetleri A.S.	TR	1
Rainbow communications India Pvt Ltd	IN	1
Ramiro Alfonso Gomez Caicedo	CO	1
R Cable y Telecomunicaciones Galicia, S.A.	ES	1
Romtelecom Data Network	RO	1
Safaricom	KE	1
SAGLAYICI Teknoloji Bilisim Yayincilik Hiz. Ticare	TR	1
SamoaTel Limited	WS	1
SAN JOSE	CR	1
Sapthagiri College of Medical Sciences,Banglore	IN	1
SA Telecable	BG	1
Sat Film	PL	1
Sat-Trakt d.o.o.	RS	1
SAT-TRAKT Telecommunications	RS	1
SaudiNet	SA	1
Servcom Sp. z o.o.	PL	1
Shiraz Hamyar Co.	IR	1
Shree Cable	IN	1
Sikka Cable	IN	1
SingNet Pte Ltd	NP	1
Siticable Network Limited	IN	1
Sixsigma Networks Mexico, S.A. de C.V.	MX	1
Skylogic S.p.A.	ES	1
Smart Link Communication	DZ	1
Smart Link Communication	FR	1
SOL-Customer-MIX	TR	1
SOLNET-Customer-Serial	TR	1
Soluciones en Telecomunicaciones, S.A.	GT	1
Solusindo Bintang Pratama, PT	ID	1
Srm Easwari Engineering College	IN	1
Starnet S.r.l	MD	1
Stetnet Telecom	BR	1
Summit Communications Ltd.	BD	1
Surfplanet GmbH	DE	1
SystemsFox prestao de servios LTDA	BR	1
T-2, d.o.o.	SI	1
Tata Mobile	IN	1
Tecmidiaweb Ltda	BR	1
Tecnologia	BR	1
Tecnowireless Telecom Ltda	BR	1
Teknotel Telekomunikasyon Sanayi Ve Ticaret A.s.	TR	1
Telconet S.A	EC	1
Telecable Central, S.A.	DO	1
Total Results		
603	**95**	**2,934**

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 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