

Global Threat Report 2018 Q3

Browse

[Contents](#)

[Introduction](#)

[Phishing - Emails Reigns Supreme](#)

[Sustained Targeted Attacks](#)

[The Geopolitics of Malware](#)

[The Impact of Malware on Elections](#)

[Malware and Military Operations](#)

[Conclusions](#)

COMODO
CYBERSECURITY

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel: +1 (877) 712 1309

Tel: +1 (888) 551 1531

Fax: +1 (973) 777 4394

Inquire: sales@comodo.com

Support: c1-support@comodo.com

Visit comodo.com to learn more

BROUGHT TO YOU BY



CONTENTS

03	Introduction Non-Stop Vigilance
04	Phishing - Emails Reign Supreme
05	Suspect Senders
07	Tracking Down Phishing Hosts
08	The Many Guises of Phishing
09	Sustained Targeted Attacks
10	On Enterprise by Malware Type
11	Regionality of Cybercrime
14	Botnets in the US Heartland
16	The Geopolitics of Malware
17	Socioeconomics of Malware
18	Top Trojans by Country
19	EBB and Flow of Malware Propagation
20	Worm Detections by Country
21	Trojan Detections by Country
22	Virus Detections by Country
23	Backdoor Detections by Country
24	The Impact of Malware of Elections
25	Republic of Mali
26	The Russian Federation
27	Republic of Turkey
28	Republic of Sierra Leone
29	Republic of Azerbaijan
30	Republic of Colombia
31	Malware and Military Operations
32	Syria Conflict
33	Iran
34	Palestine and Israel
35	Yemen and Saudi Arabia
36	Conclusions
37	Company Profiles

INTRO

The ubiquitous presence of Comodo cybersecurity tools, with a base of over 100 million installations, puts Comodo in a unique position among vendors in the field, one of overarching knowledge of the type, volume, frequency and other attributes of malware circling the globe. By leveraging real-time intelligence from this base and from other sources owned and employed by Comodo, the company can supply unique insights, and draw conclusions about the distribution and spread of malware. It can offer organizations of all sizes innovative commercial cybersecurity solutions and services uniquely available by building on the combination of this intelligence, on mature cybersecurity technology and upon the experience of the Comodo Threat Research Labs team members.

With this unique position comes a special responsibility to share intelligence and insights with the larger cyber community – with other analysts and end users and interested third parties. It is from this duty that we compile and publish our Quarterly Global Threat Report.

NON-STOP VIGILANCE

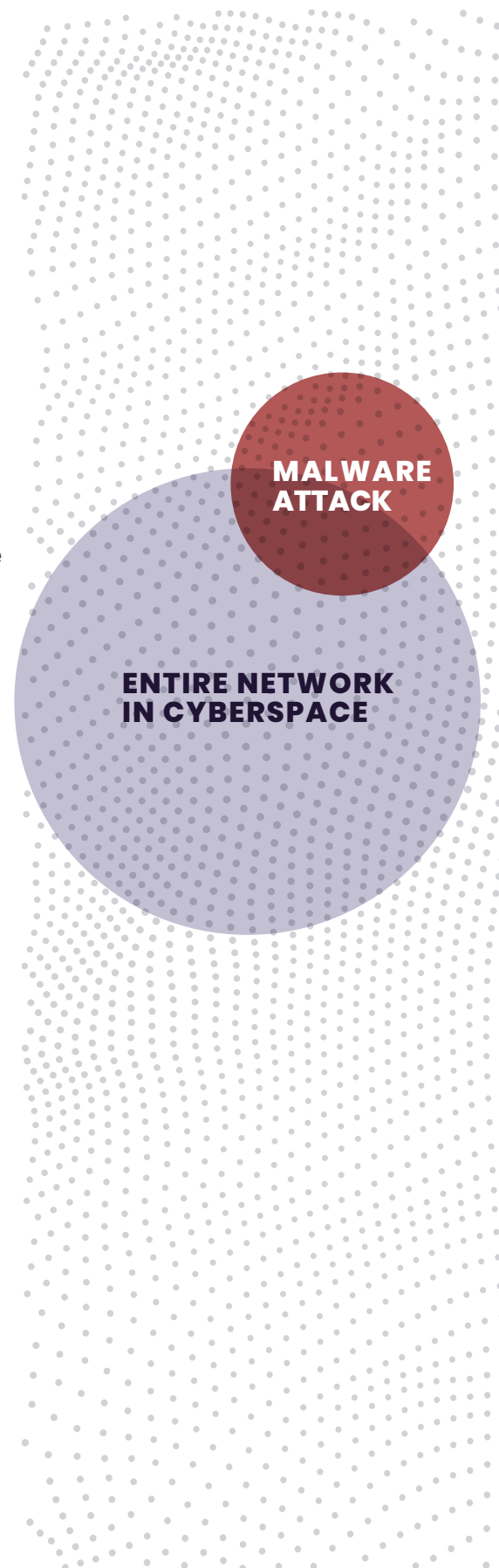
Battles in cyberspace occur every second of the day, every day of the year, non-stop. At the Comodo Threat Research Lab (CTRL), our mission is to protect IT users all over the world from ever-more cunning and sophisticated cyberattacks.

Comodo stands guard 24/7 to combat the gamut of modern [cybersecurity threats](#)

- Every week, Comodo processes over 1.4 billion files, with 28+ million containing malware
- Weekly, Comodo blocks 230,000 malicious IP addresses and categorizes 500,000 new domains or URLs
- CTRL inspects millions of emails daily, discovering over 50,000 with phishing links or embedded malware

The trends and intelligence in this report build on these monitoring and analysis activities. Comodo invites readers to peruse the findings and discoveries from Q3 2018.

WELCOME TO THE CYBER WARFARE FRONT LINE.



[BACK TO TABLE OF CONTENTS](#)

PHISHING

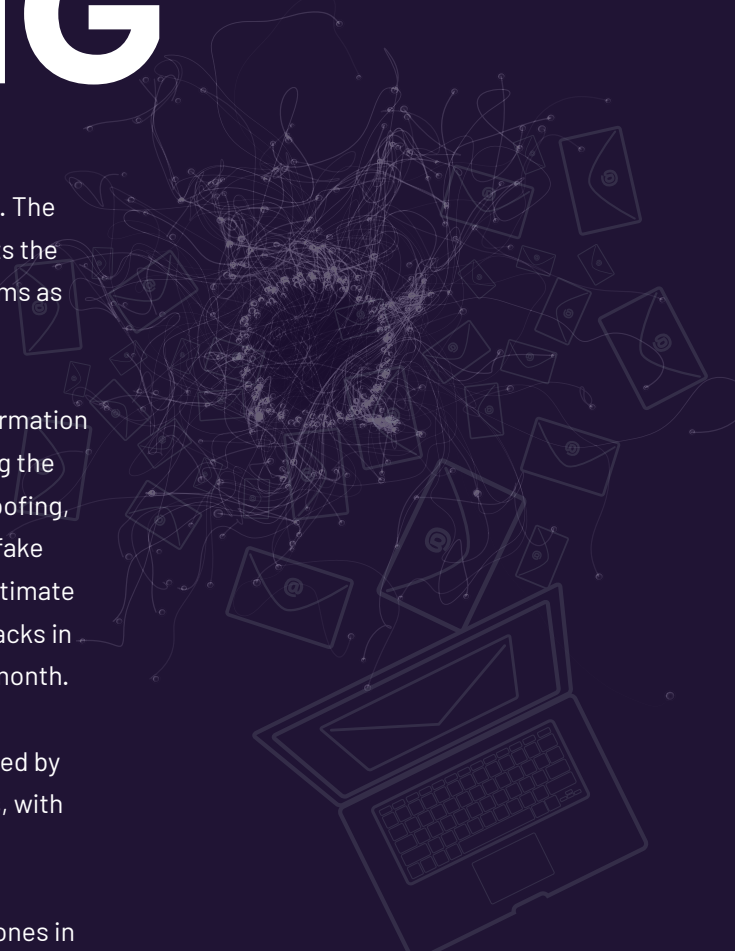
EMAIL REIGNS SUPREME

Email continues to be the most popular means of malware delivery. The preference for email as a vehicle is not surprising. Email represents the cheapest, simplest and most effective tool to exploit as many victims as possible in the shortest timeframe.

Phishing is defined as a fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising the sender as a trustworthy entity. Phishing is carried out by email spoofing, and attempts to direct recipients to enter personal information at fake website, the look and feel of which are identical to the spoofed legitimate equivalent. 76% of organizations report experiencing phishing attacks in 2017 (Wombat), with users receiving 16-20 malicious emails every month.

In today's cyber threat landscape, the phishing threat is compounded by increasing use of AI technologies to create malware-loaded emails, with poisoned message volume growing exponentially.

Below you can observe the ratio of the malicious emails to benign ones in the data processed by Comodo analysts.



TOP CATEGORIES OF EMAIL RECEIVED BY ENTERPRISE USERS



[BACK TO TABLE OF CONTENTS](#)

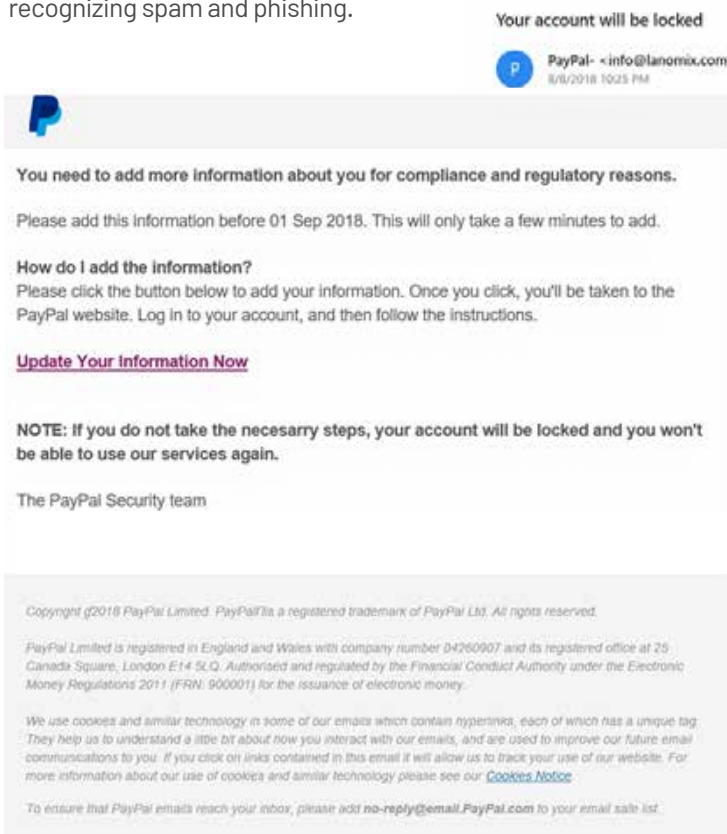
SUSPECT SENDERS

Spam and phishing emails are the favorite weapon of hackers, and in Q3 2018 this trend continued unabated. The popularity of phishing arises in large part due to its cost-effectiveness: low production cost, unlimited scalability, and potential for high profits make this vehicle attractive to cybercriminals. Just one click of a deceived recipient, and voilà, the perpetrators hit the mark. Phishing enables theft of private information and credentials, infection of compromised machines and networks with new malware types and propagation at “Internet speed”.

As computer users become more phishing-savvy, perpetrators must become ever more clever to bypass user vigilance. Attackers invent increasingly cunning tricks and cover stories to boost the plausibility of fake emails, to hook even security-aware users.

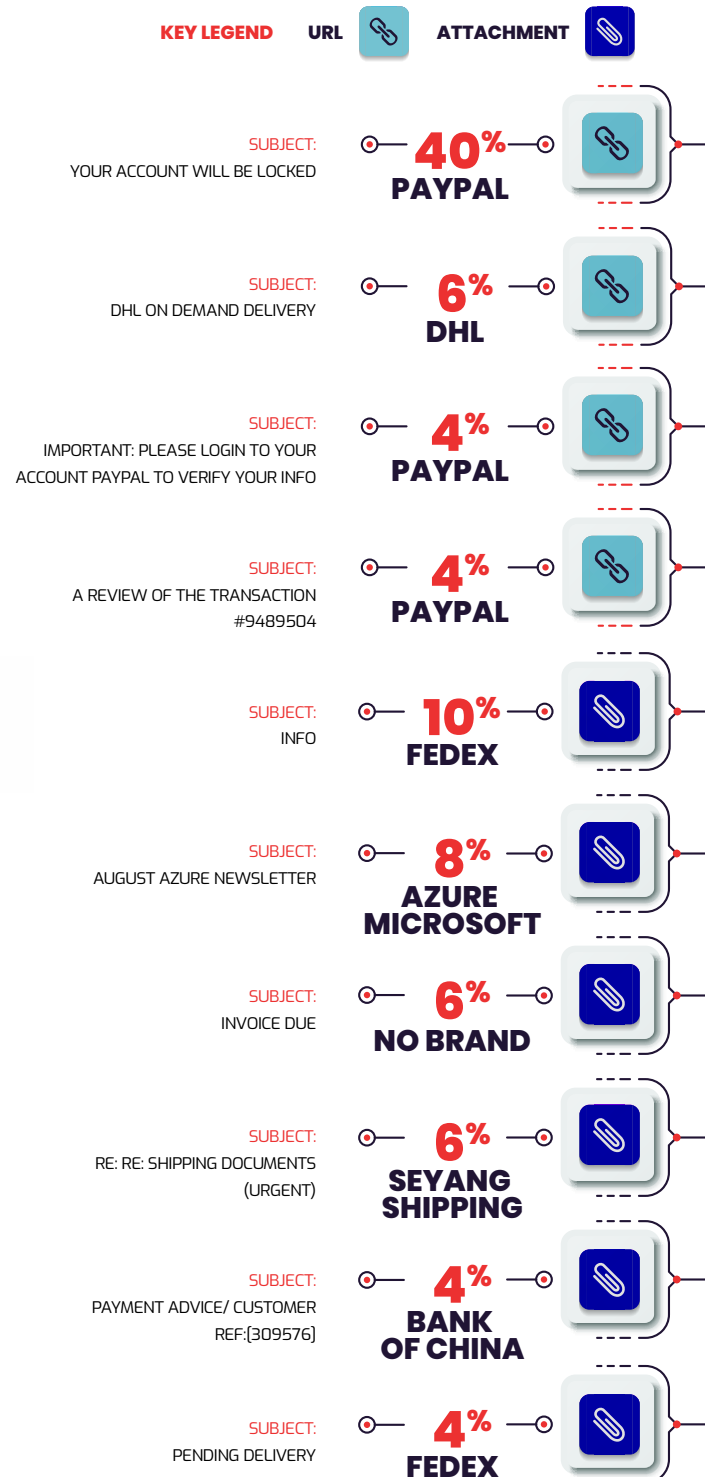
In first place is a message “from PayPal”, threatening to lock a victim’s account immediately pending update of information.

The link in the email redirects the user to a fake PayPal page to collect entered credentials. 19,562 users received this email – the attackers definitely counted on a big haul. Astute readers will notice the errors in English and typos in the boilerplate text – red flags for savvy users in recognizing spam and phishing.



In Q3 2018, CTRL encountered a range of devious emails. In the accompanying table, you can observe the top 10 phishing subject lines, spoofed senders and the threats posed by the email payloads.

PHISHING EMAILS RANKED BY SUBJECT



[BACK TO TABLE OF CONTENTS](#)

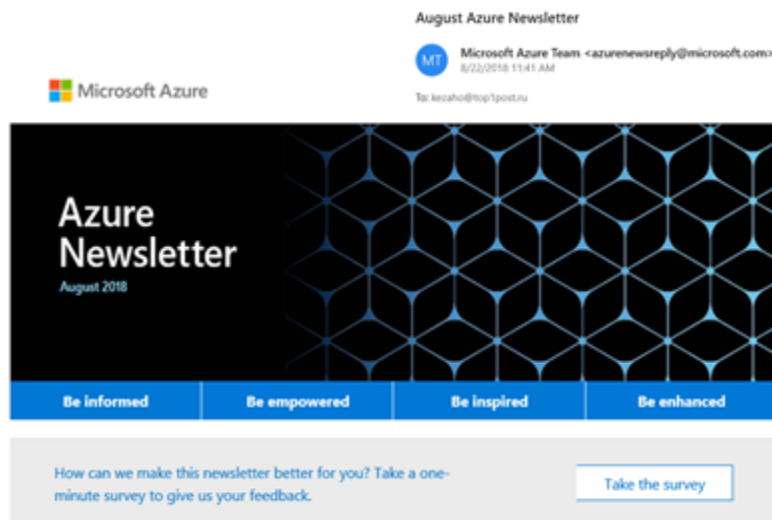
SUSPECT SENDERS

Another email that made the rounds in Q3 2018 masqueraded as an invitation to take a survey from Microsoft about its Azure cloud and is impressive for its high quality. The Microsoft Azure logo and other attributes appear very authentic, and even the address of the sender seems legitimate. Surely, many recipients might have taken the bait, had Comodo not detected and halted the attacker.

Clicking on the “Take the survey” button redirect recipients to a malware-laden webpage to covertly infect them with malware.

The following phishing email from “DHL Express” is not so sophisticated, and the sender address betrays the attackers. The “Click here to fill our form” button leads to a faked DHL webpage to steal credentials of the victim.

The next email also looks quite plausible, including the sender email address and company details. The attached malware masquerades as a .pdf file, but a educated eye will notice that in reality it has .arj extension an archive format often used for malware packaging.



Featured

Microsoft Ignite 2018: Now with more code

Azure, Windows, and Visual Studio—that’s just a sample of the development tools and platforms covered at Microsoft Ignite in Orlando, Florida this September. Check out the expanded offering of developer-focused sessions, labs, and hacks at this year’s event. [Learn more.](#)

DHL On Demand Delivery

DHL EXPRESS <manjit-singh@t-online.de>
8/20/2018 6:30 PM
To: dhlus@ackdelivery@dhl.com

Your DHL Parcel Arrived Our Office

Dear Valued Customer,

Please receive your packages:

Your packages arrived at post service center since Friday 17th August.

Our courier agent was unable to deliver the packages to you due to incorrect delivery detail.

Please Kindly Use Our Online Form To Fill Your Address Correctly So We Can Deliver Your Parcel By Today.

This email is scanned(secure) and sent to you because you are a subscriber to our newsletter.

NOTE: IF MESSAGE IS FOUND BY SPAM IN YOUR JUNK MAIL, KINDLY OPEN AS SPAM.

© 2018 DHL Express | Customer Service | [DHL India | English](#)

RE: Shipping Documents (Urgent)

Seyang Shipping Co., Ltd. <mail@seyang.co.kr>
8/20/2018 8:57 AM

Shipping_Doc23467.pdf
212.95 KB

Dear sir,

Fyi we got an instruction from our client to contact you on the above subject, please kindly take into quick shipment.

Kindly confirm that the details are correct and revert back to us asap.

Regards,

Jin-Soo Hoo
Seyang Shipping Co., Ltd.

SEYANG BLDG 3FL., # 237-1, JANGHAROGORAE-RO,
SANGU-SO, ULSAN, KOREA / 44700
Tel: 82-(0)52-261-6691/5
Fax: 82-(0)52-261-3500
Mobile: 82-(0)10-4636-2789
E-Mail: mail@seyang.co.kr



[BACK TO TABLE OF CONTENTS](#)



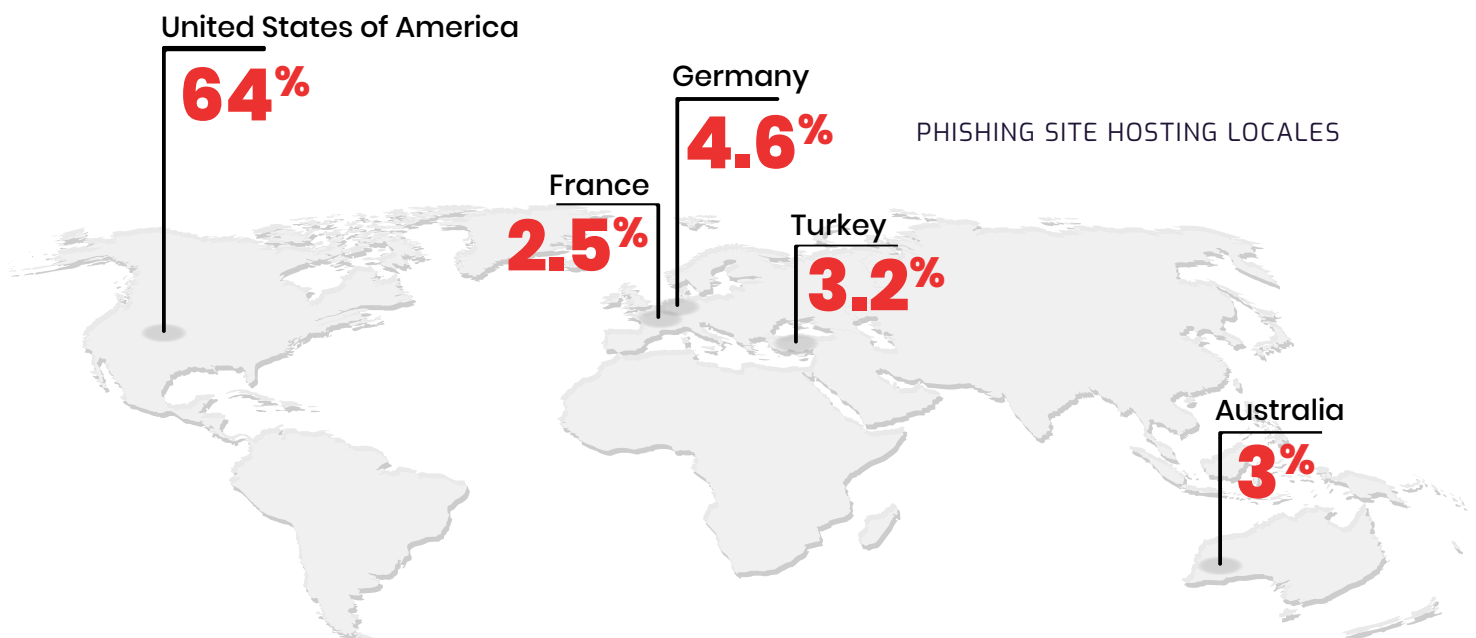
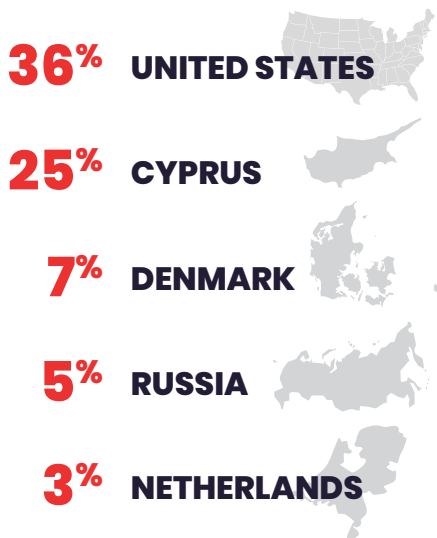
TRACKING DOWN PHISHING HOSTS

To host phishing webpages, cybercriminals register a variety of domains across multiple geographies, changing them quickly once spotted by cybersecurity enforcement. Notably, the US leads in phishing page hosting by a large margin, with over 64% of registered sites, followed by Germany (4.6%), Turkey (3.2%), Australia (3%) and France (2.5%).

Moreover, the US also leads as the origin of the phishing attacks themselves. Over a third of all phishing attacks originated from US-based IP addresses, followed by Cyprus, Turkey, Denmark, Russia and Great Britain.

At the time of publication of this report, 23% of the listed phishing pages remained online.

COUNTRIES OF ORIGIN FOR PHISHING ATTACKS



[BACK TO TABLE OF CONTENTS](#)

THE MANY GUISES OF PHISHING

The key to successful phishing lies in choosing the right sender to spoof. Understanding this choice of co-opted brands is also important in fighting the phishing onslaught. Well-known, authoritative sender brand names inspires trust in recipients. In the last quarter, Microsoft, PayPal, Google, Postmaster, and DHL comprised the top 5 of brands spoofed by phishers; the next 15 you can find in the table to the right.

Brand equity is a weapon that cuts two ways: emails apparently received from organizations with better-known brand names both inspire confidence and carry the possibility of carrying a phishing attack. Ironically, email from a famous brand name in an unsolicited email increasingly rings malware alarm bells.

Analysis of events in Q3 2018 events clearly demonstrates that phishing attacks are growing in quantity and evolving in sophistication and quality.

Trends among black hats engaging in phishing include

- Creating ever more plausible legends for disguising malicious intent of email to bypass user vigilance
- Exploitation of ubiquitous, trusted brand names
- Attaching malware payloads directly to phishing email rather than linking to fake sites

The last point is most ominous, as phishing emails are being transformed from a means of soliciting credentials into a powerful tool to directly infect users with diverse malware types. Between traditional link-based phishing and this new trend of direct malware delivery, email is steadily morphing into a main channel for malware propagation and is no longer a trusted means for communication. Comprehending this new reality is key to building reliable cybersecurity policies and practices for every organization.

TOP BRANDS CO-OPTED FOR PHISHING

All names and trademarks are property of their respective owners

 Microsoft	19.0%
 PayPal	17.0%
 Google	9.7%
 postmaster	7.5%
 DHL	6.4%
 Dropbox	5.8%
 Bank of America	4.6%
 WELLS FARGO	4.1%
 CHASE	4.1%
 YAHOO!	3.1%
 Adobe	3.0%
 Apple Store	3.0%
 facebook.	2.5%
 Alibaba.com [®]	2.1%
 Aol.	2.0%
 MyEtherWallet	1.5%
 MAILBOX	1.4%
 F R E E	1.1%
 P R O D	1.1%
 DocuSign [®]	1.0%

[BACK TO TABLE OF CONTENTS](#)

SUSTAINED

TARGETED ATTACKS



Cybercrime is ultimately a business. Commercial ends require well-resourced, financially flush targets, putting enterprise organizations squarely in hackers' cross hairs. But direct profit may not be the sole motive for an attack. Tooth-and-nail competition among companies (or governments) can drive organizations to hack their competition, destroying digital assets, deleting data, defacing web sites and disrupting operations.

Black hats employ various types of malware to penetrate and compromise enterprise networks. In Q2 2018, the most popular malware for enterprise assault included trojan droppers, trojan generics, password stealers, PUA and backdoors. And in July 2018, Comodo observed a huge spike in viruses.

- Trojan droppers covertly install various other types of malware, including ransomware.

[Continue Reading >>](#)



- Trojan generics are diverse trojans that covertly conduct various kinds of malicious activity

- Password stealers do just that – steal credentials and other critical information. Post mission, some clean up after themselves and self-destruct, such that victims remain unaware of the theft.

[Continue Reading >>](#)



- PUA (Potentially unwanted applications) often covertly install other software, including malware, on user machines.

[Continue Reading >>](#)



- Viruses impact computer functionality, impacting installed software, disrupting processes and destroying data.

- Backdoors are designed to provide clandestine access to victim machines. With such access, attackers are free to exploit compromised computers, recruiting them into botnets, infecting them with other malware, stealing information with keyloggers, etc.

[Continue Reading >>](#)



In Q3 2018, most attacks aimed to destroy enterprises digital assets and steal information. But the most intriguing and dangerous trend lies in hackers implanting long-lived malware to control compromised machines for covert use for various sustained criminal activities over a longer period. A long term approach lets attackers conduct multiple operations of different kinds utilizing infected machines, resulting in enterprise digital resources being used for cyberattacks and the onward spread of malware.

[BACK TO TABLE OF CONTENTS](#)



SUSTAINED 2018

TARGETED ATTACKS: ON ENTERPRISE BY MALWARE TYPE



Trojan Password Stealer

Sept 26.7%
Aug 14.1%
July 13.7%



Backdoor Attack

Sept 21.4%
Aug 8.1%
July 3.3%



Trojan Dropper

Sept 14.9%
Aug 25.1%
July 37.1%



P.U.A.

Sept 10.1%
Aug 18.4%
July 2.2%



Trojan Generic

Sept 8.5%
Aug 11.3%
July 2.0%



Trojan Downloader

Sept 6.7%
Aug 8.4%
July 1.6%



Virus Attack

Sept 3.9%
Aug 5.7%
July 38.1%



Worm

Sept 3.1%
Aug 3.4%
July 1.2%



Bot Attack

Sept 2.4%
Aug 1.9%
July .5%



Ransomware

Sept 1.5%
Aug 1.9%
July .3%



Rogue Attack

Sept .4%
Aug .3%
July .1%



Spyware

Sept .1%
Aug .1%
July .1%



Rootkit

Sept .1%
Aug .4%
July .2%



Remote Access Trojan

Sept .2%
Aug .3%
July .1%

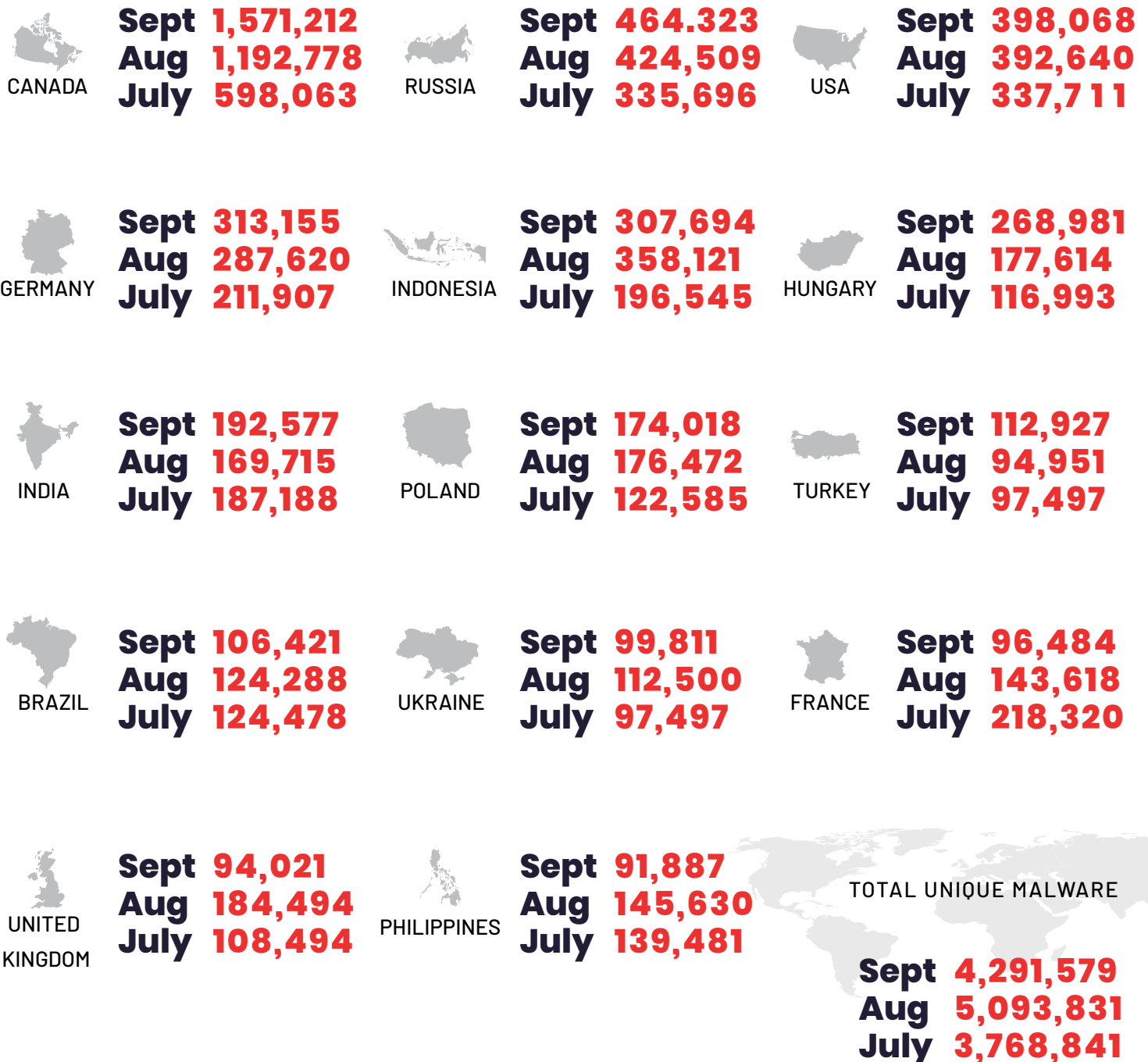
[BACK TO TABLE OF CONTENTS](#)



REGIONALITY OF CYBERCRIME

Canada happened to be the most malware-infested country throughout the entirety of Q3 2018, followed by Russia, USA, Germany and Indonesia. In July 2018, Indonesia ceded its place to France, as Indonesia slipped to sixth. But these 5 or 6 countries accounted for the lions share of malware attacks all through the quarter.

COUNTRIES MOST AFFECT BY UNIQUE MALWARE IN Q3 2018









[BACK TO TABLE OF CONTENTS](#)

REGIONALITY OF CYBERCRIME

With those half-dozen nations, we can narrow our focus to discover which cities in those affected countries bore the greatest brunt of malware. The norm is to target capitals and large financial centers, but interestingly, provincial cities with relatively small populations like Buzuluk and Yaroslavl (in Russia), and Andover and Ashburn (in the UK) detections appeared in the attackers' hit list as well. One possible explanation is that organizations in smaller cities lack adequate protection from cyberattacks (compared to their cosmopolitan counterparts) making them easy prey for perpetrators. The surge in attacking tier II urban areas seems to be a new and dangerous trend in cybercrime.

TOP FIVE CITIES BY COUNTRY AFFECTED BY UNIQUE MALWARE IN Q3 2018

01.  UNITED KINGDOM	Sept	ANDOVER 29,483	Aug	EASTBOURNE 80,056	July	EASTBOURNE 38,178
		LONDON 6,692		ANDOVER 38,734		LONDON 5,660
		WELLINGBOROUGH 4,300		LONDON 6,014		WELLINGBOROUGH 4,361
		BIRMINGHAM 3,152		WELLINGBOROUGH 4,878		CARDIFF 3,694
	LIVERPOOL 2,524		BIRMINGHAM 2,469		PONTYPRIDD 3,266	
02.  GERMANY	Sept	FRANKFURT 209,897	Aug	FRANKFURT 184,820	July	FRANKFURT 117,912
		BERLIN 11,987		MAGDEBURG 19,391		MAGDEBURG 12,810
		MAGDEBURG 11,241		BERLIN 10,961		BERLIN 11,818
		HAMBURG 6,017		MUNICH 6,839		MUNICH 6,421
	MUNICH 5,473		HAMBURG 6,376		HAMBURG 6,267	
03.  INDONESIA	Sept	SLEMAN 109,627	Aug	YOGYAKARTA 103,431	July	YOGYAKARTA 72,621
		YOGYAKARTA 59,523		SLEMAN 53,803		SURABAYA 36,368
		JAKARTA 38,152		SURAKARTA 48,796		JAKARTA 30,670
		BANDUNG 27,266		JAKARTA 39,501		BEKASI 12,684
	SURABAYA 17,034		SURABAYA 14,545		PONTIANAK 9,388	
04.  RUSSIA	Sept	MOSCOW 82,670	Aug	MOSCOW 77,522	July	MOSCOW 54,583
		IZHEVSK 80,951		BUZULUK 70,757		SAINT PETERSBURG 47,150
		BUZULUK 67,285		YEKATERINBURG 31,765		NOVOSIBIRSK 30,157
		SAINT PETERSBURG 40,779		SAINT PETERSBURG 25,049		BUZULUK 29,606
	NOVOSIBIRSK 19,468		YAROSLAVL 23,065		YAROSLAVL 20,543	
05.  CANADA	Sept	STONE CREEK 955,259	Aug	MONTREAL 593,161	July	MONTREAL 541,400
		MONTREAL 558,799		STONE CREEK 564,109		STONE CREEK 15,764
		TORONTO 7,653		TORONTO 9,732		TORONTO 8,184
		MISSISSAUGA 5,511		CALGARY 3,235		CALGARY 3,423
	EDMONTON 3,422		GATINEAU 2,755		MISSISSAUGA 2,670	
06.  USA	Sept	LITTLETON 34,013	Aug	MEAD 21,318	July	ASHBURN 21,548
		ASHBURN 23,616		ASHBURN 17,848		NEW YORK 10,872
		NEW YORK 10,816		NEW YORK 17,378		CHICAGO 9,006
		MORGANTON 8,410		LITTLETON 10,076		MORGANTON 8,581
	PEORIA 7,863		MORGANTON 8,423		HOUSTON 7,117	

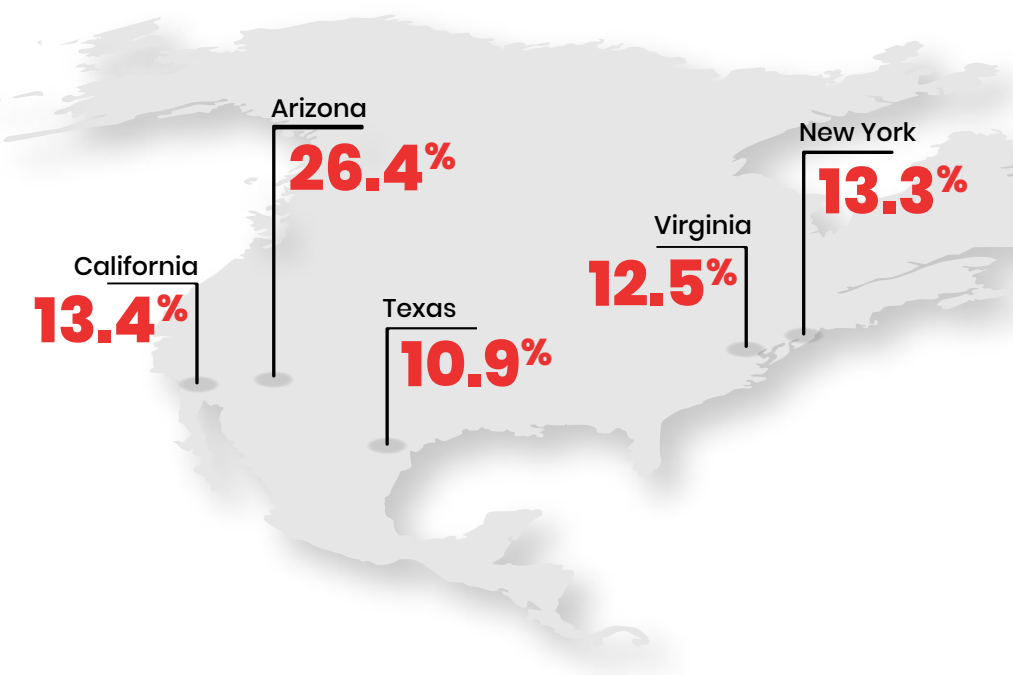
[BACK TO TABLE OF CONTENTS](#)

REGIONALITY OF CYBERCRIME

In the previous chapter, we examined phishing hosting trends by region. Let's now extend that analysis to hosting malware in general. In Q3, the US topped the list as hosting the most malware. Broken out by US states, the top 5 malware-infestations were Arizona, California, New York, Virginia, and Texas.

MALWARE HOSTING ACROSS THE UNITED STATES

1.	ARIZONA	26.40%
2.	CALIFORNIA	13.40%
3.	NEW YORK	13.30%
4.	VIRGINIA	12.50%
5.	TEXAS	10.90%
6.	MICHIGAN	5.10%
7.	FLORIDA	3.60%
8.	OREGON	3.40%
9.	NEW JERSEY	2.80%
10.	ILLINOIS	2.60%
11.	UTAH	2.50%
12.	GEORGIA	0.70%
13.	WASHINGTON	0.70%
14.	OHIO	0.50%
15.	MISSOURI	0.30%
16.	OKLAHOMA	0.30%
17.	INDIANA	0.20%
18.	NORTH CAROLINA	0.20%
19.	PENNSYLVANIA	0.20%
20.	COLORADO	0.10%
21.	IOWA	0.10%
22.	MARYLAND	0.10%
23.	MASSACHUSETTS	0.10%
24.	MINNESOTA	0.10%
25.	NEVADA	0.10%



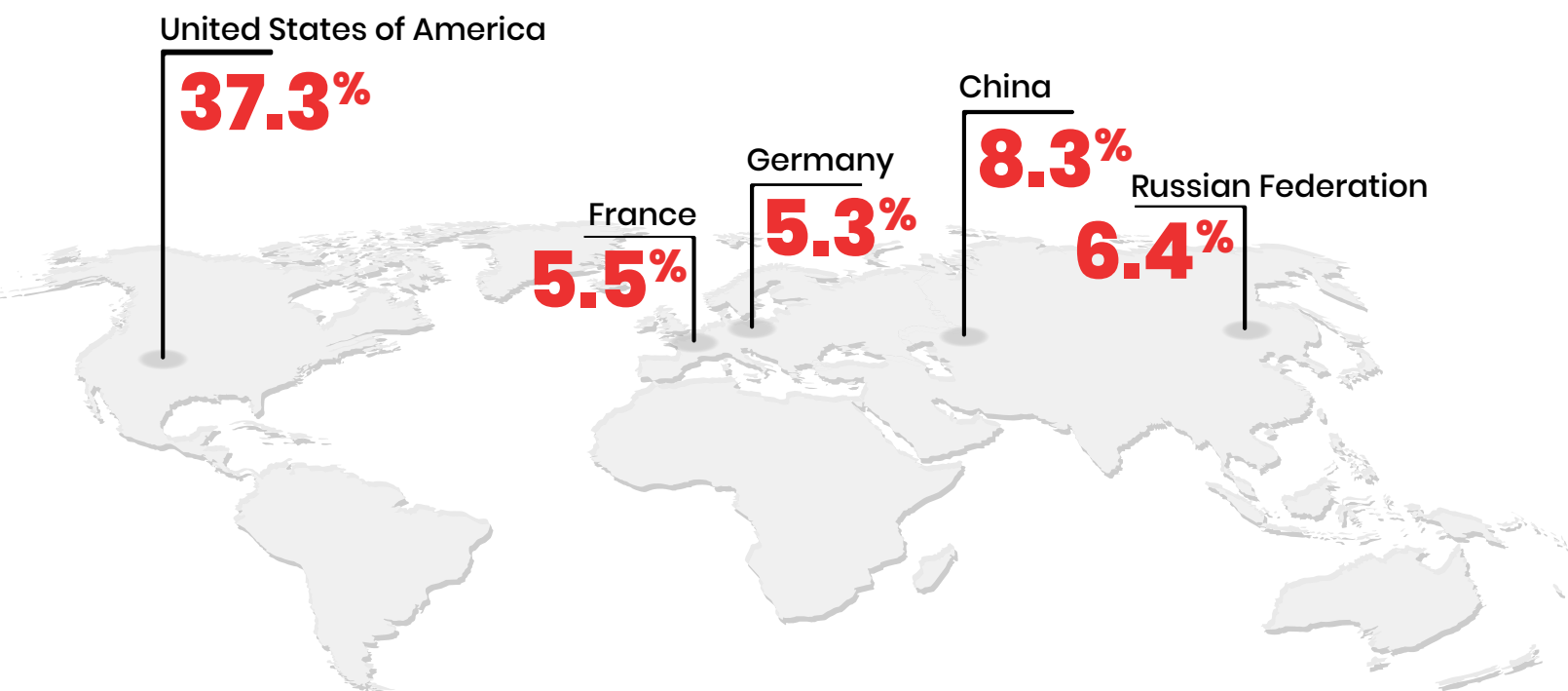
[BACK TO TABLE OF CONTENTS](#)

BOTNETS IN THE US HEARTLAND

Bots and botnets represent one of the greatest evils in the cyberspace. Botnet recruit swarms of infected computers, are managed by cybercriminals, and Borg-like constantly extend themselves by compromising new victims. Victims are seldom aware of being compromised, letting perpetrators covertly use computers and other devices for various malicious activities over extended periods. Infected machines send out spam, facilitate click fraud, conduct distributed denial-of-service (DDoS) attacks, etc.

In Q3 2018, the US, as with hosting malware and phishing websites, led other countries by a large margin, followed by China, Russia, France, and Germany.

BOTNET HOSTING BY COUNTRY

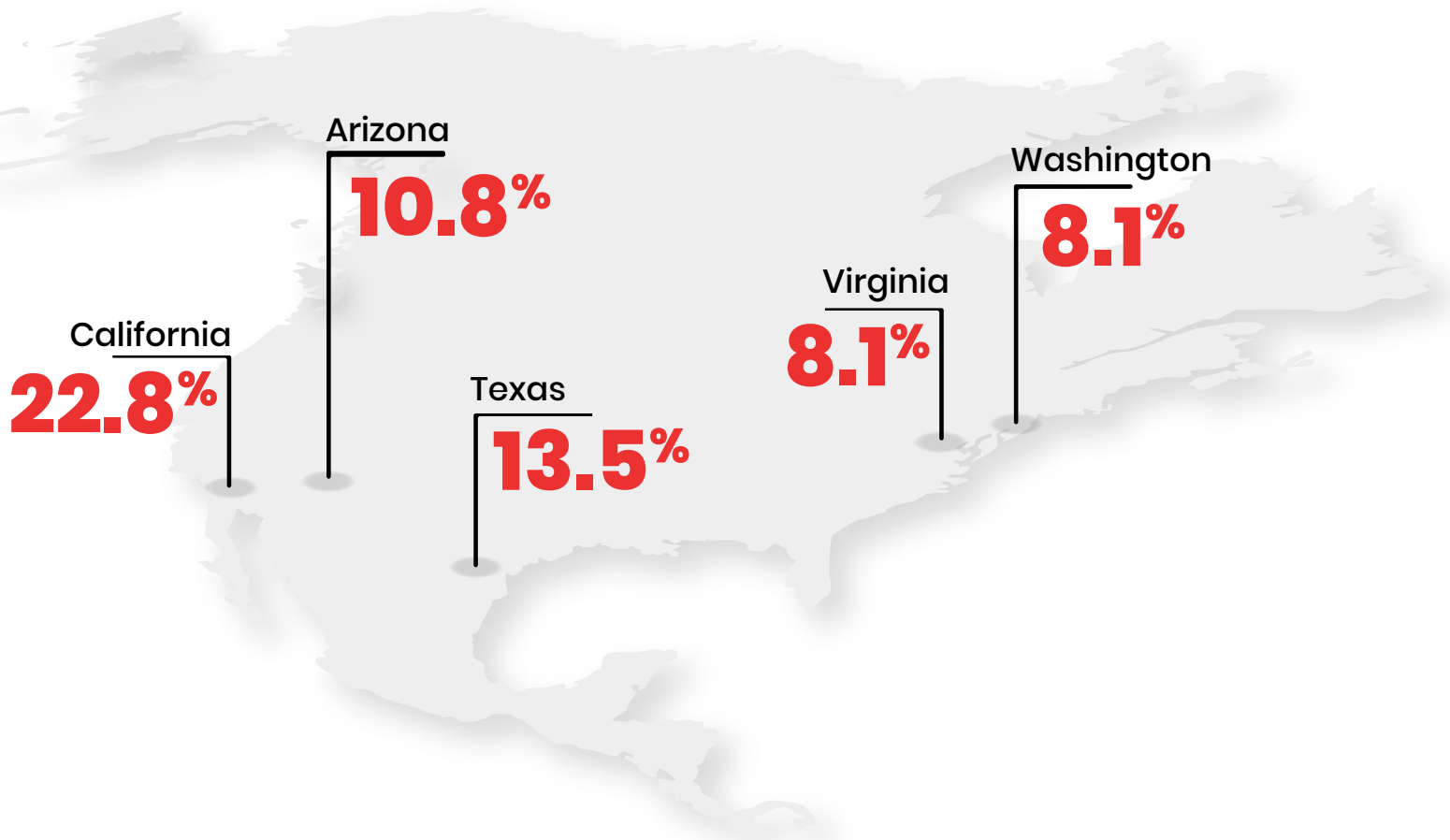


1. USA	37.30%	14. SPAIN	1.10%	27. BULGARIA	0.60%	40. KAZAKHSTAN	0.30%	53. SERBIA	0.10%
2. CHINA	8.30%	15. BRITISH VIRGIN ISLANDS	1.10%	28. ROMANIA	0.60%	41. SOUTH AFRICA	0.20%	54. AUSTRIA	0.10%
3. RUSSIA	6.40%	16. INDIA	1.00%	29. CZECHIA	0.60%	42. NORWAY	0.20%	55. CHILE	0.10%
4. FRANCE	5.50%	17. CANADA	1.00%	30. IRAN	0.60%	43. TAIWAN	0.20%	56. ESTONIA	0.10%
5. GERMANY	5.30%	18. DENMARK	0.90%	31. PORTUGAL	0.50%	44. MONTENEGRO	0.20%	57. MEXICO	0.10%
6. NETHERLANDS	4.50%	19. REPUBLIC OF KOREA	0.90%	32. PALESTINE	0.40%	45. NIGERIA	0.20%	58. CYPRUS	0.10%
7. BRAZIL	2.80%	20. ITALY	0.90%	33. SWEDEN	0.40%	46. EGYPT	0.20%	59. PANAMA	0.10%
8. TURKEY	2.30%	21. INDONESIA	0.80%	34. MONACO	0.40%	47. COLOMBIA	0.10%	60. LATVIA	0.10%
9. UNITED KINGDOM	1.90%	22. AUSTRALIA	0.80%	35. MALAYSIA	0.40%	48. NEW ZEALAND	0.10%	61. BELGIUM	0.10%
10. VIETNAM	1.70%	23. ALGERIA	0.80%	36. HUNGARY	0.40%	49. MOROCCO	0.10%	62. QATAR	0.10%
11. UKRAINE	1.50%	24. THAILAND	0.70%	37. FINLAND	0.30%	50. REPUBLIC OF LITHUANIA	0.10%	63. GREECE	0.10%
12. JAPAN	1.30%	25. POLAND	0.70%	38. SWITZERLAND	0.30%	51. SYRIA	0.10%	64. TUNISIA	0.10%
13. SINGAPORE	1.20%	26. IRELAND	0.60%	39. BELARUS	0.30%	52. ISRAEL	0.10%		

[BACK TO TABLE OF CONTENTS](#)

BOTNETS IN THE US HEARTLAND

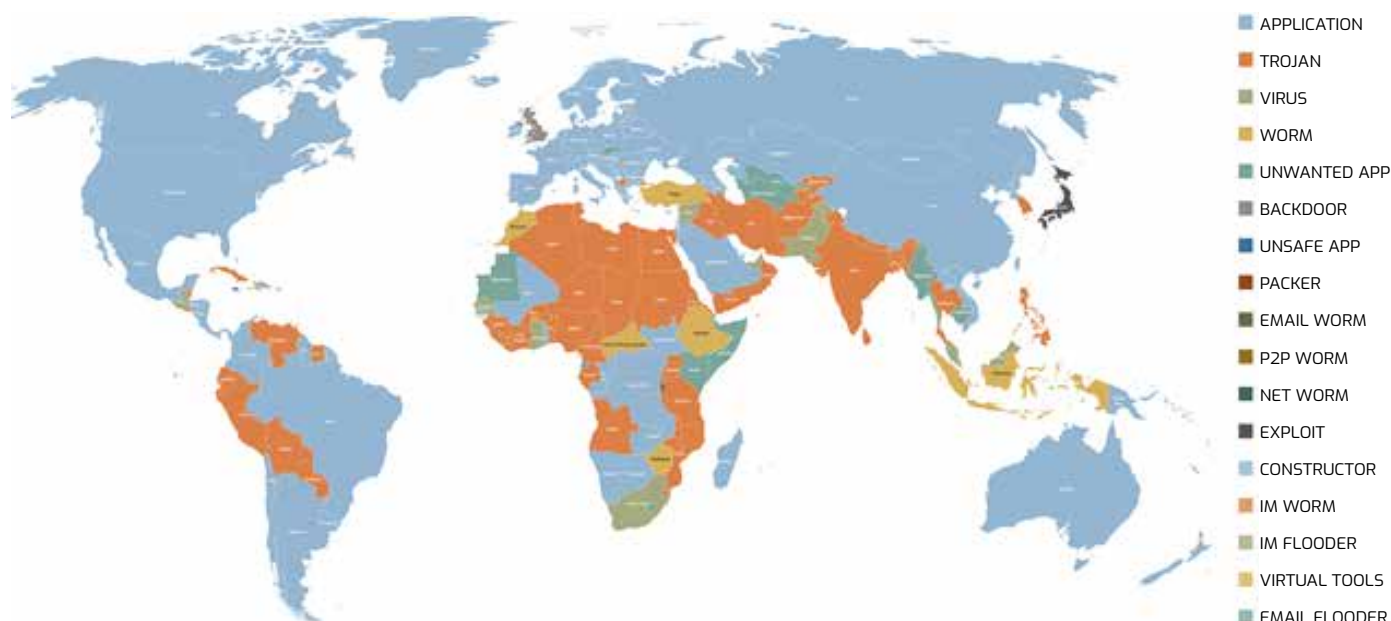
Within the US, botnet hosting breaks out across the following US states. Predictably, the top five US states for botnets are also the in hosting malware in general. The only change is New York replaced with Washington, reflecting the position of the US in the eye of the cybercrime storm.



1. CALIFORNIA	22.80%	9. NEW JERSEY	3.20%	17. OHIO	0.80%	25. DELAWARE	0.10%
2. TEXAS	13.50%	10. MASSACHUSETTS	2.90%	18. KANSAS	0.70%	26. DISTRICT OF COLUMBIA	0.10%
3. ARIZONA	10.80%	11. FLORIDA	2.70%	19. GEORGIA	0.60%	27. INDIANA	0.10%
4. VIRGINIA	8.10%	12. NEVADA	2.30%	20. NORTH CAROLINA	0.50%	28. MARYLAND	0.10%
5. WASHINGTON	8.10%	13. NEW YORK	2.20%	21. IOWA	0.40%	29. OKLAHOMA	0.10%
6. MICHIGAN	5.50%	14. MISSOURI	1.70%	22. COLORADO	0.20%	30. TENNESSEE	0.10%
7. UTAH	5.20%	15. OREGON	1.20%	23. MINNESOTA	0.20%	31. WISCONSIN	0.10%
8. ILLINOIS	4.10%	16. PENNSYLVANIA	1.20%	24. ALABAMA	0.10%	32. WYOMING	0.10%

[BACK TO TABLE OF CONTENTS](#)

GEOPOLITICS OF MALWARE



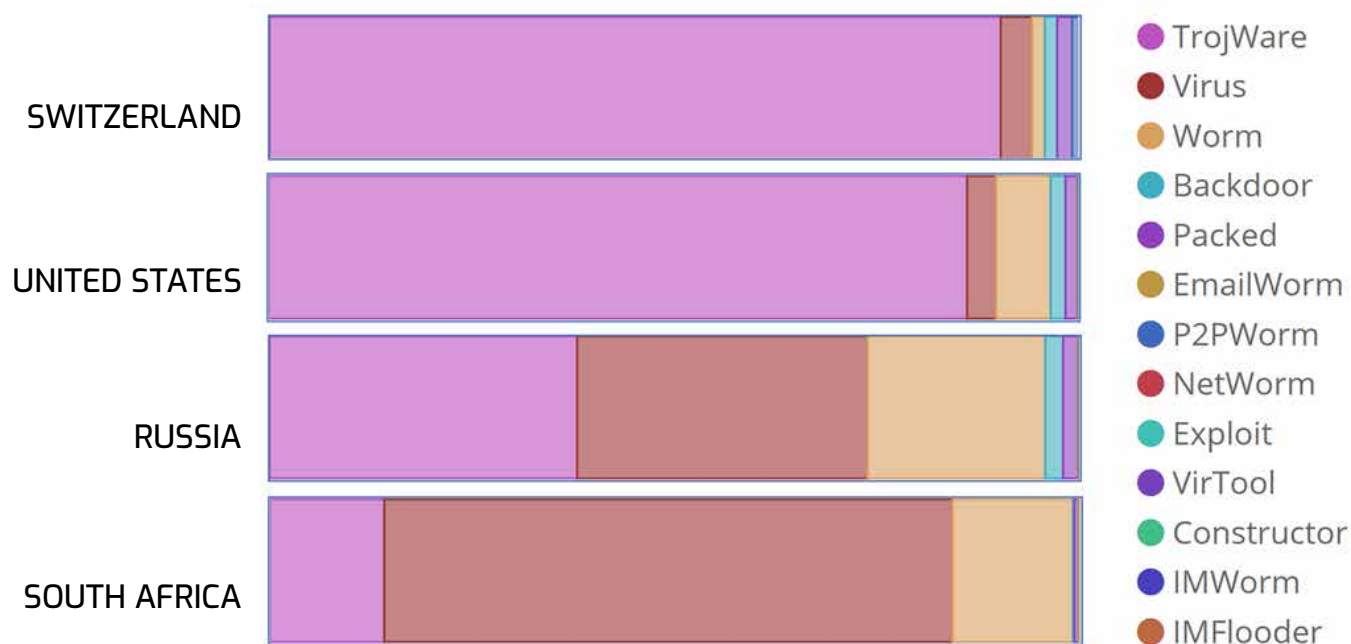
In previous sections, this report reiterated the fact that malware is both a global and local challenge for IT staff and end users. In this section, we'll examine malware detection in terms of strategic trends and correlations to current events in geopolitics.

The map above illustrates a high-level overview of the top 17 types of malware detected by Comodo Cybersecurity during Q3 2018. The map makes clear that the Internet is not a level playing field when it comes to malware. For example, the blue regions that dominate the northern hemisphere, large parts of South America and Australia represent application-level malware. This distribution shows that more wealthy, developed countries boast more modern and up-to-date software, properly licensed and professionally managed. But applications can include malicious code and "Potentially Unwanted Applications" or PUA. PUA operates somewhat like trojan horses, purporting to have benign functionality but installing files that run at startup, add drivers, inject processes, alter browser behavior, modify DNS settings, and more.

Another equally important phenomenon to notice on the map is how fraught southern hemisphere is with network-based malware. Relatively poorer nations and enterprises therein are more likely to deploy older, unlicensed, or unpatched software, accompanied by the gamut of malware.

[BACK TO TABLE OF CONTENTS](#)

SOCIOECONOMICS OF MALWARE



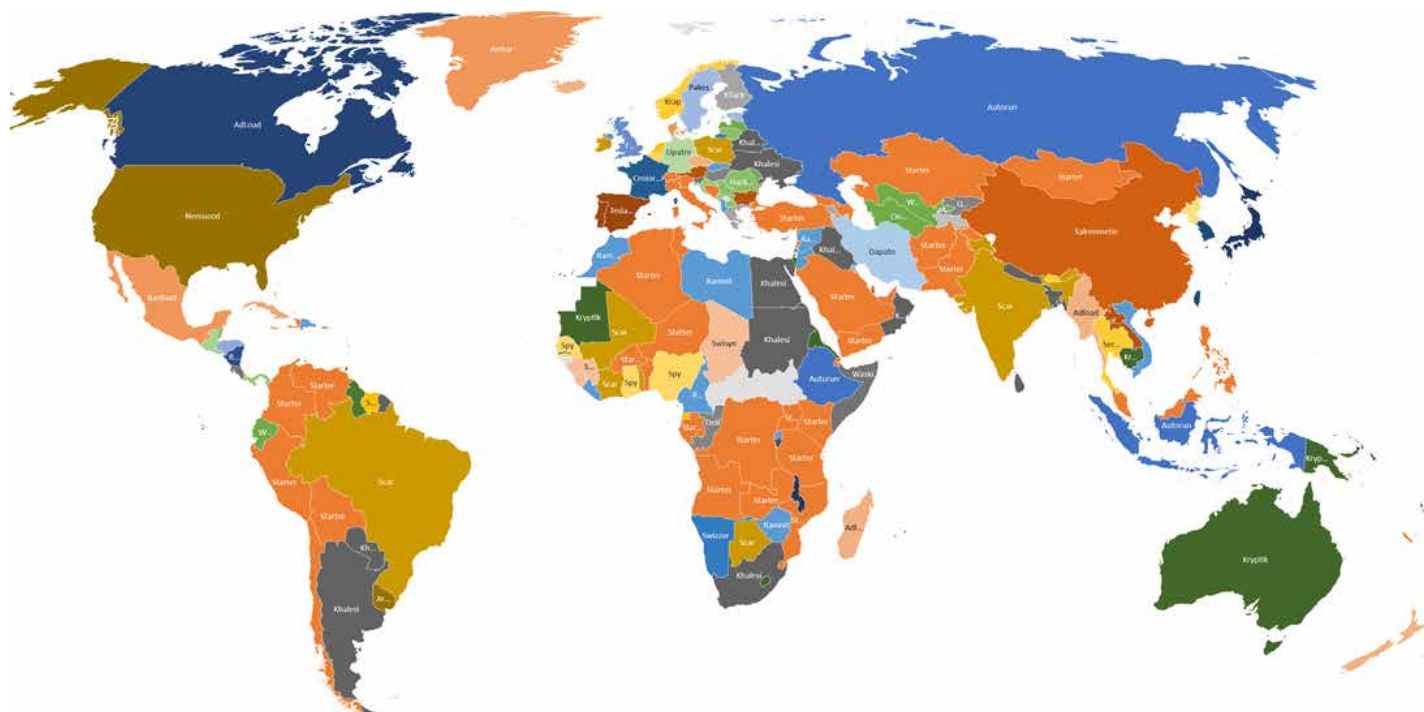
This next chart serves to strengthen this point. While exact proportions change over time, and there are exceptions, the relative affluence of a nation affects its malware profile. Each country is unique in cyberspace and so are the profiles of hackers and malicious code targeting them.

Switzerland, as a very rich, tightly-run country, has a very high percentage of trojans, and to a lesser degree, so does the United States. These countries easily afford the latest software and likely have professional cyber defense teams managing most of their networks. Thus, they are generally protected from older, random malware, especially viruses and worms, that can easily take advantage of gaping holes in network architecture, like older unpatched vulnerabilities. To penetrate Swiss or US networks, a hacker must employ a higher level of deception.

Conversely, Russian networks appear to be in very poor health, likely stemming from use of older and/or pirated software, notoriously difficult to update or patch. And finally, computers in South Africa unfortunately appear to be wide open to worms, which travel the Internet autonomously, and are capable of quickly compromising many computers over a short time span.

[BACK TO TABLE OF CONTENTS](#)

TOP TROJANS BY COUNTRY

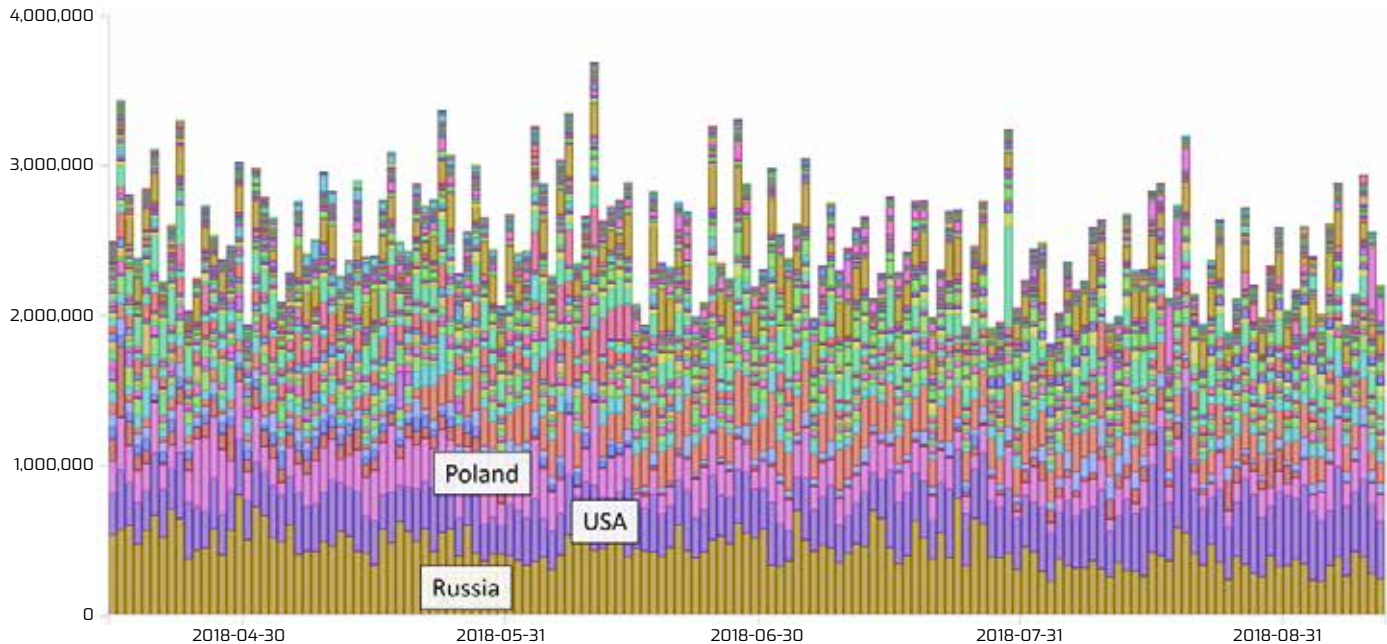


To highlight the complexity of each one of these malware types, let's take a closer look at just one – trojans – which are often the most common malware type in any nation. “Trojan” programs take their name from the famous wooden horse of Greek mythology, as they purport to have useful or benign functionality but in fact contain secret or hidden code that can steal, block, or alter data on the attacker’s whim. Trojans typically grant remote attackers the same rights and privileges as a local user. The map above shows the most common trojan family for each country. Here are the top ten trojans for Q3 2018, the number of raw detections worldwide, and the country where it was most often encountered.

1. Scar – 297,877 (Brazil)
2. Nemucod – 248,361 (USA)
3. ServStart – 138,438 (Thailand)
4. Autorun – 134,844 (Indonesia)
5. VB – 108,814 (El Salvador)
6. Salrenmetie – 98,489 (China)
7. Khalesi – 97,679 (Ukraine)
8. Paskod – 81,636 (Taiwan)
9. Starter – 68,127 (Philippines)
10. DataStealer – 65,080 (Cape Verde)

[BACK TO TABLE OF CONTENTS](#)

THE EBB AND FLOW OF MALWARE PROPAGATION



Plotting Q3 2018 malware detections (plus a bit more from the spring, which allows for a more strategic perspective) on a timeline, we arrive at a different understanding of the enormity of the challenge facing network security personnel. Today, network security personnel stand upon the shore of an ocean of malware, whose tide rolls in every day without fail.

In the graph, the three countries where Comodo detected the most malware in this period were Russia, the US and Poland.

This timeline encompasses a wealth of other cyber intelligence, including:

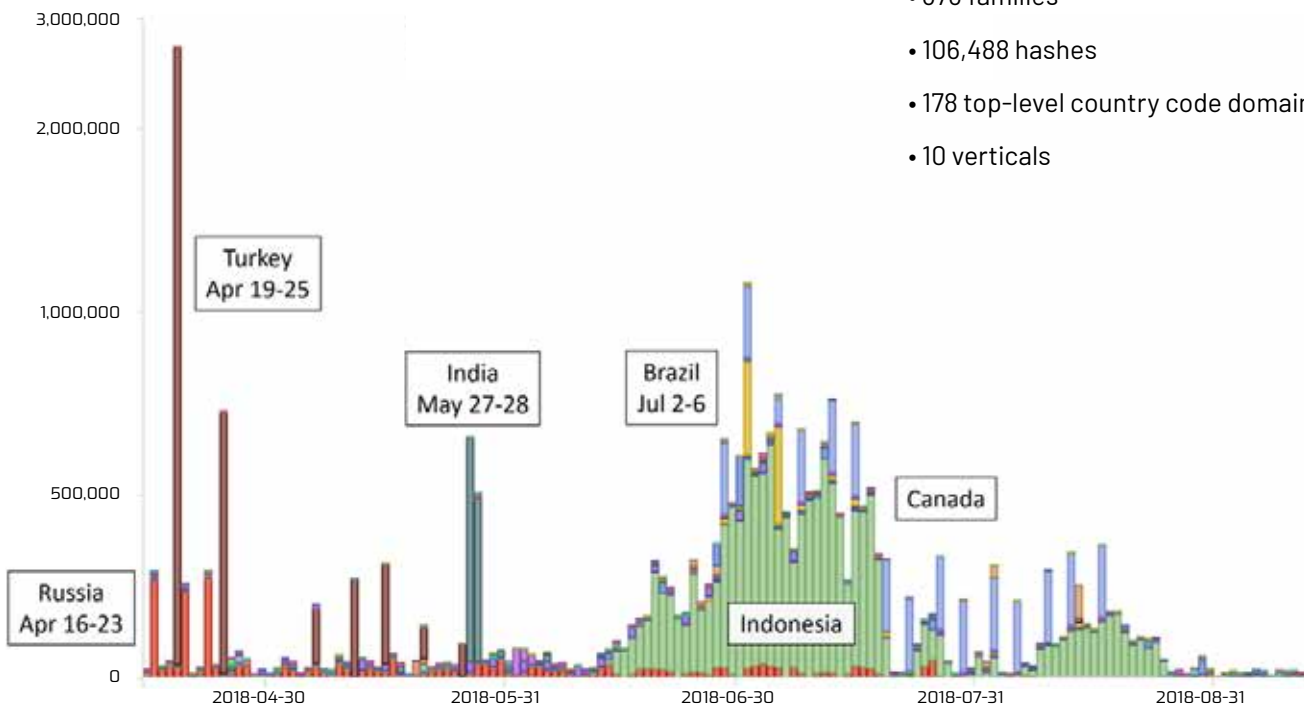
- 597,216,971 unique malware detections
- 9,691,896 malware hashes
- 6,209 malware families
- 238 country code top-level domains (ccTLD)
- 67,376 cities, and
- 27 economic verticals.

[BACK TO TABLE OF CONTENTS](#)

WORM DETECTIONS BY COUNTRY

Primary statistics for Q3 2018 worm detections:

- 373 families
- 106,488 hashes
- 178 top-level country code domains (ccTLD)
- 10 verticals



The analysis above is based on this extraordinary worldwide visibility.

A computer worm is like a virus, but typically travels autonomously, exploiting vulnerabilities in network defenses as it spreads across the Internet. Worms are designed as vehicles to deliver malicious payloads to victims' computers or networks. However, even worms without a payload can consume enormous bandwidth, diminish network or local system resources, and possibly cause a denial-of-service. Comodo considers computer worms to be a strategic cyber threat from their ability to travel quickly across the Internet and compromise many computers in a short time.

The timeline above shows the world's largest computer worm outbreaks over the past six months. They include:

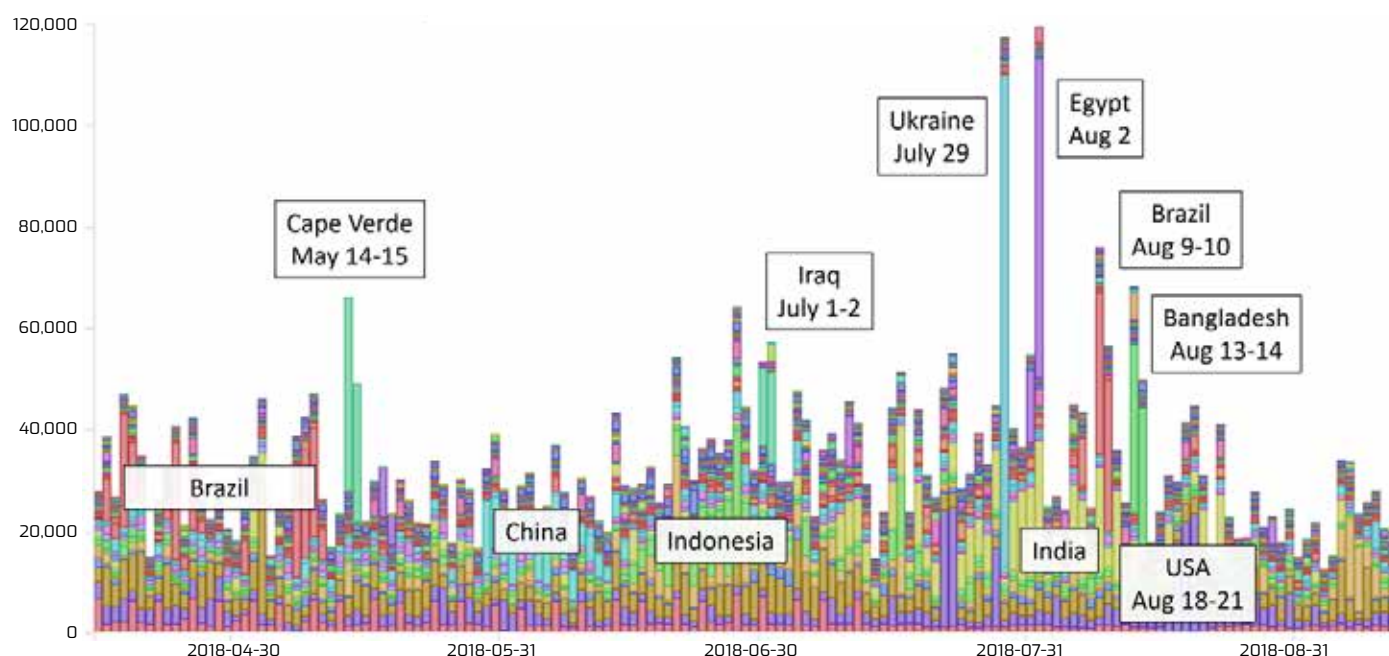
- Sharp spikes in Turkey and India, indicative of sudden, major malware outbreaks
- Numerous smaller spikes in Russia, Turkey, Brazil, and Canada, signaling a recurring problem with worms
- A massive wave of worms in Indonesia, indicating not only a targeted campaign, but one that may have successfully compromised a significant portion of Indonesian networks

The five most common computer worms were

- Autorun (1.5M)
- Brontok (843K detections)
- Conficker (257K detections)
- Nimda (171K detections)
- Gael (48K detections).

[BACK TO TABLE OF CONTENTS](#)

TROJAN DETECTIONS BY COUNTRY



Next, let's look at large-scale trojan infections across the globe. As noted earlier, trojans are not only the most common malware type, but they have flexible functionality which has earned them the moniker as the "Swiss Army Knife" of malware. They can be used for anything from innocent pranking to the installation and execution of ransomware.

Primary statistics for trojan detections during Q3 2018 are

- 1,998 malware families
- 634,959 hashes
- 217 ccTLD
- 21 industry verticals

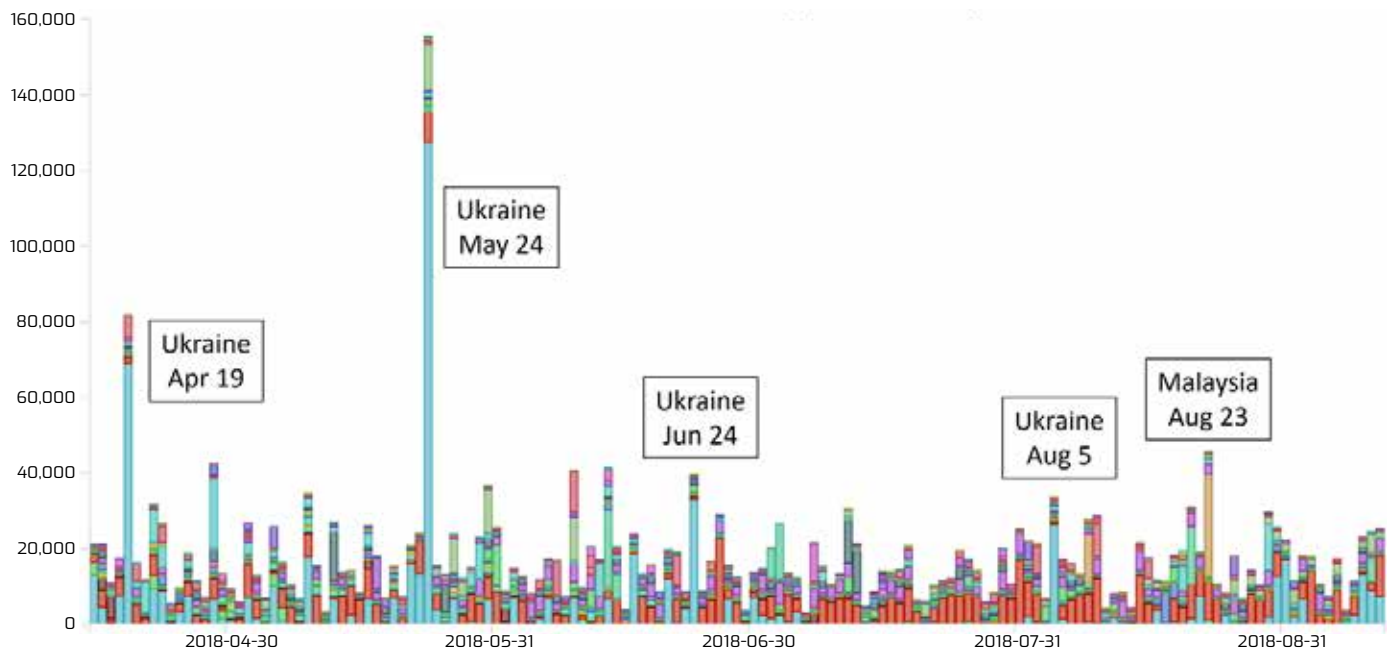
The timeline highlights how trojans come in all shapes and sizes, and infect diverse networks. Trojans constitute Comodo's largest single malware dataset, found across the most countries.

The highest single spikes were detected in Cape Verde (May 14-15), Iraq (July 1-2), Ukraine (July 29), Egypt (Aug 2), Brazil (Aug 9-10), and Bangladesh (Aug 13-14). Such high volumes of malware propagation may be due to the normal ebb and flow of cyber criminal malware, but could equally be related to geopolitical events within the countries in question, such as an election, international military tension, or internal political unrest.

The five most common trojans that Comodo detected were: Scar (298K), Nemucod (248K), ServStart (138K), Autorun (135K), and VB (109K).

[BACK TO TABLE OF CONTENTS](#)

VIRUS DETECTIONS BY COUNTRY



Consider computer viruses – self-replicating code that “infects” other computer programs and devices by corrupting them in malicious ways to facilitate data theft, spam dissemination, data destruction, and more. A virus usually cannot propagate across computers unless a user moves the infected file or performs some other action, e.g., opening an attachment or clicking a link.

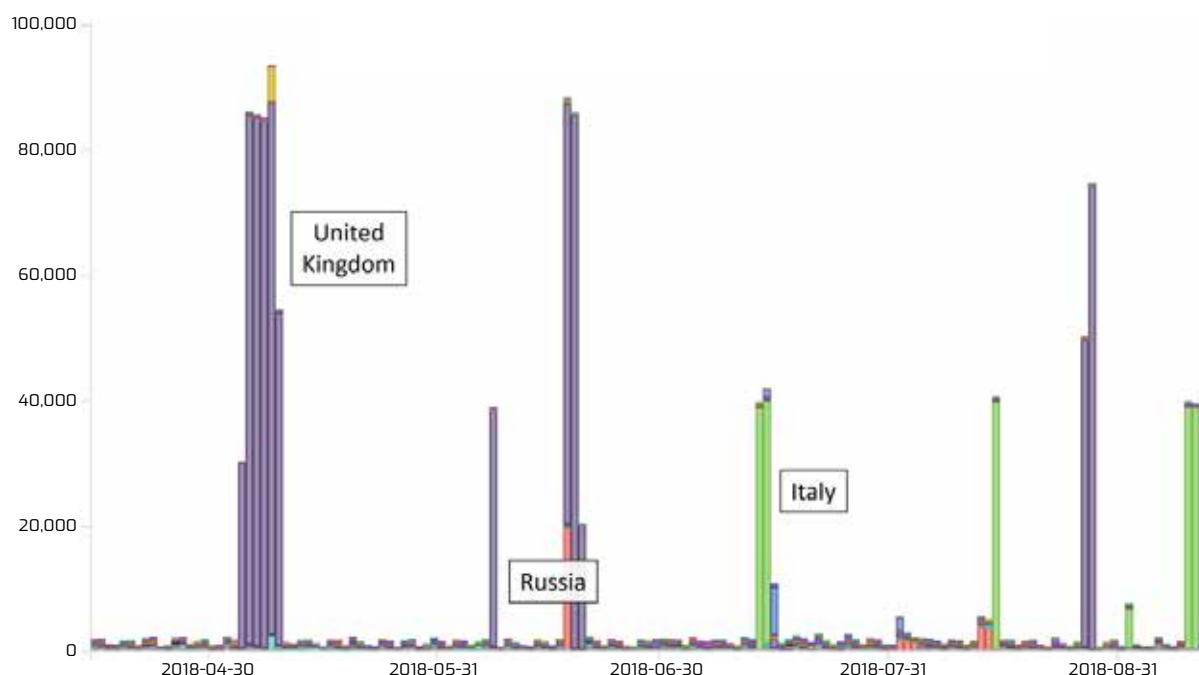
Comodo’s high-level statistics for detected viruses during Q3 2018 are

- 545 backdoor families
- 645,713 hashes
- 164 (country code top-level domains)
- 10 verticals

A quick look at the timeline clearly shows that Ukraine currently leads the world in computer viruses, by far. The five most common viruses in Ukraine during this timeframe were Ramnit (1.5M), DealPly (897K), Virut (740K), Expiro (578K), and Sality (252,867). The five most affected cities in Ukraine were Kyiv (2.1M), Lviv (1.3M), Zhytomyr (1.1M), Mariupol (1M), and Zaporozhye (698K detections). As might be expected of a country at war, many of these detections are likely associated with Ukraine’s ongoing conflict with Russia. On May 24, for example, there was heavy fighting in the country, as well as a claim by the Ukrainian government of a hostile cyber-attack attributed to Russia.

[BACK TO TABLE OF CONTENTS](#)

BACKDOOR DETECTIONS BY COUNTRY



Backdoors, which are a secret or hidden way to bypass normal user authentication. Black hats leverage backdoors leveraged to gain covert, remote access to computer systems, cryptosystems, or algorithm. A backdoor can be an installed program or a modification to an existing, legitimate program.

For this Q3 2018 report, Comodo Cybersecurity detected and analyzed the following backdoors

- 552 backdoor families
- 55,106 hashes
- 149 (country code top-level domains)
- 12 verticals

This graph is strikingly different from the other three. It appears to reflect not only major, but also recurring campaigns against certain countries. The United Kingdom is currently locked in a high stakes international contest with Russia over the alleged assassination attempt of a former Russian spy on British soil, which makes the nearly-simultaneous spike on particularly June 18 noteworthy. In the case of Italy, almost all of the detections were near Venice, giving the age-old practice of spying in this city a very modern look.

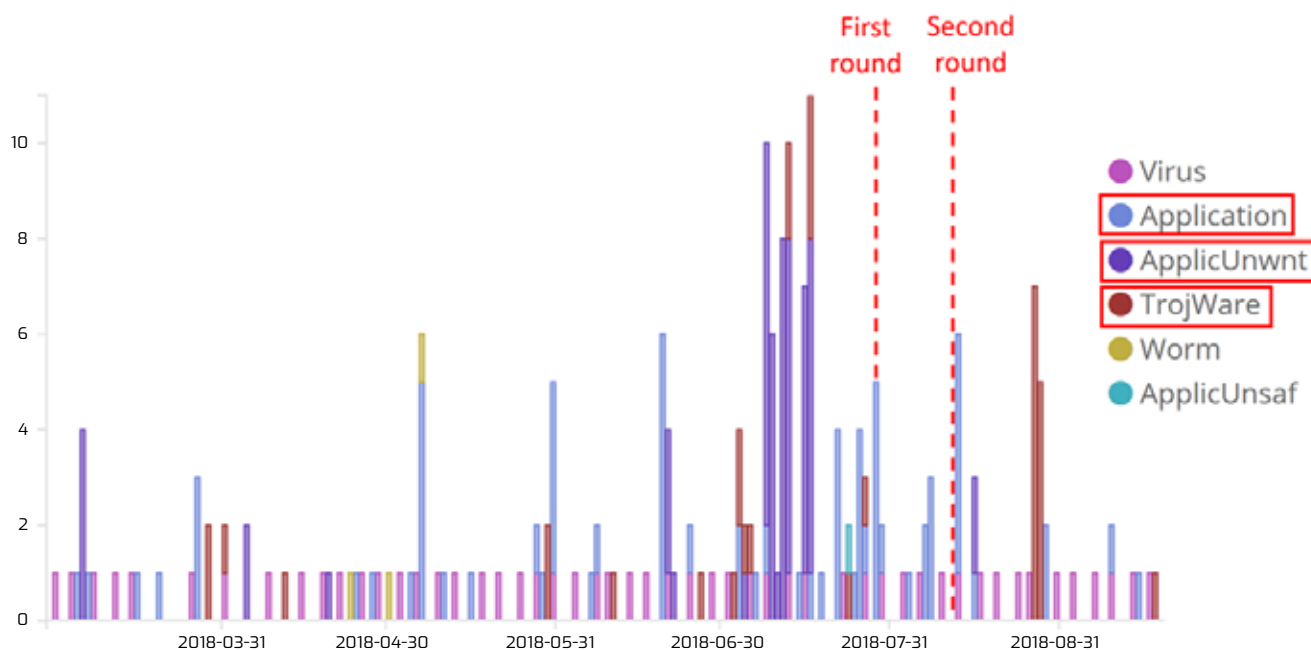
[BACK TO TABLE OF CONTENTS](#)

HACKING DEMOCRACY

As the November 2018 US Election approached, Comodo Cybersecurity detected a range of malware in and from other countries also holding elections. We will address six cases from very different parts of the world and provide strong evidence that malware now plays a major role in elections – no matter where they are held.

[BACK TO TABLE OF CONTENTS](#)

THE IMPACT OF MALWARE ON ELECTIONS: REPUBLIC OF MALI

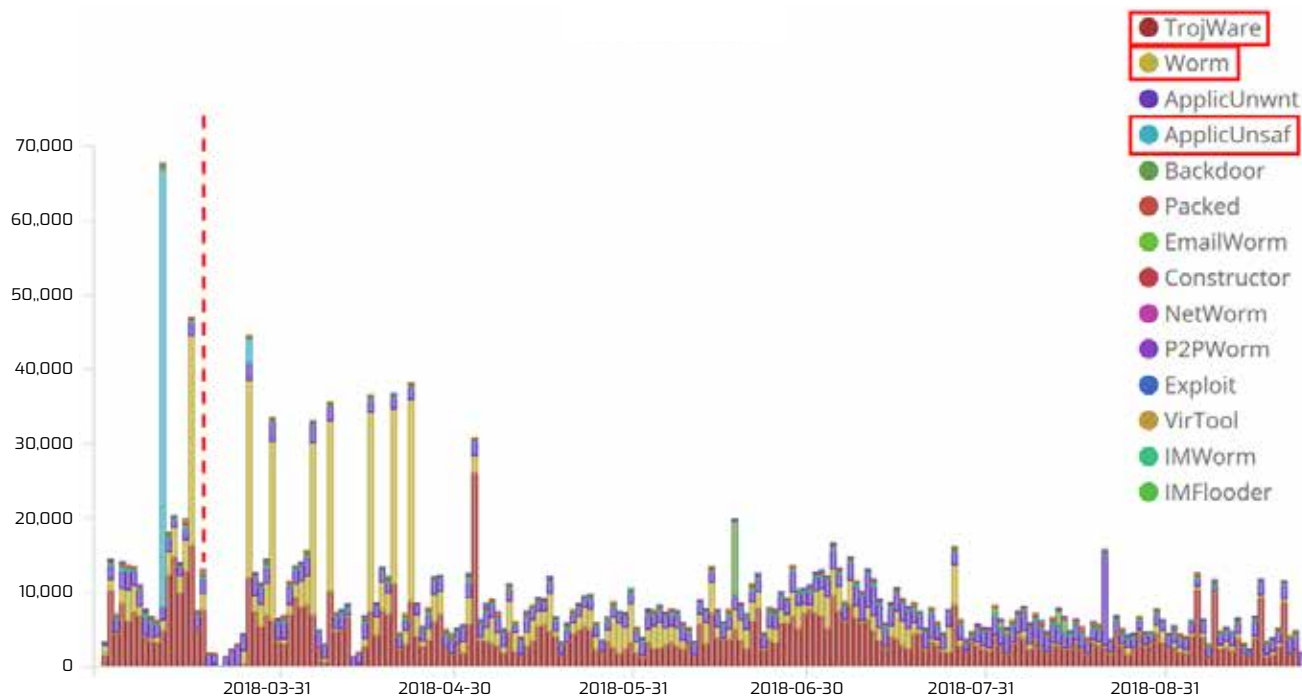


The African country of Mali held presidential elections on 29 July 2018. No candidate received more than 50% of the vote in the first round, triggering a runoff on 12 August 2018 between the top two candidates. As you can see in this Comodo malware detection timeline, the two polls in Mali were nicely bracketed by detections of malicious code. Just prior to the first vote, Mali saw a rash of commercial applications that exhibited suspicious behavior. Following the election, Comodo detected Mali’s highest spike in trojans, the most common of which belonged to the Scar family.

Pay attention to this ordering of malware, because we will see something very similar for subsequent elections in other countries. It appears that common, trusted applications may be used for data gathering including network reconnaissance, after which trojans, backdoors, and packed malware can leverage garnered intelligence for more targeted computer network operations.

[BACK TO TABLE OF CONTENTS](#)

THE IMPACT OF MALWARE ON ELECTIONS: THE RUSSIA FEDERATION



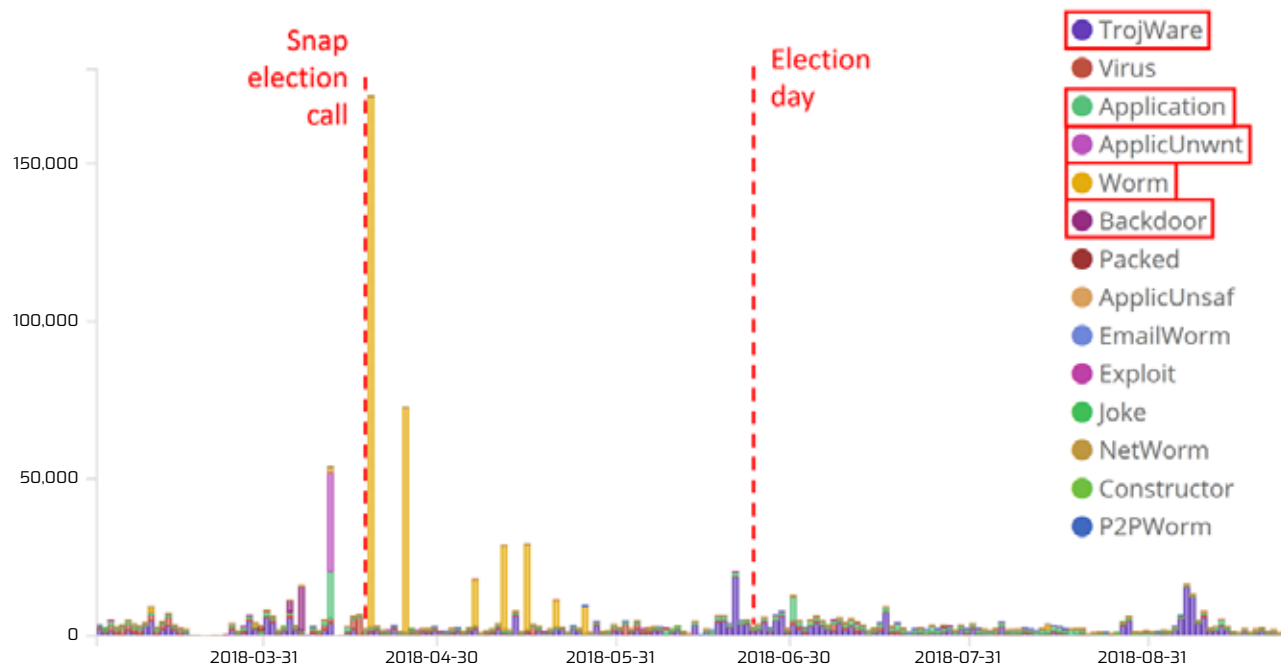
Russia held a presidential election on 18 March 2018. Incumbent Vladimir Putin won reelection for his second consecutive term in office with 77% of the vote. The Comodo malware timeline for Russia shows a fascinating pattern in which a massive spike of suspicious commercial applications preceded a violent period of computer worm detections (Conficker was the most frequent, followed by BrontoK detections).

The repeated worm activity suggests that these hackers were quite determined in the weeks following the election to insert malware onto Russian networks. Finally, at the beginning of May, this remarkable period of malware activity in Russia concluded with a sharp spike in trojan detections.

In Russia like Mali, note the order of operations: applications -> worms -> trojans.

[BACK TO TABLE OF CONTENTS](#)

THE IMPACT OF MALWARE ON ELECTIONS: REPUBLIC OF TURKEY



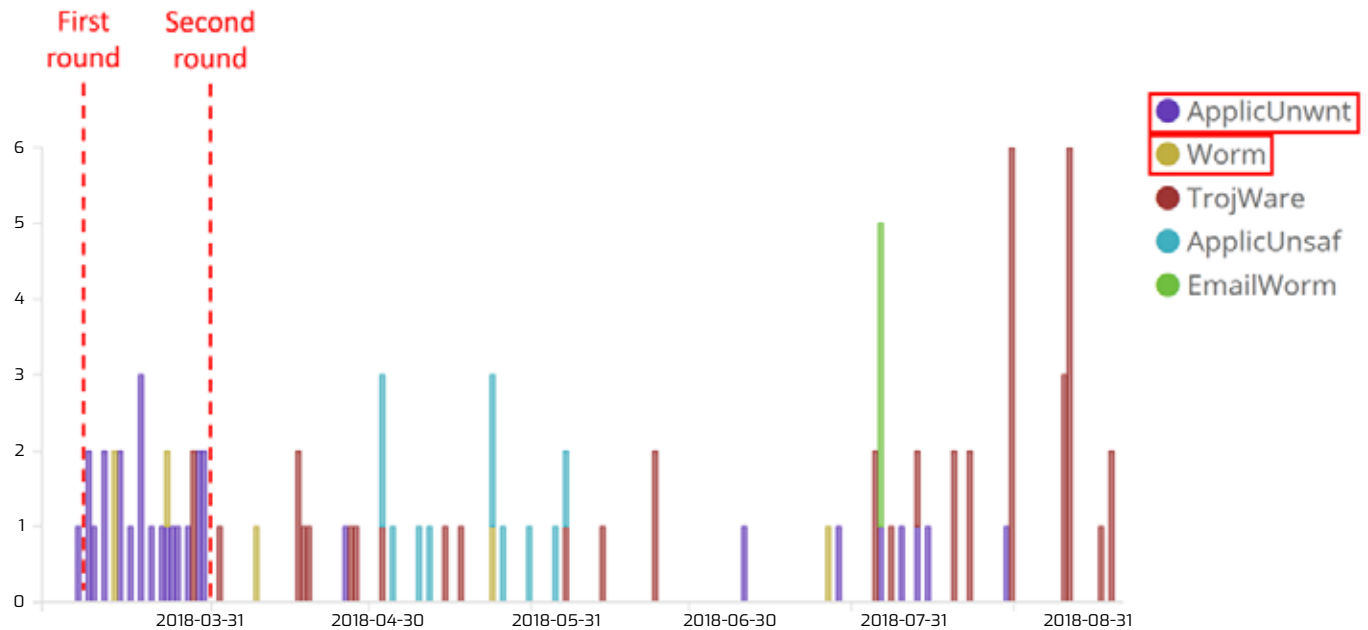
The Republic of Turkey held general elections on 24 June. Originally scheduled for 3 November 2019, President Recep Tayyip Erdoğan announced on 18 April 2018 that the vote would be brought forward, occurring well over one year early. Astonishingly, on 19 April – one day after the President’s announcement – Turkey experienced its highest single day volume of malware on this six-month timeline: a massive propagation of computer worms (99% of which were BrontoK detections). As with Mali and Russia, in hindsight we can see that this activity was preceded by detections of application malware.

Then, during the election itself, Comodo detected widespread trojan activity (including Agent, Starter, Ramnit, Winsecsrv, Delf, and more).

An added twist to this story, perhaps unrelated, is that Comodo’s largest detection of backdoors during this timeframe occurred on April 5 and April 7, even before the application activity. In this case (after the backdoor detections, which were smaller in scale), we again saw applications -> worms -> trojans.

[BACK TO TABLE OF CONTENTS](#)

THE IMPACT OF MALWARE ON ELECTIONS: REPUBLIC OF SIERRA LEONE



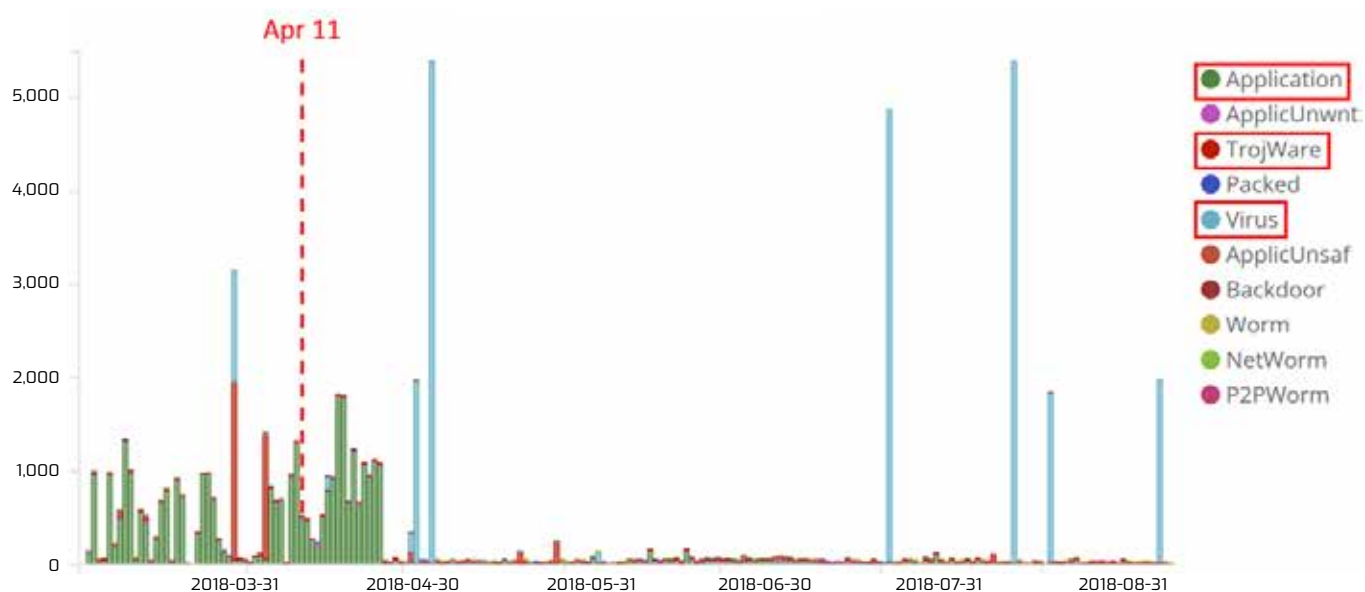
Turning our attention back to Africa, to Sierra Leone, where Presidential and Parliamentary elections took place on 7 March 2018. No candidate received the required 55% of the vote to win in the first round, so a second round of voting was held on 31 March between the top two candidates. Opposition leader Julius Maada Bio ultimately won with 51.8% of the vote.

In the timeline above, the most notable aspect is the right grouping of suspicious applications simultaneous to the two election events.

These were interspersed with computer worm detections (Nimda). And finally, even in this tight window, we see our now-common pattern of applications -> worms -> trojans. Nice right?

[BACK TO TABLE OF CONTENTS](#)

THE IMPACT OF MALWARE ON ELECTIONS: REPUBLIC OF AZERBAIJAN



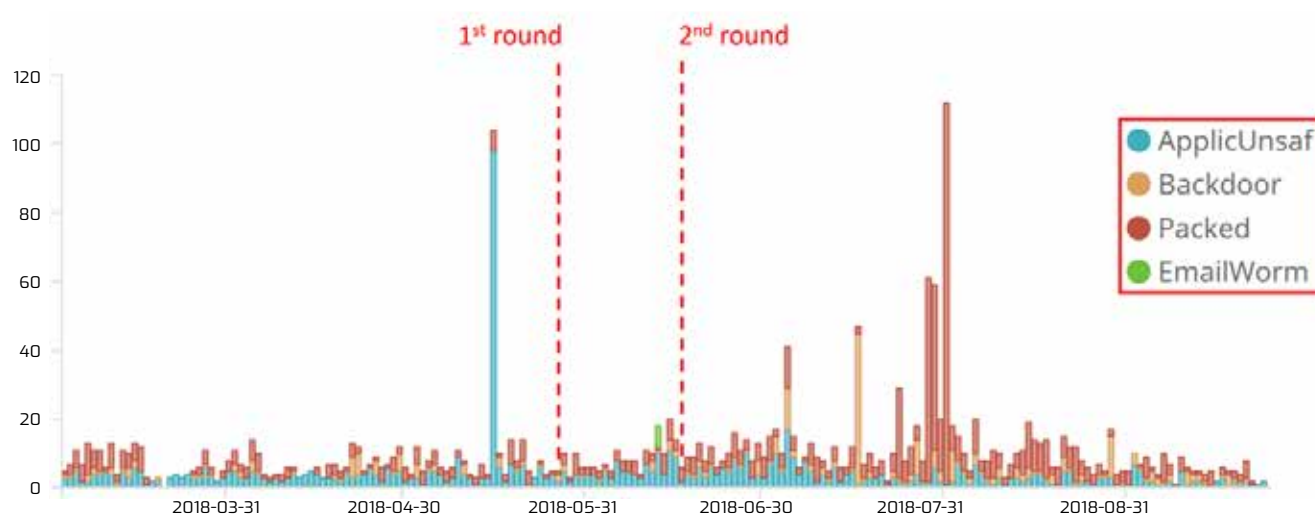
Azerbaijan held Presidential elections on 11 April 2018. Although many candidates were in the race, incumbent President Ilham Aliyev was re-elected President for a seven-year term.

This Comodo malware timeline is a bit different, but still has most of the same dynamics observed elsewhere. Here again application malware is followed by computer viruses (which play a similar role to computer worms in this case and were 99% Ramnit) and trojans (mostly Starter, but also Agent, Kryptik, and many more).

However, trojan activity this time preceded the actual vote. Therefore, this is a slightly different graph, but the primary takeaway is the same: who could argue that the large green cluster of application malware (accompanied by viruses and trojans) was unrelated to the Presidential election?

[BACK TO TABLE OF CONTENTS](#)

THE IMPACT OF MALWARE ON ELECTIONS: REPUBLIC OF COLOMBIA



Spinning the globe to South America, Presidential elections were held in Colombia on 27 May 2018. No candidate received a majority of the vote, so a second round of voting occurred on 17 June. This malware detection timeline shows that both events were encompassed by a fascinating pattern of malicious code. First, there was a large spike in unsafe applications that appeared just prior to the first round of voting. Second, an email worm (Runonce) appeared just prior to the second round of voting.

And finally, following both rounds, there were large spikes in backdoor detections (Poison, Xbot, Tofsee, Hupigon, IRCBot, NetWiredRC, Rbot and many more) as well as prominent detections in malware packers (MUPX, or the Modified “Ultimate Packer for Executables”).

As with most of the examples shown in this report, the first two malware outbreaks are logically tied to the propagation of malicious code, while the latter are reflections of hackers likely leveraging existing compromises for data theft and exfiltration.

[BACK TO TABLE OF CONTENTS](#)

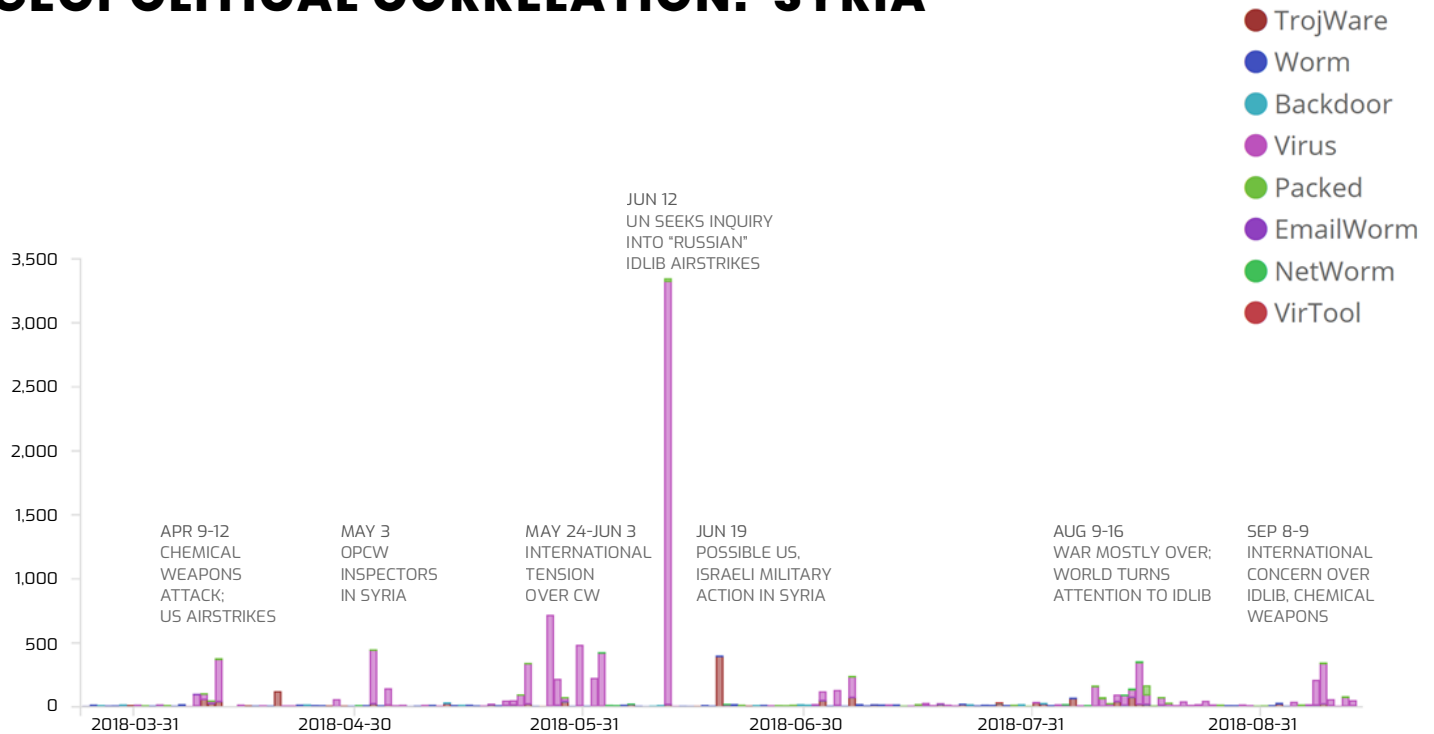
MALWARE & MILITARY OPS

Hackers not only pursue political intelligence, they provide support for ongoing military operations. Studying cyber-war can prove difficult due to the veil of secrecy surrounding nation state hacking. However, when a cybersecurity leader like Comodo, with ubiquitous presence on endpoints around the world, encounters upsurges in malware in conflict regions, reflections of those conflicts in cyberspace begin to stand out with great clarity.



[BACK TO TABLE OF CONTENTS](#)

MALWARE DETECTION & POSSIBLE GEOPOLITICAL CORRELATION: SYRIA

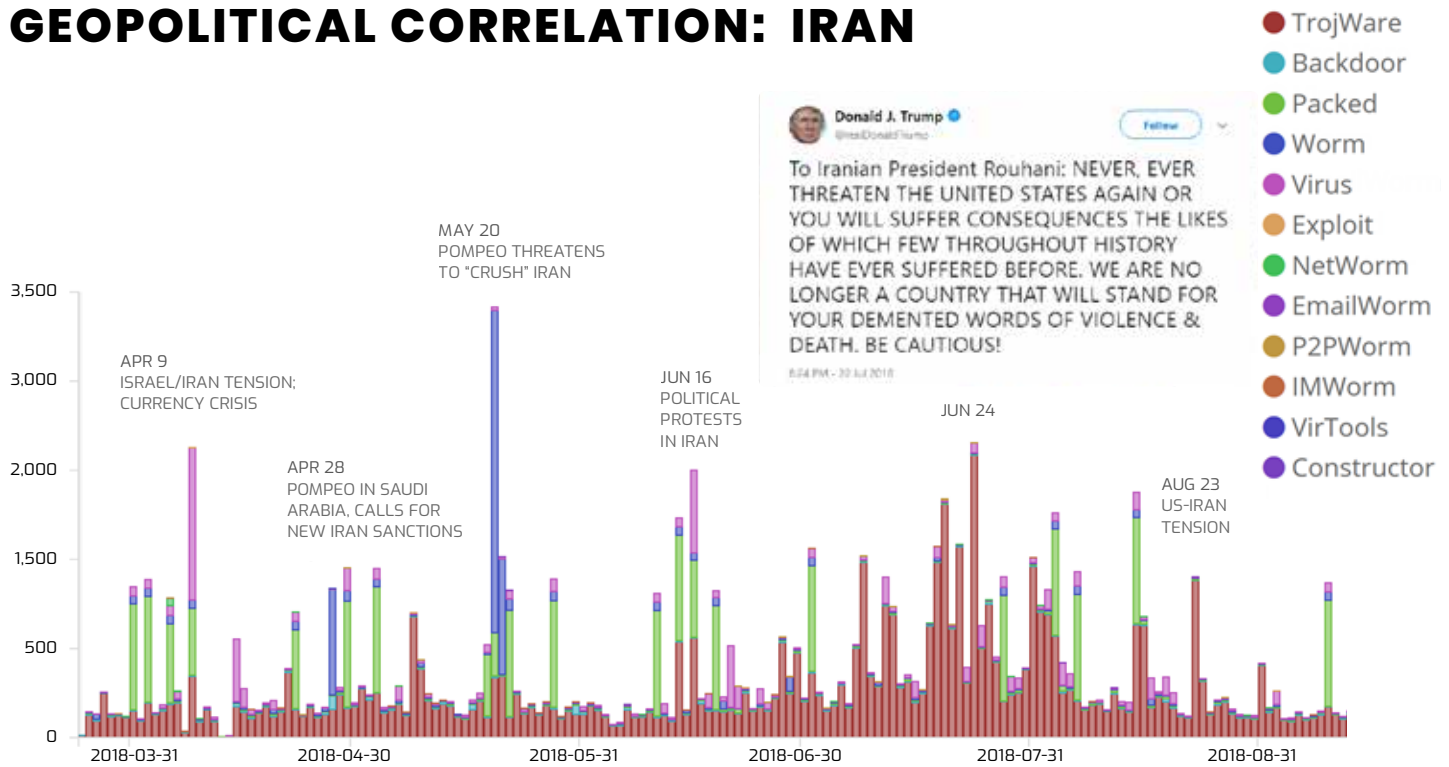


The timeline above shows malware detections in Syria over the last six months and lists possible real-world correlations. As Syria is a country at war, and nearly every medium- to great-power among nation-states seems to have an interest in its outcome, there should be little surprise that computer network operations are quite common within Syrian Internet protocol space. The current events in red, written just above the dates of the malware detections in black, describe in part what were the major stories happening in Syria at the time of detection.

What exactly is the correlation among malware and events in Syria? Above all, the most common correlation is cyber espionage, or an attempt by world powers to gather information from Syria, which is then quickly transformed into intelligence reporting that is read by national leadership. In Syria, the primary stories mentioned relate to the possible use of prohibited chemical weapons and the response of the international community to their suspected use.

[BACK TO TABLE OF CONTENTS](#)

MALWARE DETECTION & POSSIBLE GEOPOLITICAL CORRELATION: IRAN

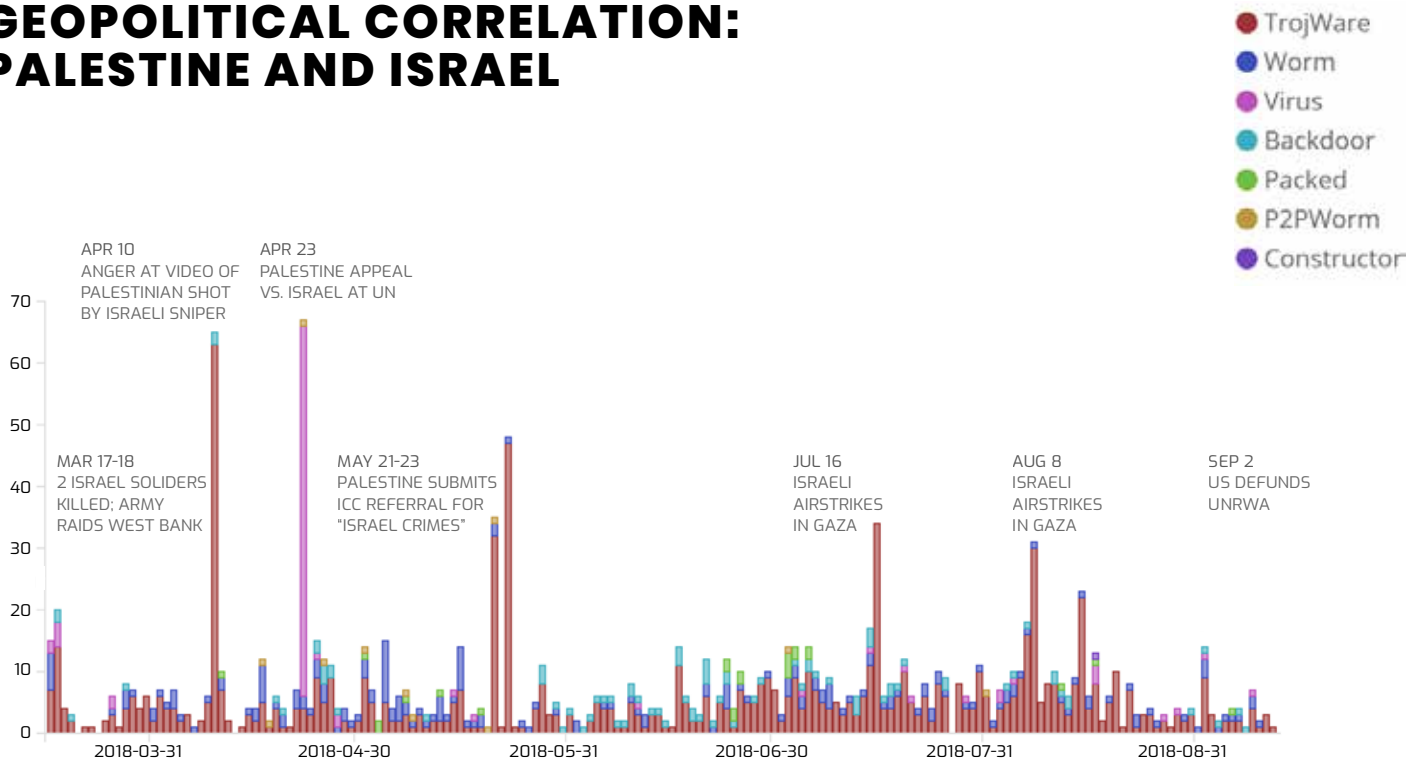


Comodo has great visibility into the cyber situation Iran, from data collected on the many endpoints protected there by Comodo tools. , as this chart shows not only more but also a wider range of malware detections. Notice how theThe different colors shown in the charthere depict different various types of malware that may be used for different kinds of computer network operations. The virus detections on April 9 are examples of file-changing malicious code that requires user interaction, such as opening an email attachment or clicking on a malicious hyperlink.

The blue lines on May 20-21 signify computer worm detections; worms can be even more dangerous than viruses because they travel the Internet independently and autonomously, taking advantage of vulnerabilities in network defenses at scale. The most interesting feature about this chart is likely the large red cluster toward the end of July, which was simultaneous to a sharp dispute with U.S. President Donald Trump, as clearly seen in his ALL-CAPITAL-LETTER tweet, threatening Iranian President Rouhani.

[BACK TO TABLE OF CONTENTS](#)

MALWARE DETECTION & POSSIBLE GEOPOLITICAL CORRELATION: PALESTINE AND ISRAEL



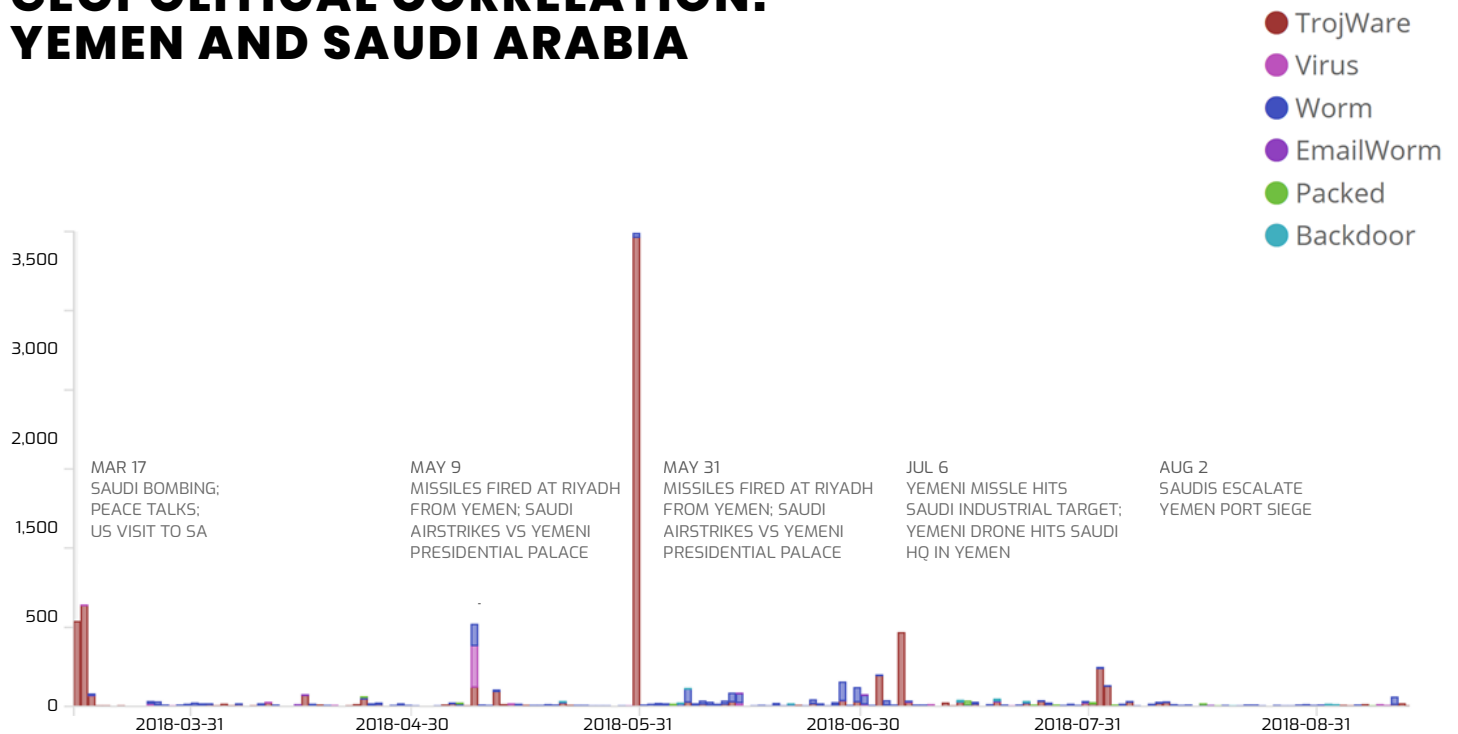
There exist relatively few published analyses of attacks within Palestinian National Authority network space. In part, this paucity of reporting arises from few companies having truly global visibility into cyberattacks. With the Comodo Cybersecurity global installed base of 100+ million endpoints, however, a panoply of threats and attacks within this contentious network domain become clearly visible. This year, as seen in the timeline above, it is possible to see malware detections that appear to be tightly correlated with real-world geopolitical events. Naturally, these detections occur during points of high tension with neighboring Israel.

Several events involve international interests, including the United Nations, the International Criminal Court, and the United States.

These are only possible geopolitical correlations. It is very difficult to prove causation, but this chart provides compelling evidence that computer network operations are being used as a force multiplier in many political, military, and intelligence operations, most likely in terms of cyber espionage. All of these events would be high collection priorities for numerous intelligence agencies, not just regionally but around the world.

[BACK TO TABLE OF CONTENTS](#)

MALWARE DETECTION & POSSIBLE GEOPOLITICAL CORRELATION: YEMEN AND SAUDI ARABIA



Finally, in Yemen, where there is also an ongoing war, and we can see instances where real-world conflict is visible in cyberspace. Such computer network operations are not only used for information gathering, but also in targeted operations in support of broader military objectives.

In this case, large malware spikes appear to be correlated to major events on the battlefield between Yemen and Saudi Arabia, providing a growing body of evidence for a burgeoning relationship between cyber operations and traditional military operations.

[BACK TO TABLE OF CONTENTS](#)

CONCLUSIONS

In Q3, 2018, Comodo Threat Research Labs encountered the gamut of malware. Standing out amidst the ever-growing threat barrage were a number of key trends

- Email continues as the attack vector of preference for malefactors around the world
- Black hats are deploying multi-pronged attacks – phishing, in particular – to deploy malware that includes trojan droppers, trojan generics, password stealers, PUA, backdoors and botnets
- Viruses continue to infect the world’s computers, as evidenced by the spike in July 2018
- And, while most threats occur over a short period of time, hackers are increasingly implementing various types of sustained and long-term attacks, implanting long-lived and “sleeper” malware, both to attack organizations and to use compromised resources to facilitate the further spread of malware
- Malware is regional – some countries and municipalities appear to be more vulnerable than others, attracting cybercrime and serving as the base for attacks on other geographies
- While cybercrime is primarily a for-profit activity, state actors and black hats are also leveraging malware and other threats to take down competition, besmirch reputations and influence elections

Fighting cybercrime and online threats is a grueling code war.

Comodo Cybersecurity is a front-line combatant, gathering intelligence via Comodo Threat Research Labs and joining the fray as customers deploy Comodo products and services to protect their LANs, web and cloud presence, and computing endpoints.

[BACK TO TABLE OF CONTENTS](#)



BROUGHT TO YOU BY



Comodo Threat Research Labs monitors, filters and analyzes the gamut of malware, ransomware, viruses and unknown potentially dangerous files 24/7/365 across 193 countries. With 5 sites in the Americas, Asia and Europe, the Lab comprises a team of 220 IT security professionals, ethical hackers, computer scientists and engineers to analyze millions of instances of malware, phishing, spam or other malicious/unwanted files and emails every day. The Lab collaborates with trusted partners in academia, government and industry to gain additional insight and fulfill its mission to use the best combination of cybersecurity technology and innovations, machine learning-powered analytics, artificial intelligence and human expertise to secure and protect Comodo Cybersecurity customers, partners and the public.

COMODO CYBERSECURITY

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats harmless, across the LAN, web and cloud. The Comodo One platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Comodo Cybersecurity has experts and analysts in 193 countries, protects 100 million endpoints and serves 200,000 customers globally. Based in Clifton, New Jersey, the company has a 20-year history of protecting the most sensitive data for both businesses and consumers worldwide. For more information, visit comodo.com or our blog. You can also follow Comodo on Twitter (@ComodoDesktop) and LinkedIn.

[BACK TO TABLE OF CONTENTS](#)



Global Threat Report

GTR

Edition

Q3

Year

2018



COMODO
CYBERSECURITY

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel: +1 (877) 712 1309

Tel: +1 (888) 551 1531

Fax: +1 (973) 777 4394

Inquire: sales@comodo.com

Support: c1-support@comodo.com

Visit comodo.com to learn more

BROUGHT TO YOU BY

 **COMODO**
Threat Research Labs

