Has The Sun Set On The Necurs Botnet?

shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/

March 15, 2020

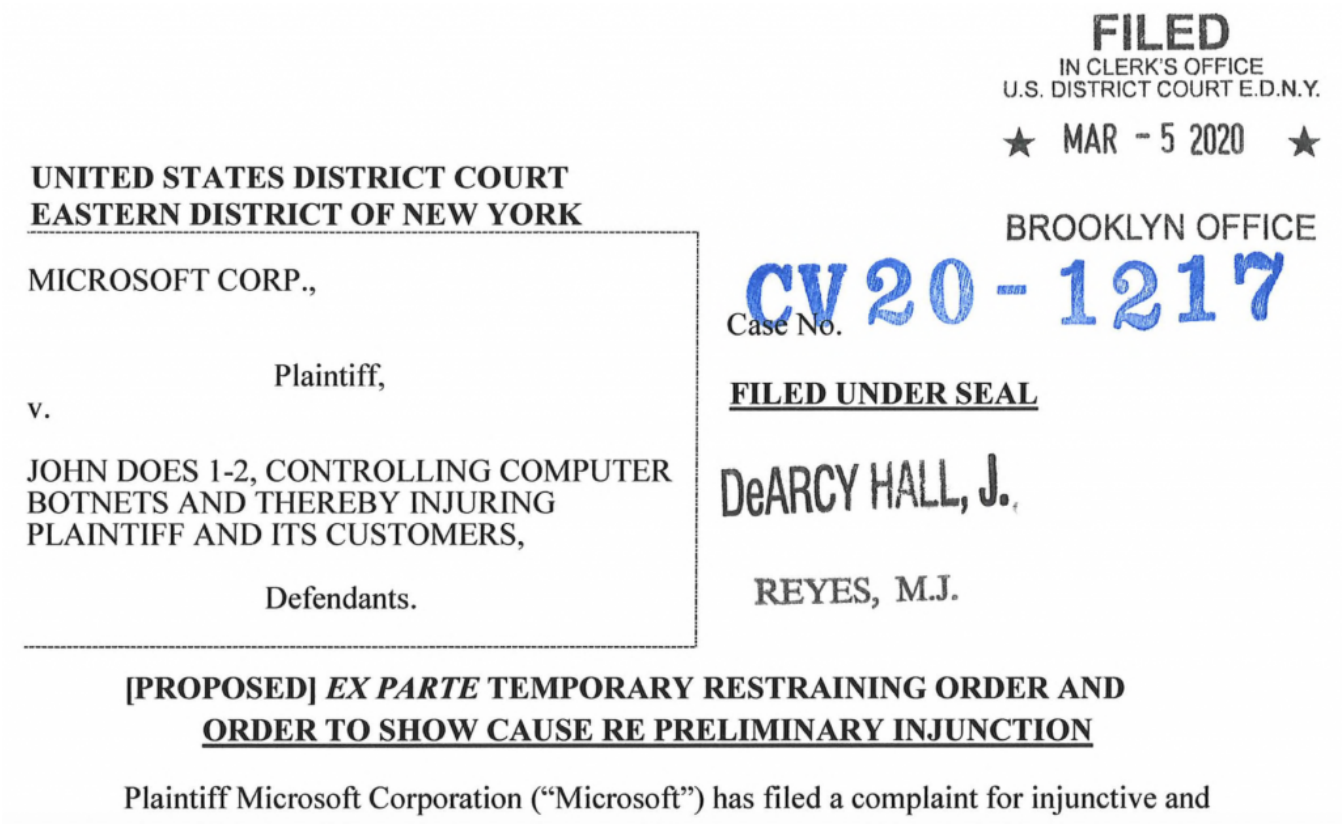
On **March 10th 2020**, while many people around the world were increasingly focused on the spreading COVID-19 pandemic, **Microsoft's Digital Crime Unit (DCU)** announced a disruption action against a long-lived and very damaging virtual threat – the **Necurs** botnet. Microsoft DCU described Necurs as "*the world's largest online criminal network*" responsible for "*infecting over 9 million users globally since 2012*". The Necurs botnet has historically been used to deliver a torrent of other high profile cyber threats to the world, including the GameOver Zeus and Dridex banking trojans, **Locky** ransomware and, more recently, the banking trojan turned all purpose cybercrime-as-a-service, **Trickbot**. It has also been used to promote pump-and-dump stock scams, fake pharmaceutical spam emails and "Russian dating" scams.

Shadowserver has previously collaborated with Microsoft DCU on successful botnet takedowns, such as the Waledec spambot and the Andromeda malware dropper (part of Avalanche). It has also assisted with the take down of other historic spambots by collaborating with private partners (**Grum**) and with Law Enforcement, such as against various versions of Kelihos with the FBI, DoJ and other private sector partners. Microsoft DCU and Bitsight had conducted a multi-year investigation into Necurs, and Shadowserver was asked to support their disruption efforts once an action plan had been agreed.

We would usually provide in-depth details here about the technical functionality of the Necurs malware, reverse engineering information, the use of multiple layers of Domain Generation Algorithms (DGAs) – including .bit for blockchain based name to IP address resolution, the tiered command and control (C2) infrastructure, the structure of the multiple sub-botnets or the disruption strategies employed, but we recommend you read Bitsight's already published series of excellent Necurs articles. We will instead focus on some other interesting aspects of the Necurs disruption operation.

Registry Actions

Some botnet takedowns are purely criminal cases, performed by Law Enforcement Agencies using criminal laws – although, not every country has developed such legislation. In some countries, particularly the USA, LEAs can use civil legal orders in the fight against cybercrime. This avenue is also open to private sector organizations; indeed, Microsoft has previously used civil court orders to tackle large botnets. Where the name of a suspect behind the botnet is **not** known, but damages can be demonstrated, it is still possible for a plaintiff (in this case Microsoft) to make an "ex parte" (meaning in the interests of one side, when the other side is not present) "John Doe" complaint through a civil court. If successful, a judge can issue a Temporary Restraining Order (TRO) that grants injunctive relief to the plaintiff. This is the legal approach that was adopted by Microsoft in regards to Necurs. You can view the Eastern District of New York court documents here and read the wording of its TRO application here.



FILED
IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.
★ MAR - 5 2020 ★
BROOKLYN OFFICE

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP.,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Case No. CV 20 - 1217

FILED UNDER SEAL

DeARCY HALL, J.

REYES, M.J.

[PROPOSED] *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft") has filed a complaint for injunctive and

Microsoft Necurs Ex Parte Temporary Restraining Order (TRO)

Shadowserver were on site with Bitsight and Microsoft at its Digital Crime Center in Redmond, WA, USA to support the Necurs disruption effort. Our contribution to the operation was primarily in two areas:

1. Coordinating with our extensive, international network of country-code, top-level, domain (ccTLD) Registry operators who trust us to report malware to them that uses millions of unregistered DGA domains, as in previous large botnet takedown operations such as Avalanche.
2. Using Shadowserver's proven victim remediation network, of 107 National CERTs/CSIRTs in 136 countries and over 4,600 vetted network owners (covering 90% of the Internet by IP space/ASN/CIDR), to ensure that the collected sinkhole data was quickly distributed to as many constituents as possible, in order to maximize world-wide victim remediation. Data is also available through Microsoft CTIP and Bitsight's commercial services.

Our special purpose **The Registrar of Last Resort Foundation** (RoLR), another Dutch Stichting non-profit, public-benefit organization, created specifically by Shadowserver to quarantine toxic domain names, provided crucial support to the Necurs disruption activities. Voluntary action was successfully secured across **22 ccTLD registries**, complementing Microsoft's US civil court orders, which had been executed on 5 US-based registries.

The Necurs botnet makes use of hardcoded domains and multiple layers of DGAs to attempt to guarantee reliable command and control (C2) capabilities. Since the Necurs DGAs and seed values had been reverse engineered by security researchers and reimplemented in code, 25 months of future domains could be forward calculated (a total of **6.1 million** potential botnet C2 domains across **42 TLDs**).

Under the wording of Microsoft's civil court ordered TRO, all existing Necurs botnet C2 domain names (except those determined to belong to legitimate security researchers) within US-operated TLDs should be seized and sinkholed by the Registry. Any unregistered DGA domain names would be blocked so that they could not be registered in the future – except by "*Microsoft or its security industry partners Stichting The Registrar of Last Resort Foundation and The Shadowserver Foundation for the purposes of analyzing the botnet*".

third party. "Dynamically generated domains" shall mean the discrete list of domains automatically generated by the botnet software running on test machines in a laboratory environment and which is not subject to discretion. Nothing in the foregoing shall prevent registration or activation of the domains by Microsoft or its security industry partners Stichting Registrar of Last Resort Foundation and The Shadowserver Foundation for purposes of analysis of the botnet.

Microsoft Necurs Ex Parte Temporary Restraining Order (TRO) Wording

Shortly before the operation took place, a subset of the pre-calculated domains for all of the **Necurs 5,7,9,11,13 and 15 sub-botnets** was registered and pointed to Microsoft's and Bitsight's sinkhole servers, to ensure that all infected victims would attempt to resolve at least one sinkholed botnet C2 domain and communicate with at least one sinkhole server every day; hopefully, without being able to communicate with the criminals operating the botnet. This approach allows the victim population to be identified and hopefully remediated, while minimizing the number of potential DGA C2 domains that actually have to be registered (around a thousand C2 domains per year, rather than the potentially millions of C2 domains).

RoLR was used to register Necurs C2 domains for sinkholing purposes and to manage the ongoing maintenance and renewal of the domains. The actions of breaking the DNS resolution of criminal controlled C2 domains, and instead delivering infected victim computers to the Microsoft and Bitsight sinkhole servers, attempts to protect victims from further criminal abuse, and allows National CERTs/CSIRTs and responsible network owners to be notified to remediate those infections. The Necurs disruption sinkhole data is available through Microsoft's CTIP service, Bitsight's commercial service and Shadowserver's free daily network reports. If you or your organization do not already subscribe to this **free public benefit service**, then please do sign up.

The TLDs used by the Necurs botnet for C2 communications were:

ccTLDs: .ac, .bz, .cc, .cm, .co, .cx, .de, .eu, .ga, .im, .in, .ir, .jp, .ki, .kz, .la, .me, .mn, .ms, .mu, .mx, .nf, .nu, .pw, .ru, .sc, .sh, .so, .su, .sx, .to, .tv, .tw, .ug, .us, .tj

gTLDs / **nTLDs**: .biz, .com, .net, .org, .pro, .xxx

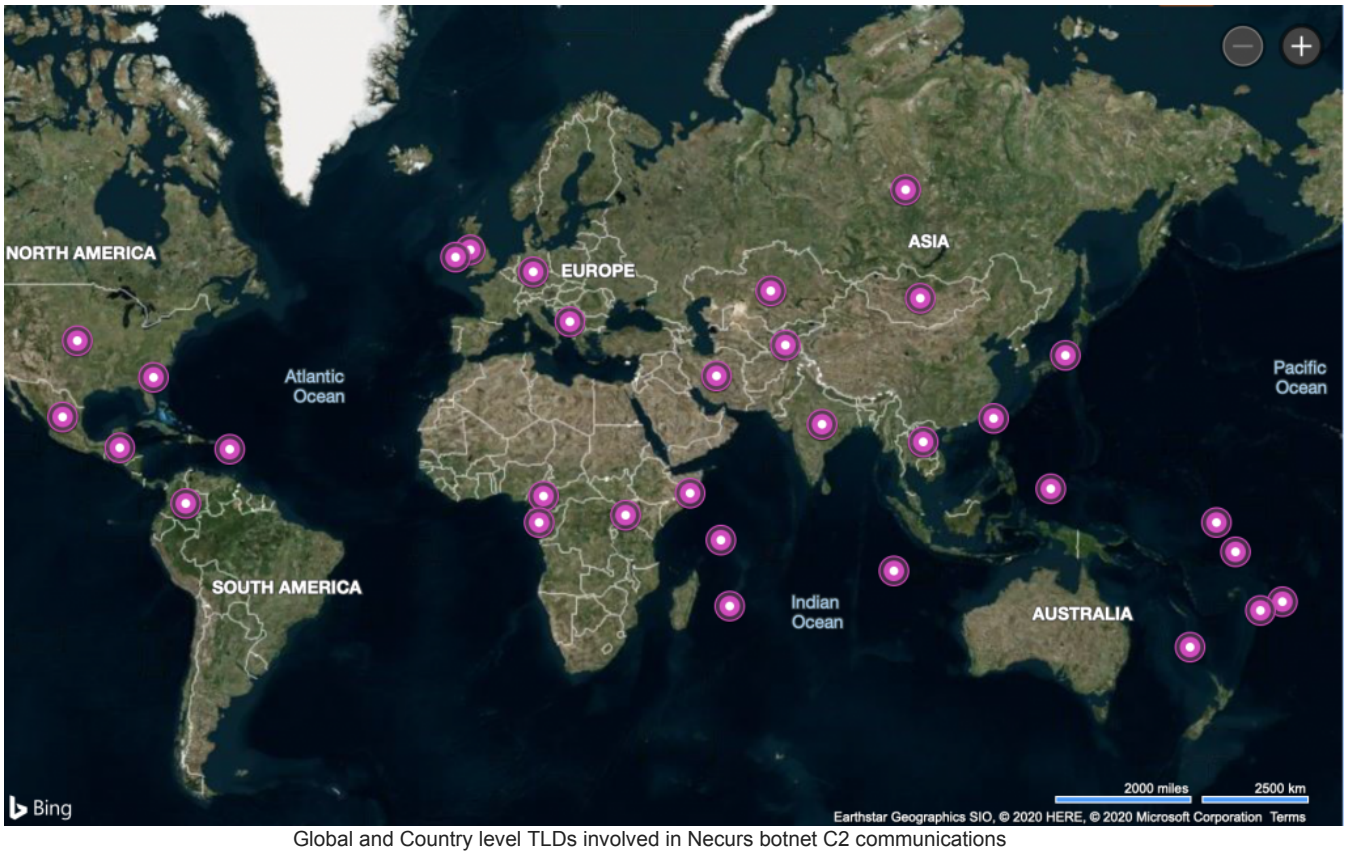
Other: .bit

The number of C2 domains per TLD over the calculated period were:

TLD	Domains
ac	**186,399**
bit	**85,887**
biz	**86,136**
bz	**164,375**
cc	**185,819**
cm	**186,274**
co	**165,067**
com	**85,993**
cx	**185,314**
de	**164,369**

eu	**164,837**
ga	**85,512**
im	**186,611**
in	**185,952**
ir	**85,767**
jp	**186,266**
ki	**185,968**
kz	**86,148**
la	**185,341**
me	**164,255**
mn	**185,988**
ms	**186,076**
mu	**186,152**
mx	**85,579**
net	**85,446**
nf	**185,738**
nu	**185,807**
org	**86,240**
pro	**85,292**
pw	**85,979**
ru	**164,611**
sc	**185,811**
sh	**186,049**
so	**186,200**
su	**85,734**
sx	**85,681**
tj	**186,089**
to	**85,665**
tv	**163,823**
tw	**186,388**
ug	**85,766**
us	**85,576**
xxx	**86,020**

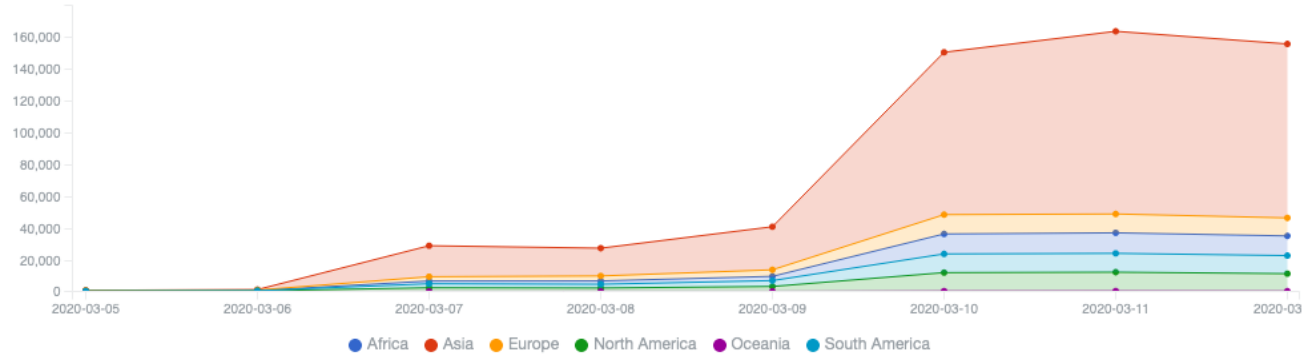
This map showing the distribution of global and country TLDs helps to demonstrate the size and breadth of the effort that was required to gain legal and voluntary action for coverage in all the TLDs used by for Necurs DGA C2 domains:



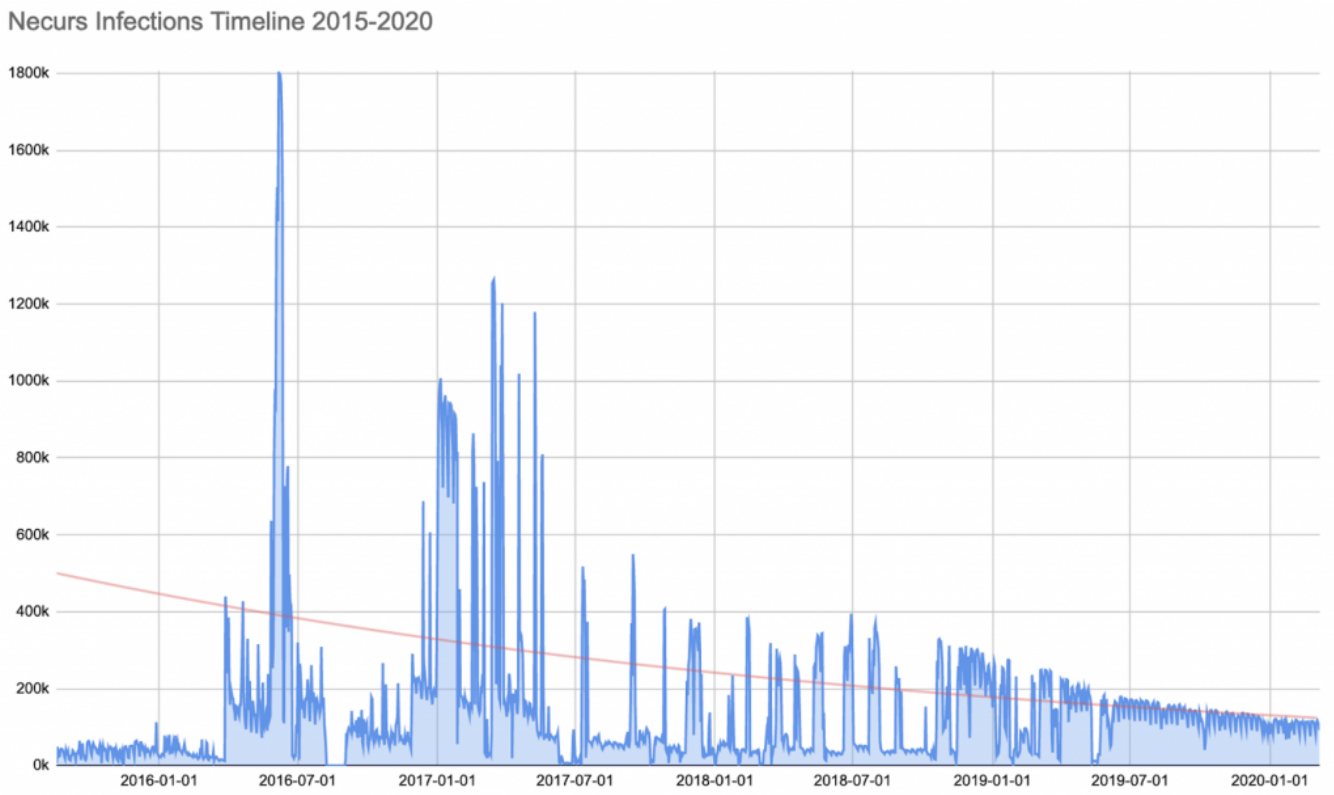
Global and Country level TLDs involved in Necurs botnet C2 communications

Sinkhole Data Analysis

Although Necurs may have been eclipsed by **Emotet** as the main dropper of current top threats such as **Trickbot** and **Dridex,** now that we have reported out the initial few days of sinkhole data, we can see that around **155,000 Necurs infected unique IP addresses per day** are being observed by the sinkholes. In operations where we have accurate bot IDs, we typically see about a one-to-one ratio of bots to IP addresses when taking into account DHCP lease churn and multiple bots behind a single NAT gateway. That number aligns well with Bitsight's own published historical analysis, which shows a gradual decline in the number of detected unique Necurs victim IP address per day since the peak botnet populations that were observed in 2016 and 2017.

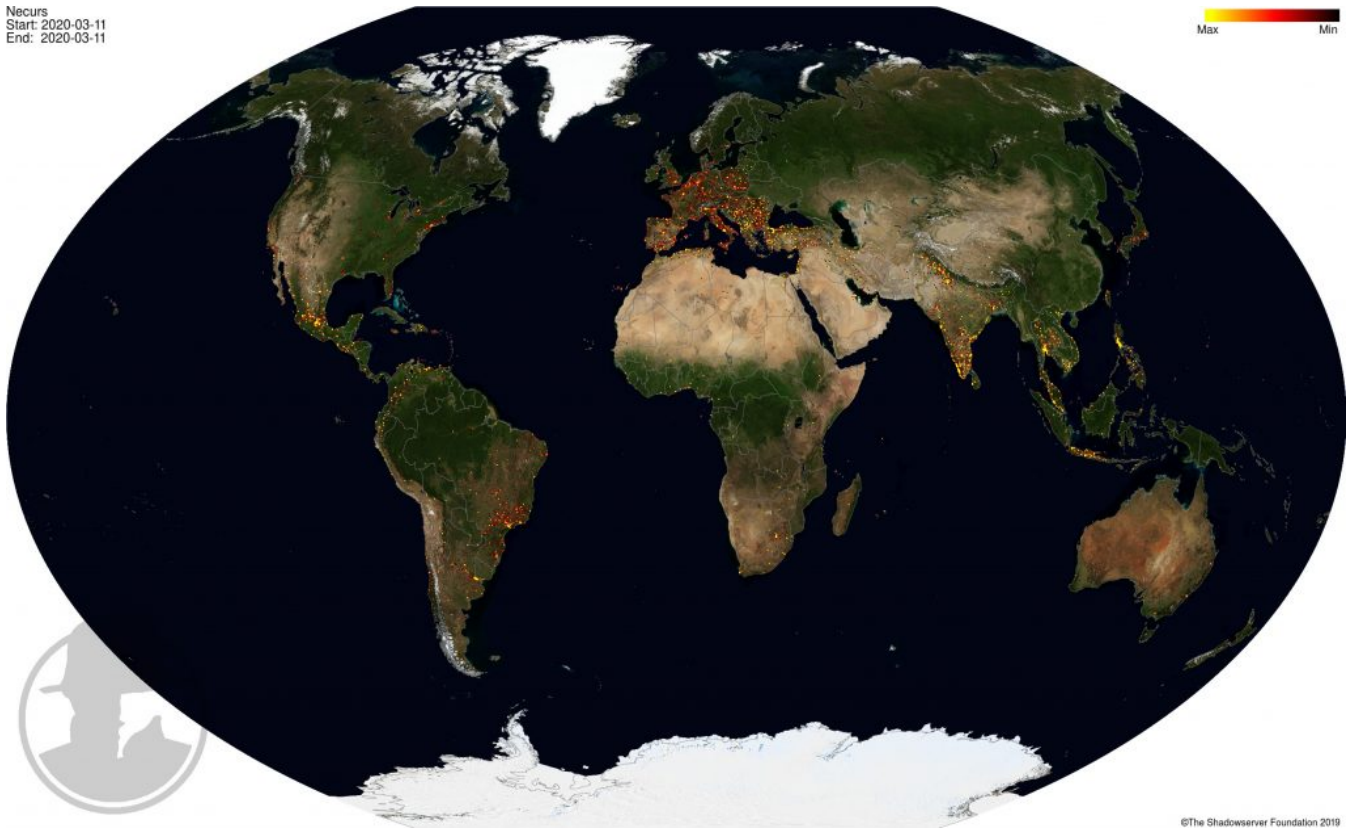


Microsoft Necurs sinkhole event feed provided via Shadowserver reporting

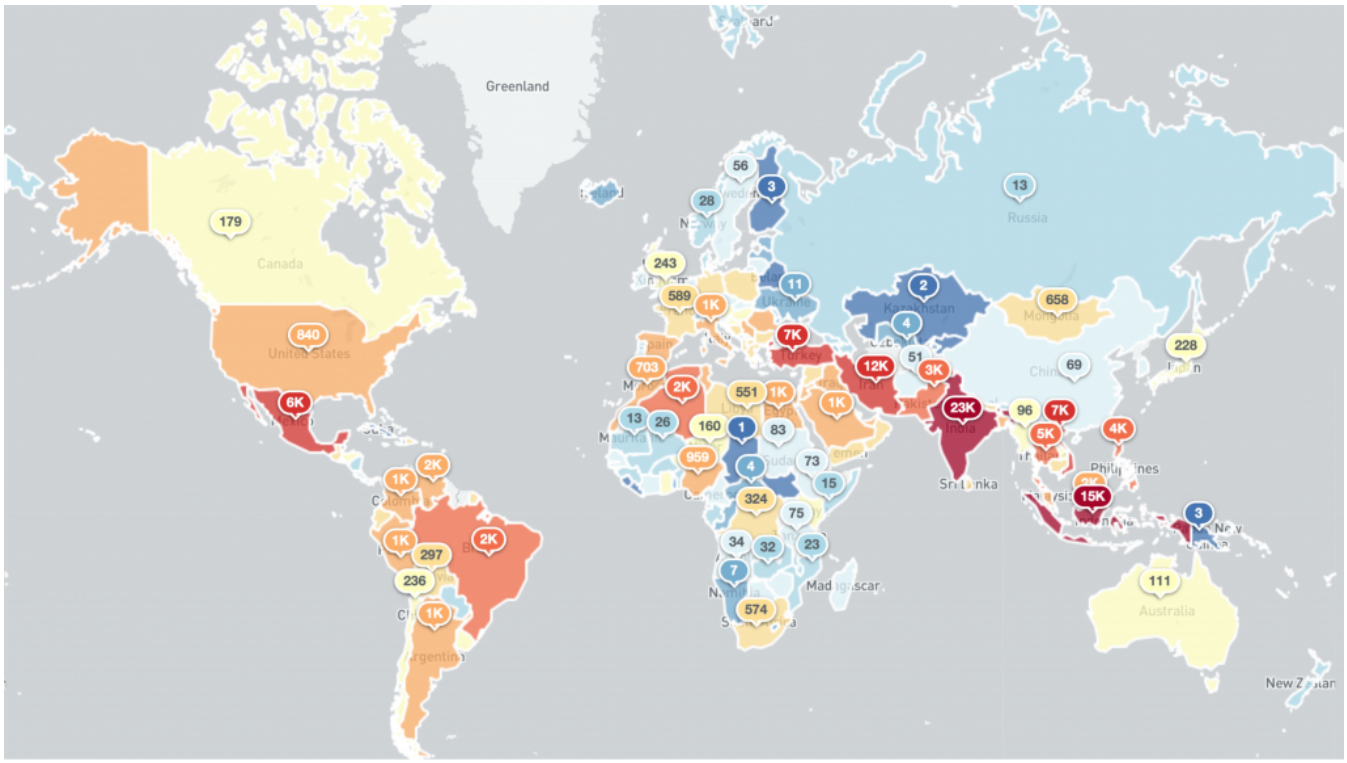


Bitsight historical Necurs sinkhole events

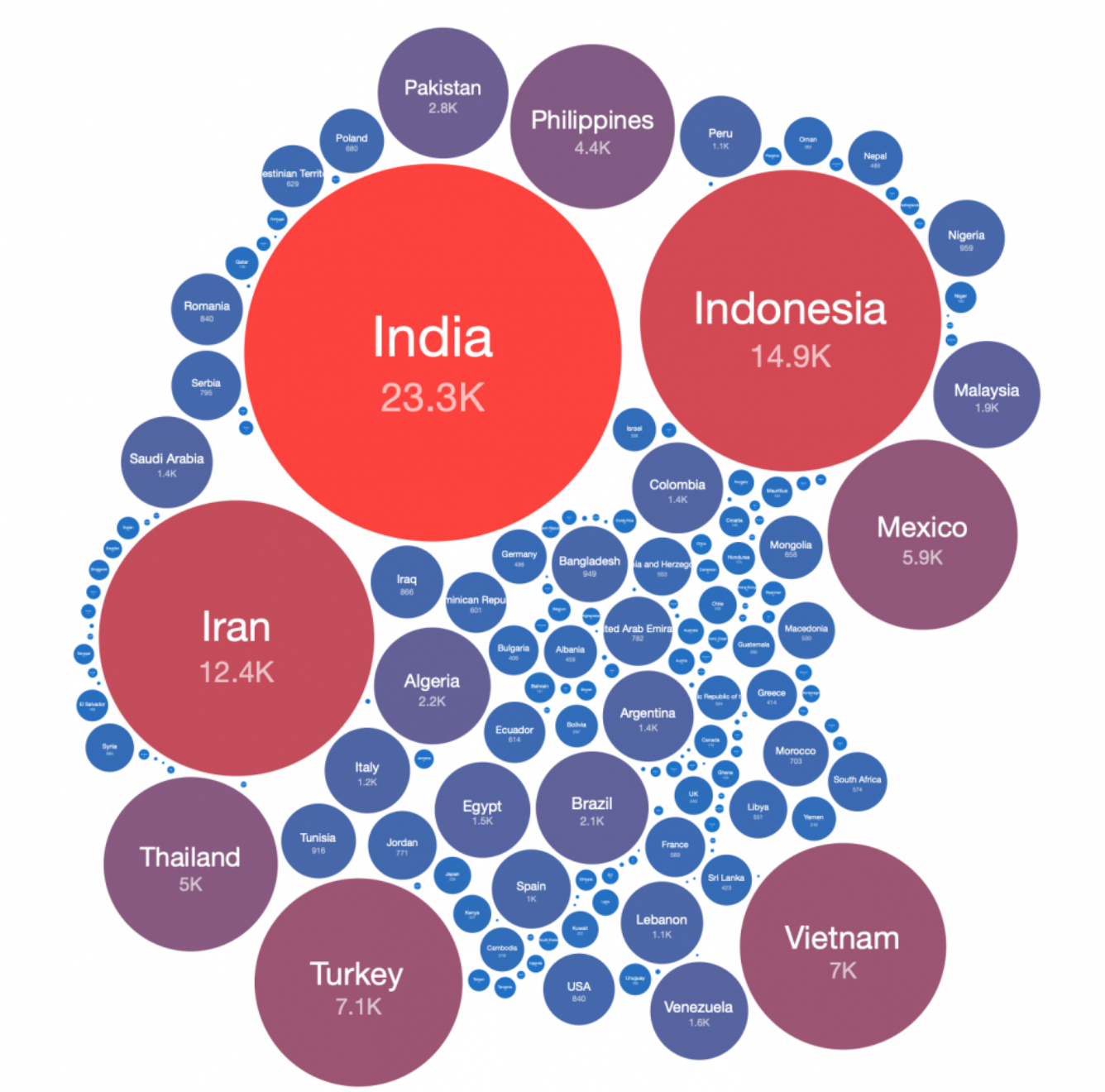
The global IP-geolocations of the current daily Necurs victim infections globally is shown below:



2020-03-11 IP-geolocated Necurs sinkhole events – locations



2020-03-11 IP-geolocated Necurs sinkhole events – victims per country



2020-03-11 IP-geolocated Necurs sinkhole events – top countries

Analysis

When blogging about specific botnet takedowns, we try to provide analysis that is unique to our own perspective on that operation. Ideally, we also present that analysis in the context of the wider and historical threat ecosystem, using Shadowserver's own unique and extensive datasets.

For Necurs, we thought that it would be interesting to compare the IP-geolocated country level victim distributions of victims during the peak 24 hours after sinkholing data collection began.

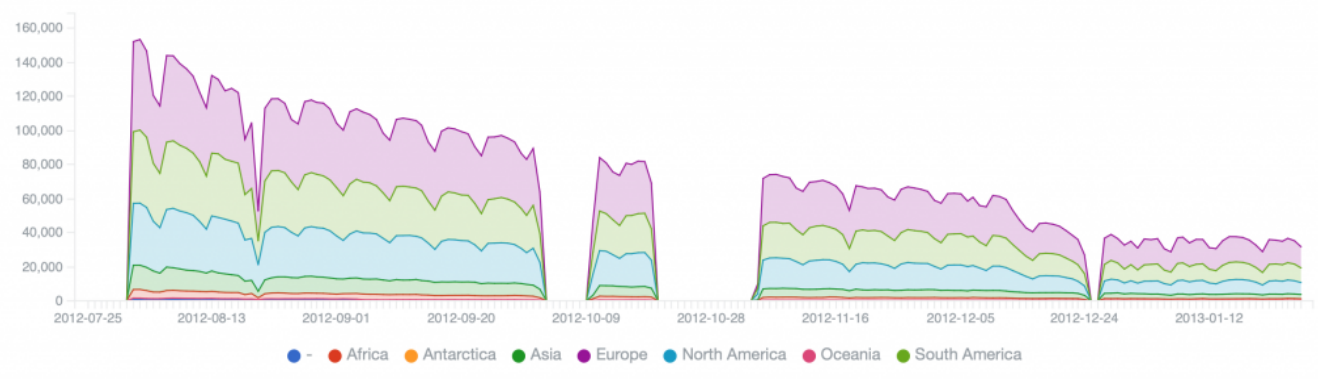
Selected spam botnet subjects are:

1. **Grum** (2012/2013)
2. **Pushdo/Cutwail** (2013/2014), multiple datasets

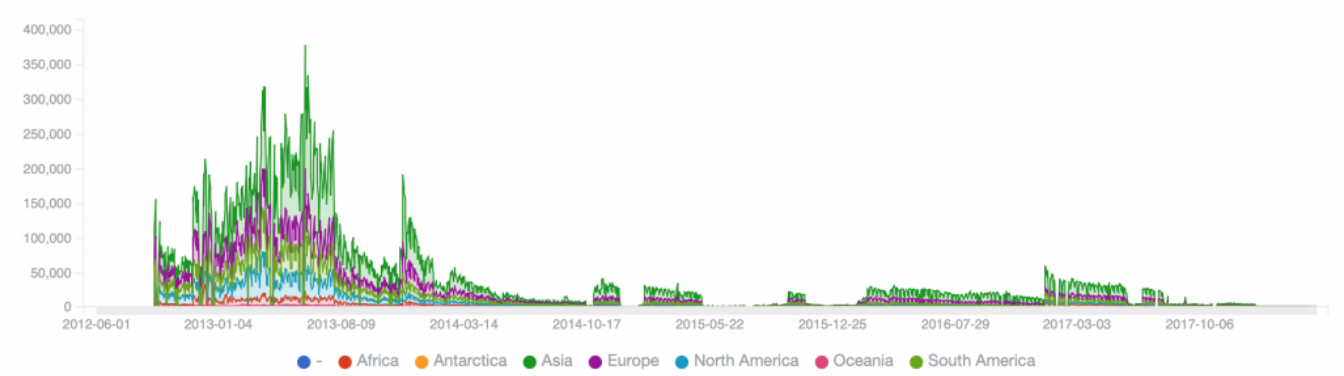
3. **Kelihos.C** spambot (2014/2015)
4. **Kelihos.E** spambot (2017-2018)
5. **Necurs** spambot (2020)
6. **Andromeda** malware dropper, for comparison (2017 to 2020)

We will start by comparing relative victim population sizes (number of unique IP addresses observed at each sinkhole per day), to provide the historical activity timelines and demonstrate each botnet's remediation decay curve (either due to reporting and victim remediation, or through background bot atrophy/die off).

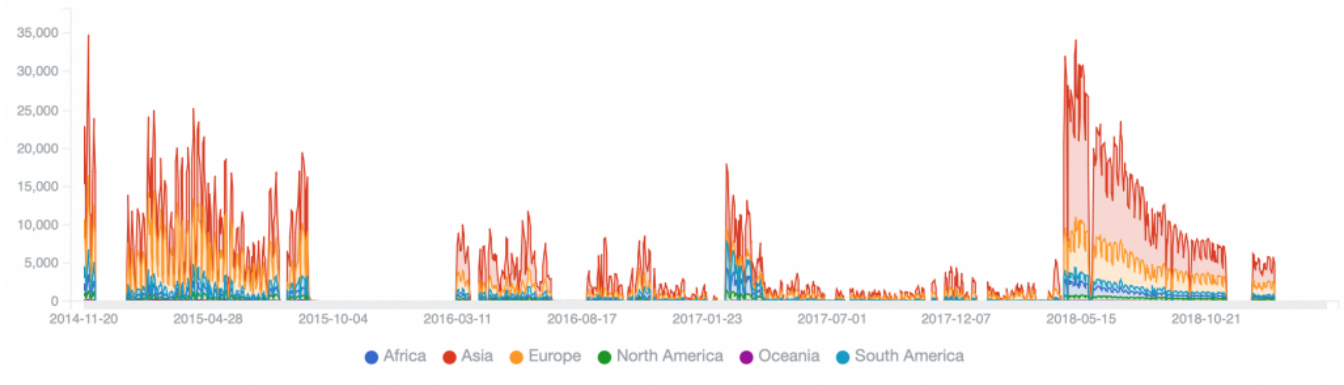
Grum (2012/2013) – peak of 153,186 on 2012-08-12, reduced to 73,910 by 2012-11-06, 50% remediation in about 3 months



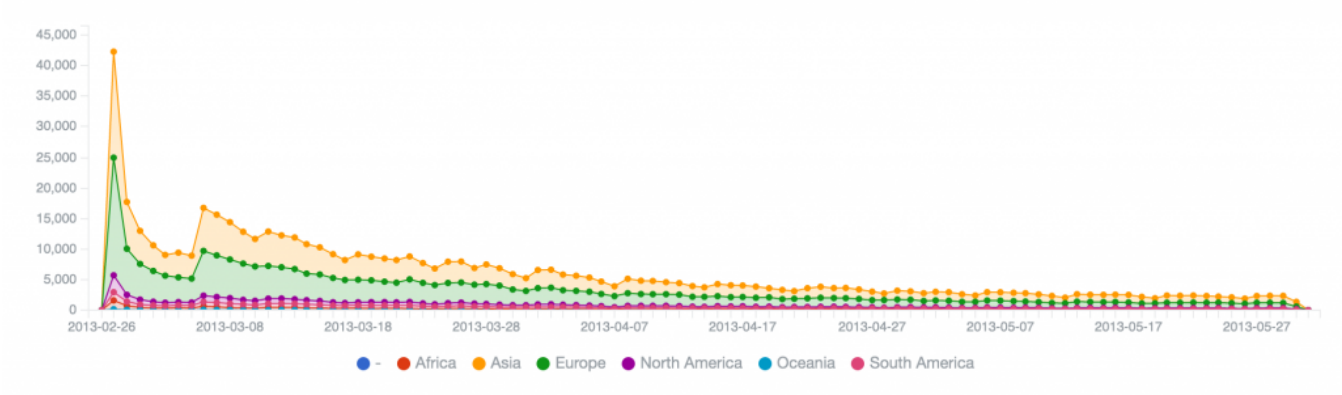
Pushdo (2013/2014) – peak of 375,898 on 2013-06-05, reduced to 180,242 on 2013-07-08, 50% remediation in about a month



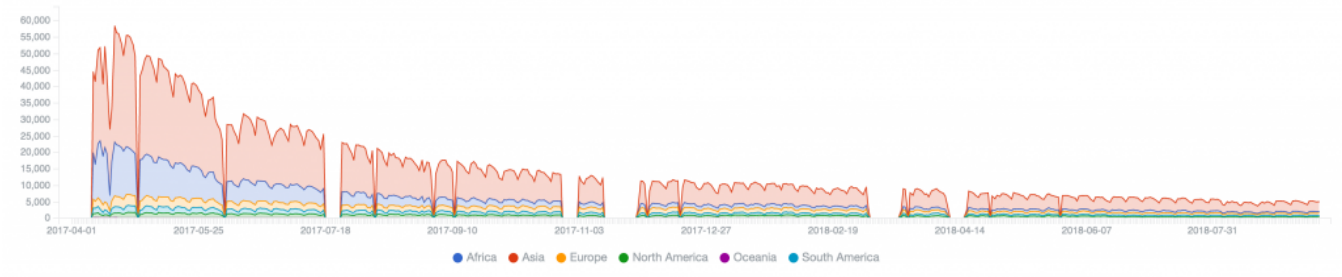
Cutwail (2014/2015) – peak of 36,662 on 2014-11-25, reduced to 16,591 on 2015-08-28, 50% remediation in about 9 months (but had repeated rebuilds/takedowns)



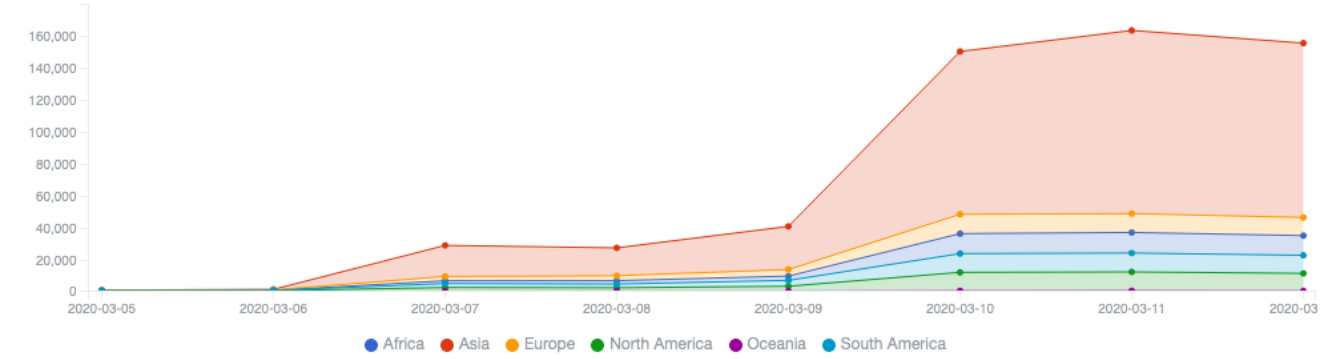
Kelihos.C (2013) – peak of 43, 124 on 2013-02-27, reduced to 17,622 by 2013-02-28, 50% remediation in first 24 hours



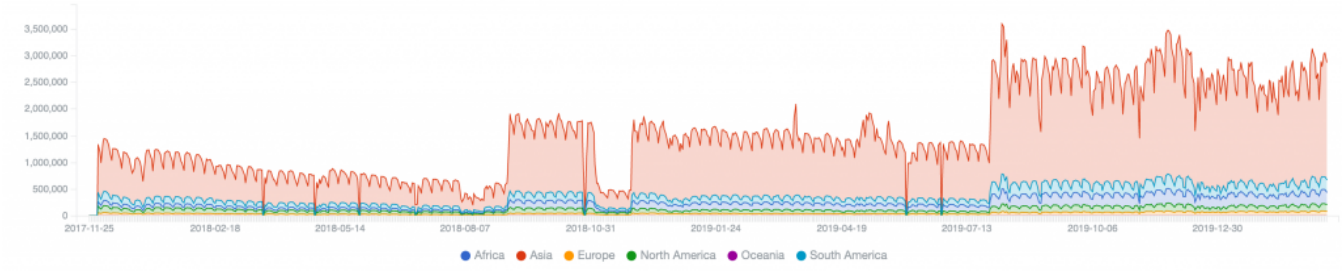
Kelihos.E (2017-2018) – peak of 58,318 on 2017-04-10, reduced to 27,836 on 2017-06-17, 50% remediation in about 2 months



Necurs (2020) – peak of 162,953 on 2020-03-11, just sinkholed, so initial days of remediation



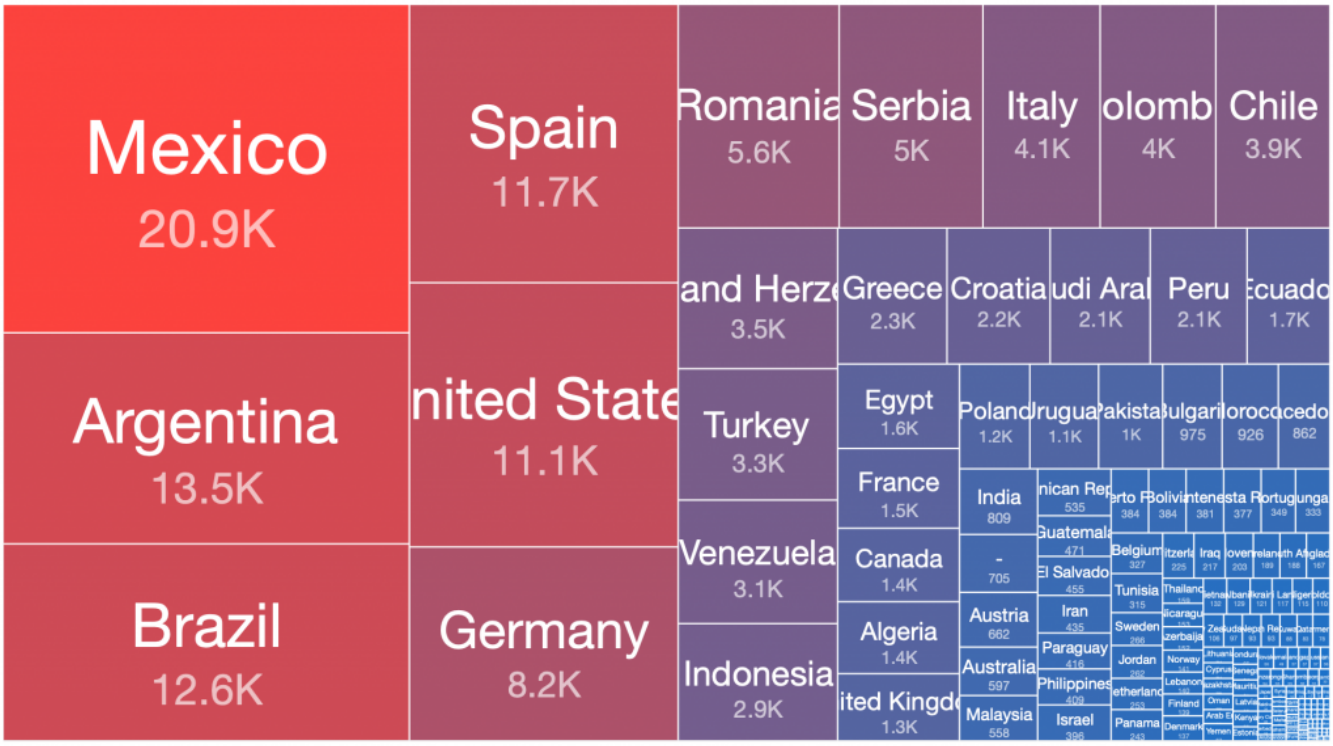
Andromeda (2017-2020) – peak of 1,443,705 on 2017-12-05, then 1,904,451 on 2018-09-12, then 3,584,470 on 2019-09-06, with long, slow cycles towards 50% remediation



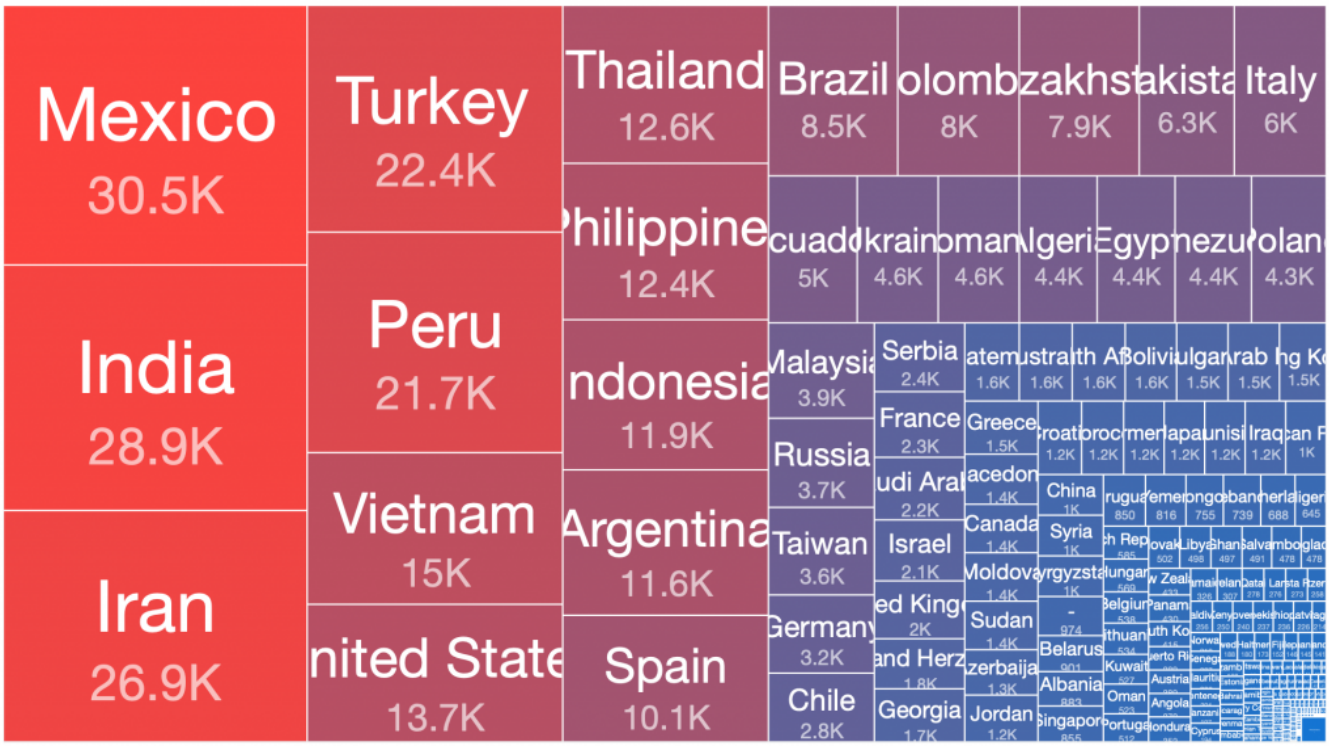
Each of these selected botnets was fairly prolific during their prime time. They have all been used to deliver much of the spam, phishing lures and malware that was received globally. Andromeda in particular continues to to resist large scale clean up.

We can use treemaps to easily visualize the relative ratios of sizes of botnet populations in different countries. Interestingly, when these treemaps are viewed side by side, there are some obvious observations that can be made about which countries the bulk of the infected victim systems of each of these botnets are located:

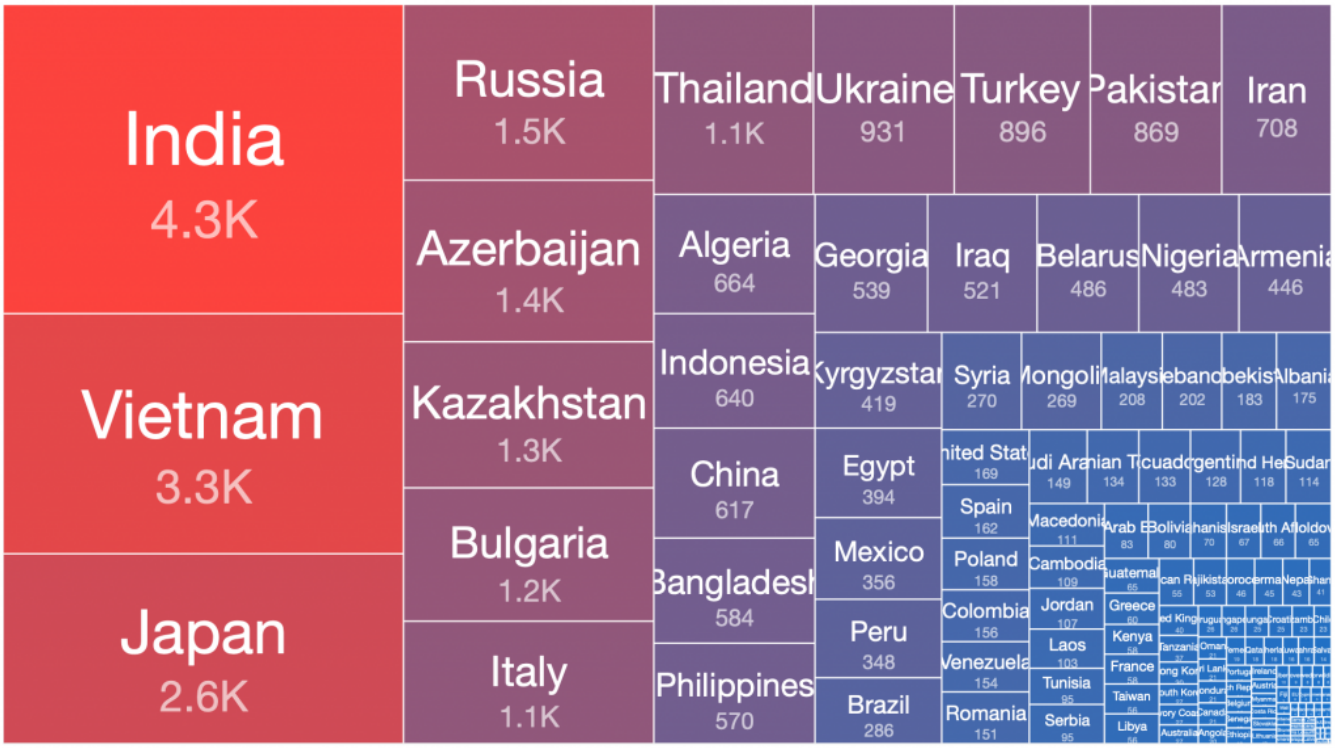
Grum – 2012-08-02



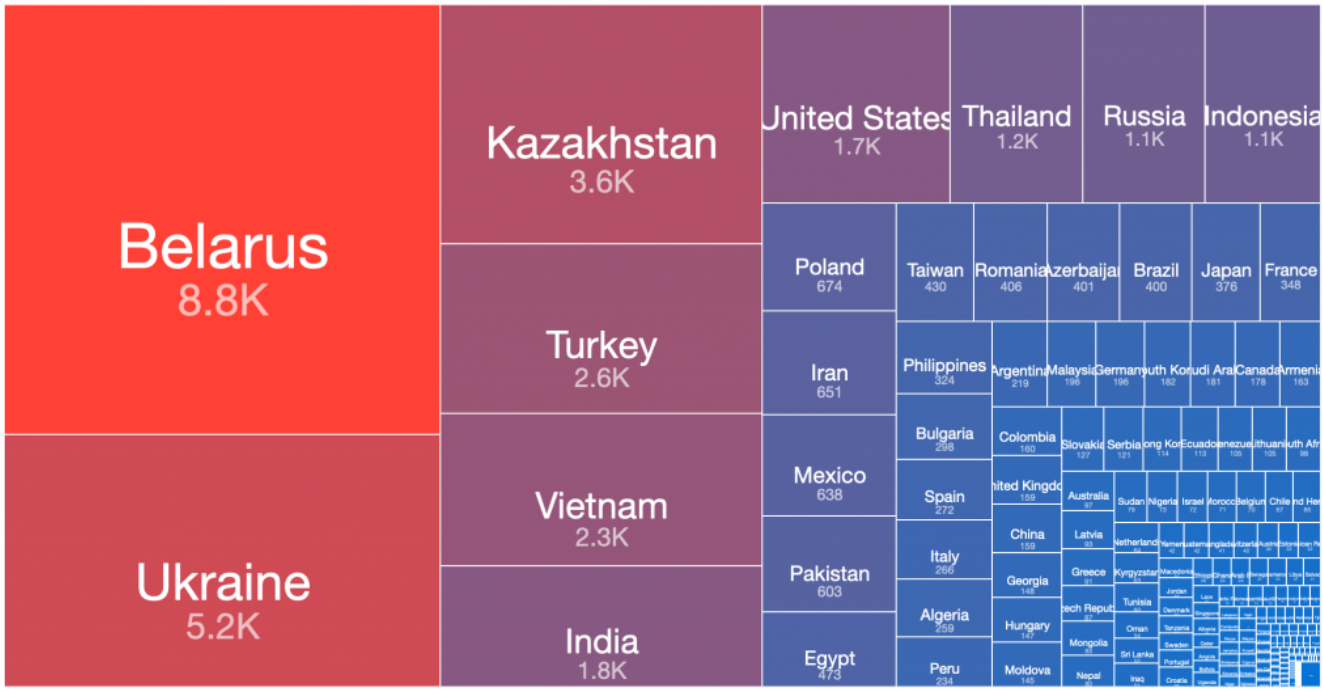
Pushdo – 2013-06-05



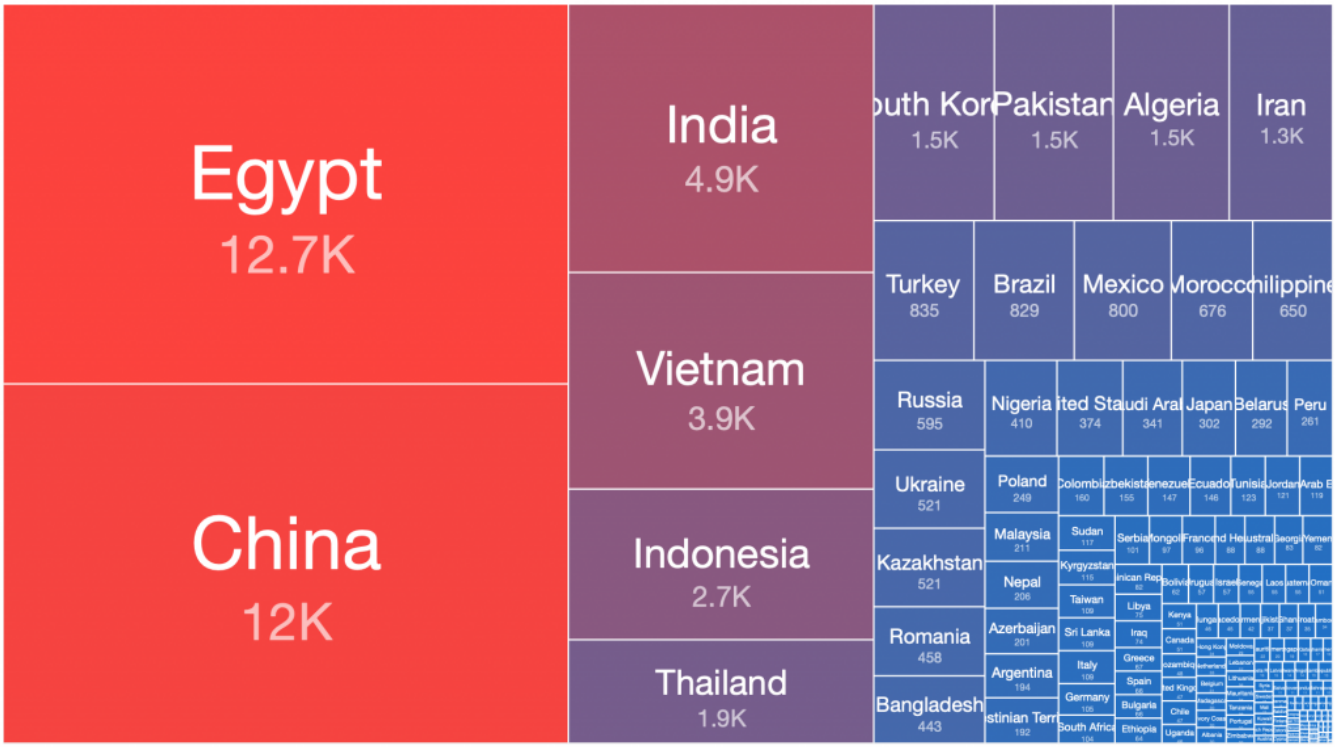
Cutwail – 2014-11-25



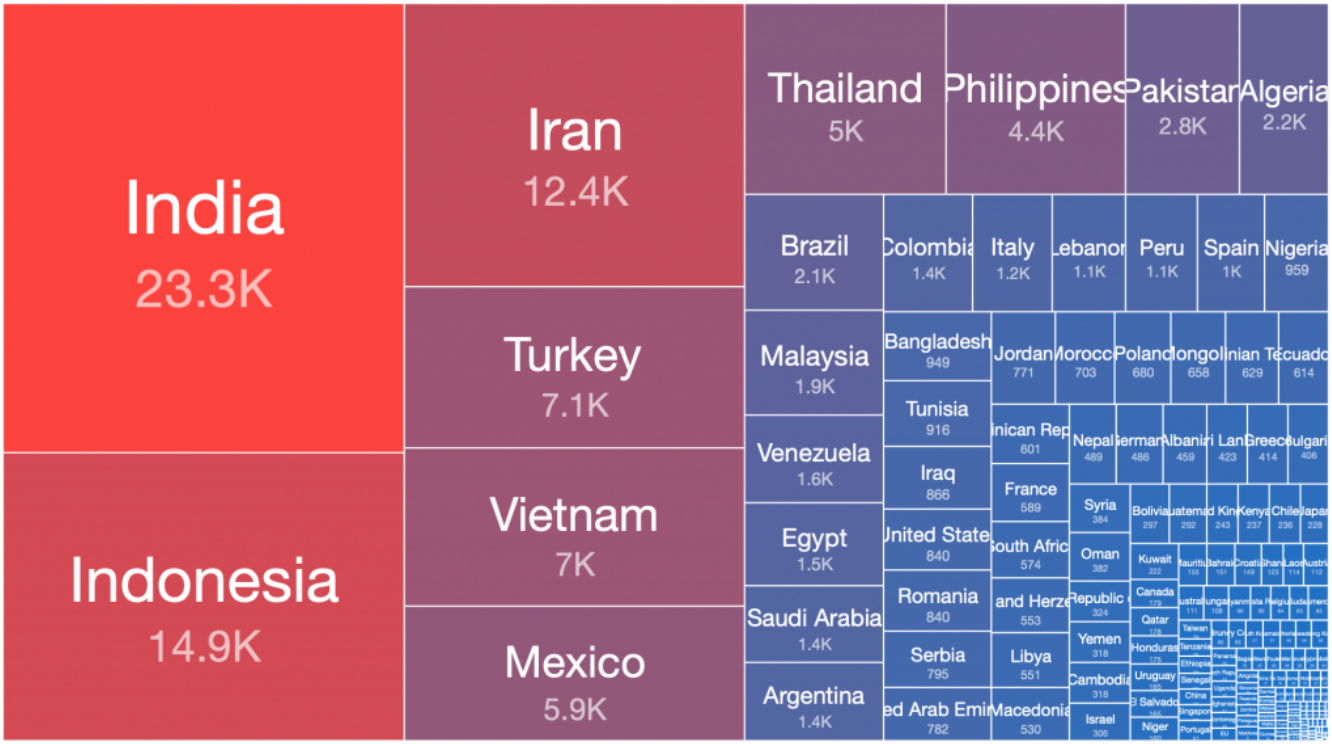
Kelihos.C – 2013-02-27



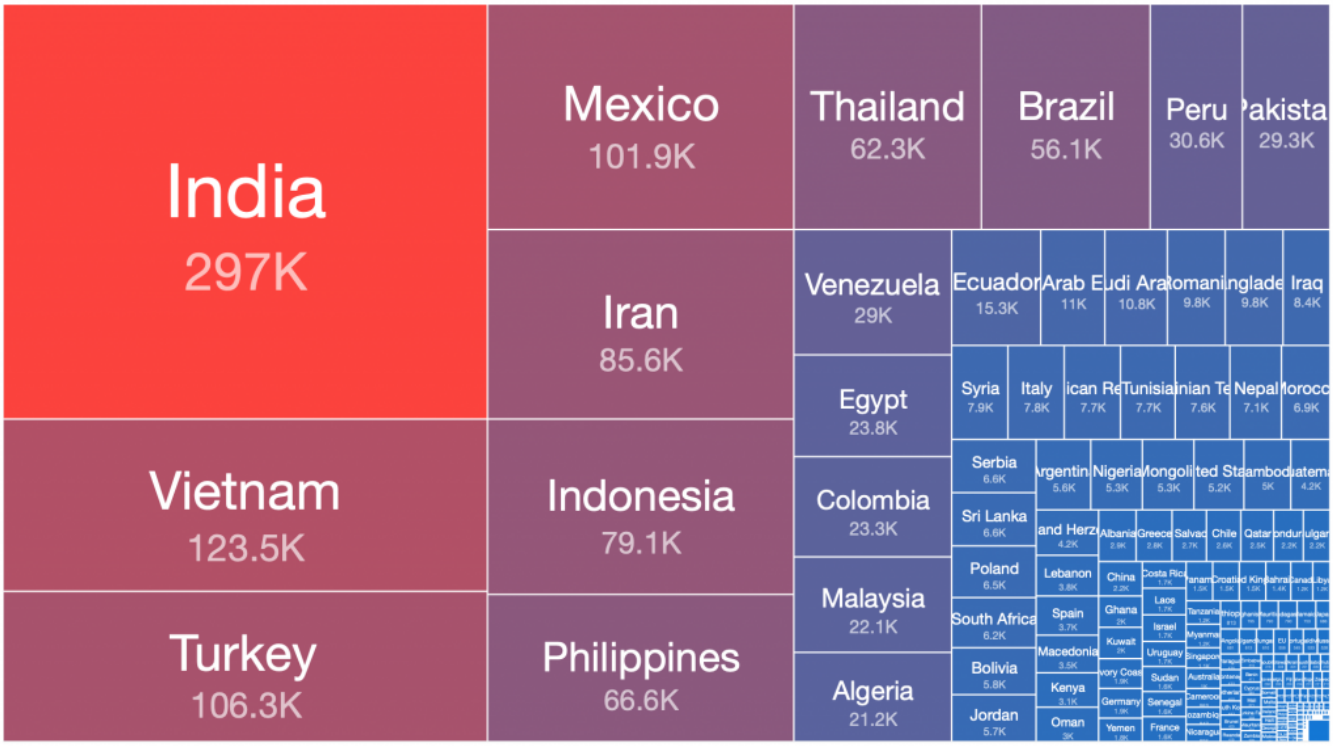
Kelihos.E – 2017-04-19



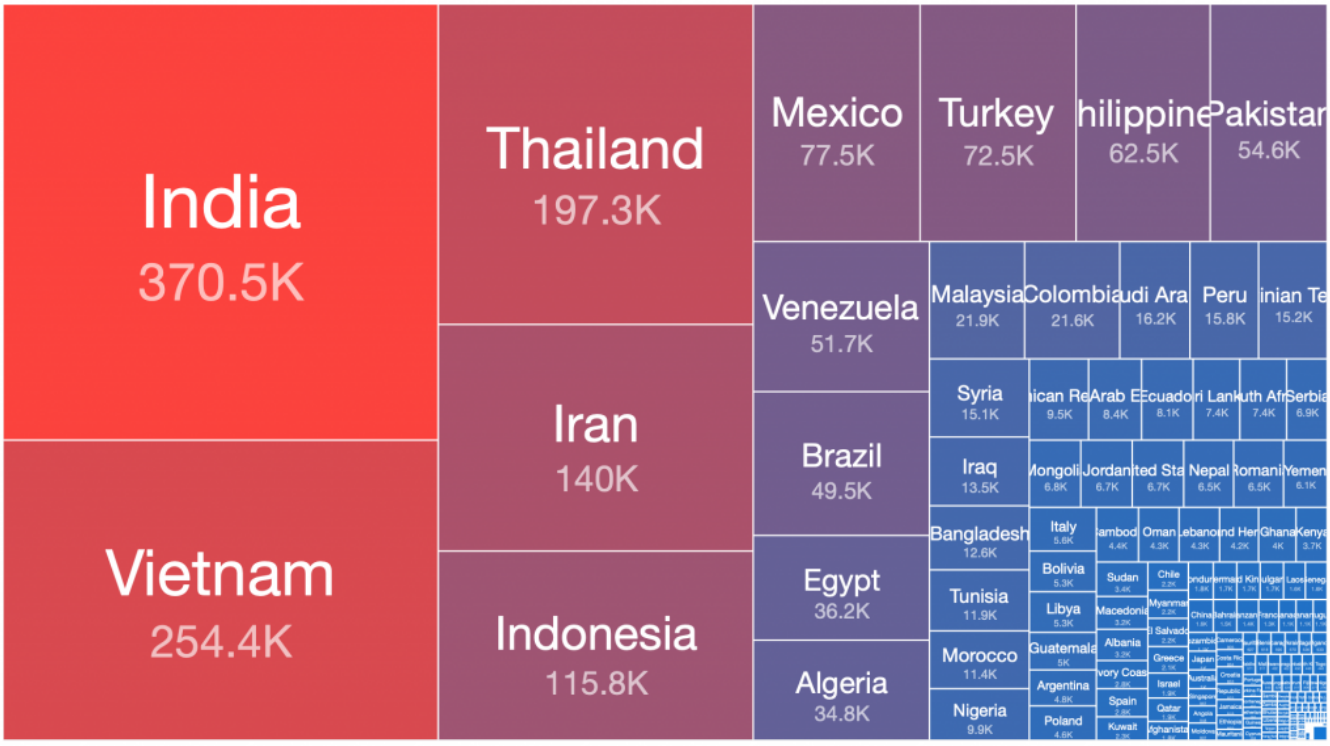
Necurs – 2020-03-11



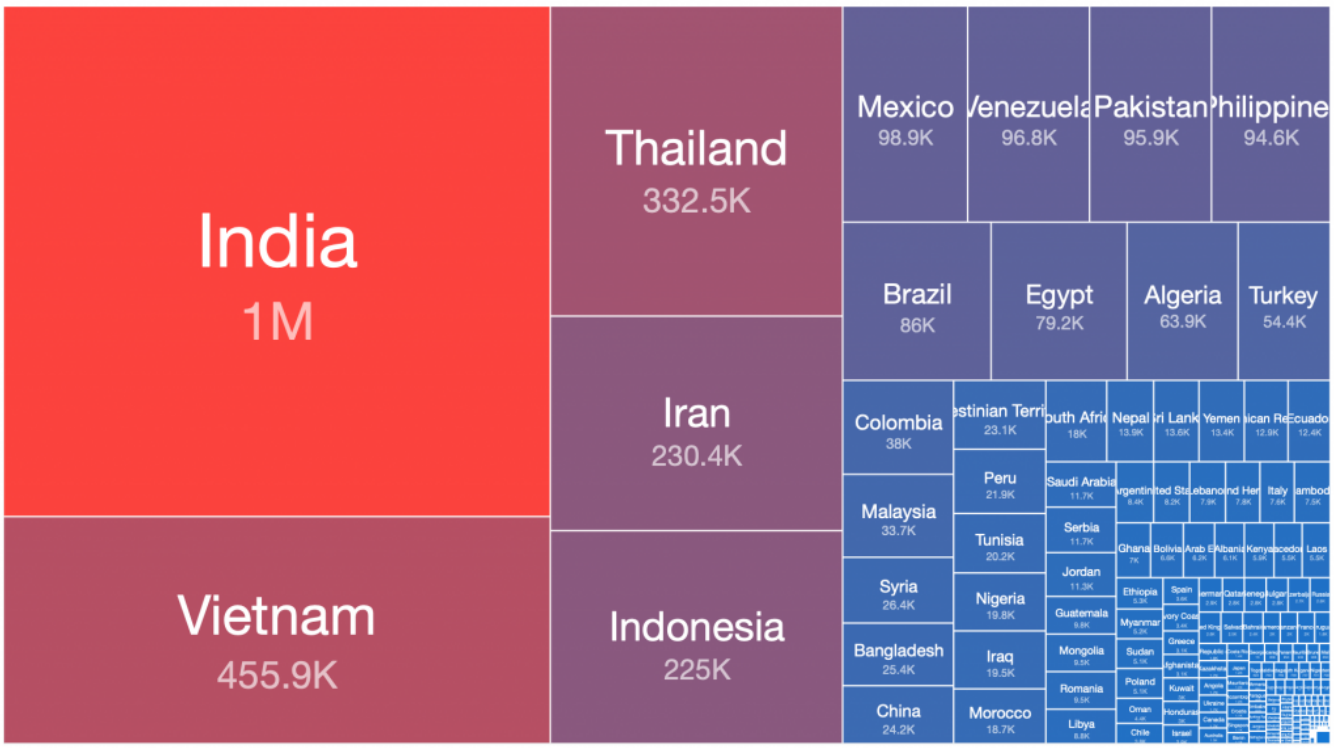
Andromeda – 2017-12-05



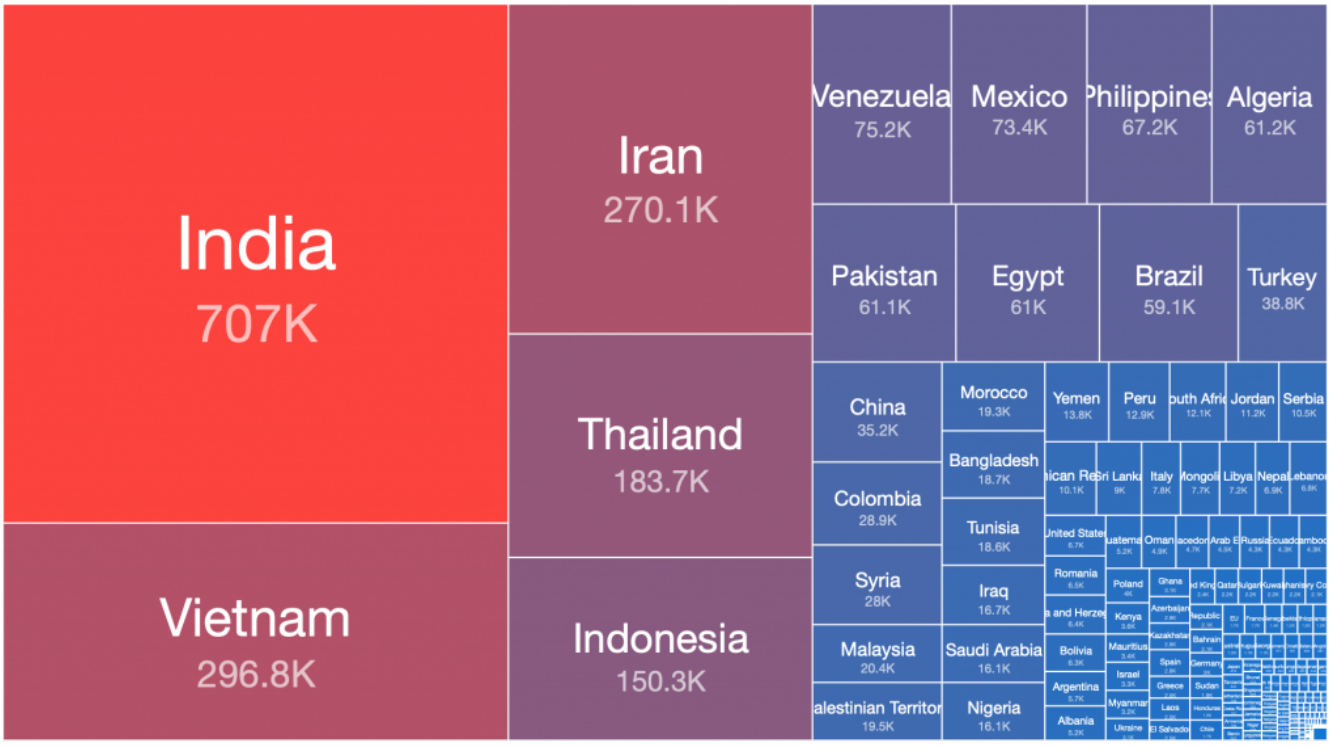
Andromeda – 2018-09-12



Andromeda – 2019-08-06



Andromeda – 2020-03-15



From our range of historical and current sinkhole datasets, if we take the peak 24 hours of each botnet's observed victim population, there are a number of countries where the largest victim distributions are typically found. This pattern has repeated in many of the spamming botnet networks built up and then disrupted or taken down over the past decade. Similar distributions occur in the still very large Andromeda malware dropper victim pools, which have experienced very slow remediation rates over the past three years, despite significant attention being drawn to this at industry conferences, in blog posts, through events in victim remediation feeds such as Shadowserver's free daily network reports, etc.

Below is a simple ordered count of which countries appear in the top 50% of victim populations for each of the above botnets:

Country	Grum 2012-08-02	Kelihos.C 2013-02-27	Pushdo 2013-06-05	Cutwail 2018-05-08	Kelihos.E 2017-04-19	Necurs 2020-03-14	Andromeda 2017-12-05	Andromeda 2018-09-12	Andromeda 2019-08-06	Times Features in Top 50% of Infections
India		1	1	1	1	1	1	1	1	8
Vietnam		1	1	1	1	1	1	1	1	8
Indonesia	1			1	1	1	1	1	1	7
Iran			1			1	1	1	1	5
Turkey	1		1	1		1	1			5
Mexico	1		1			1	1			4
Thailand			1	1				1	1	4
Spain	1		1	1						3
Argentina	1		1							2
Philipines			1				1			2
Ukraine		1		1						2
United States	1		1							2
Allied Arab Emirates				1						1
Belarus		1								1
Bosnia & Herzegovina	1									1
Brazil	1									1
Chile				1						1
China					1					1
Egypt					1					1
Germany	1									1
Italy				1						1
Kazakhstan		1								1
Peru			1							1
Romania	1									1
Russia				1						1
Saudi Arabia				1						1
South Korea				1						1
Turkey		1								1
Venezuela	1									1

The purpose of this comparison analysis is not to disparage any particular country, or to blame anyone for this situation (other than the cyber criminals who have been victimizing these populations for years). We have deliberately chosen to focus at a country level, rather than the individual ASN or IP level (although we do have that data available). The Shadowserver Foundation is a **public benefit** non-profit organization which gives data away for **free** each day to any vetted network owner and National CERT/CSIRT, and we have strived to help remediate these victim populations for many years now. We merely want to highlight the observed trends across a decade of spam and malware dropping botnets, to better assist defenders in protecting **all** networks, in every country.

From a global Internet security hygiene perspective, you might ask the question "**After the next big takedown or disruption of the next big spamming botnet (perhaps Emotet?) – where would the victim population likely be located?**" Every botnet is obviously different, as are the owner's goals and the circumstances on the Internet at that time. But 15 years of historic sinkhole data would suggest that it would likely be many of the same areas again.

These repeated botnet population patterns could be due to limited infosec budgets in certain countries, ignorance of the available (free) remediation data sources (such as Shadowserver), a lack of public awareness and good security practice guidance, larger populations of older, more vulnerable operating systems and computer hardware, perhaps a higher chance of software licensing compliance problems, or it could just be simple economic realities. Given that spamming botnets and malware droppers have proven to be highly effective, are often long lived, and are one of the primary attack vectors against the entire online world, it seems likely that countries with fewer infections will continue to be bombarded with spam and malware from similar locations in the future.

This is a obviously a complex topic, requiring more than a single blog post to do the subject justice. At a time when the physical world is dealing with the current COVID-19 pandemic and isolation is being considered, at both national and personal level, it is obviously difficult for many people to worry too much about malware and Internet-borne viruses. That is understandable, and protecting human lives needs to come first. However, we should all also think about some of the difficult challenges in maintaining good global internet hygiene, and how best the various members of the National CERT/CSIRT, network owner, Law Enforcement Agency, private sector business and ordinary members of the public can work together to help minimize the risk of another major spambot outbreak soon.

Conclusion

It has been good to work again with Microsoft and Bitsight on another major cybercrime disruption operation. We appreciate being offered the opportunity to support the final phase of their Necurs disruption effort, and to assist in what will hopefully be a rapid, effective, global remediation effort.

Thanks to the way Microsoft have managed this investigation and the civil court orders that they obtained, along with the use of RoLR for non-US TLDs, hundreds of thousands of unique daily victim IP addresses observed by the Necurs sinkholes will not only be made available to Microsoft and Bitsight's customers, but will also be available through Shadowserver's free daily network reports (in the Shadowserver drone feed, tagged as **type=necurs**). Some ISPs will also be blocking outbound connections to the known C2 infrastructure to further protect their end users.

This is a truly laudable effort from two private sector companies collectively trying to clean up this persistent, highly effective and impactful botnet. Regardless of whether the Necurs botnet will eventually be rebuilt, notifying – and hopefully remediating – so many victims of cybercrime is always a positive result for the good guys, and hopefully a bad day for the criminals.

If you receive an infection notification from your ISP, network owner or National CERT/CSIRT, please use anti-virus software to disinfect your computer and reduce the risk to yourself and others who might be impacted as a consequence of further malware attacks launched from your infected system. At this time in particular, we should all be aware that not only do we need to look after our own health, but we also have to think about our social responsibility towards others.

- Botnets
- Bots
- Malware
- Takedowns

« Back to News & Insights