# Joint Effort with Microsoft to Disrupt Massive Criminal Botnet Necurs

Written by Valter Santos March 10, 2020 Share Facebook Twitter LinkedIn

Since 2017 Bitsight has been working together with Microsoft's Digital Crimes Unit (DCU) to understand the inner workings of the Necurs malware, its botnets and command and control infrastructure in order to take disruptive action against the threat, including reverse engineering, malware analysis, modules updates, infection telemetry and command and control updates and forensic analysis. This week, an action took place to disrupt all Necurs botnets, followed by mitigation and eradication actions.

## The Malware

Necurs was first detected in 2012. It's used in a variety of illegal activities, but it is primarily known as a dropper for other malware, including GameOver Zeus, Dridex, Locky, Trickbot and others. Its main uses have been as a spambot, a delivery mechanism for ransomware, financial malware and for running pump and dump stock scams. From 2016 to 2019, it was the most prominent method to deliver spam and malware by criminals and was responsible for 90% of the malware spread by email worldwide.

The malware infects a victim's system by being dropped by other malware, through either spammed email attachments or malicious advertisements. Once on a system, Necurs utilizes its kernel mode rootkit capabilities to disable a large number of security applications, including Windows Firewall, both to protect itself and other malware on the infected system. Necurs is modular, in that it allows the operators to change how they operate it over time.

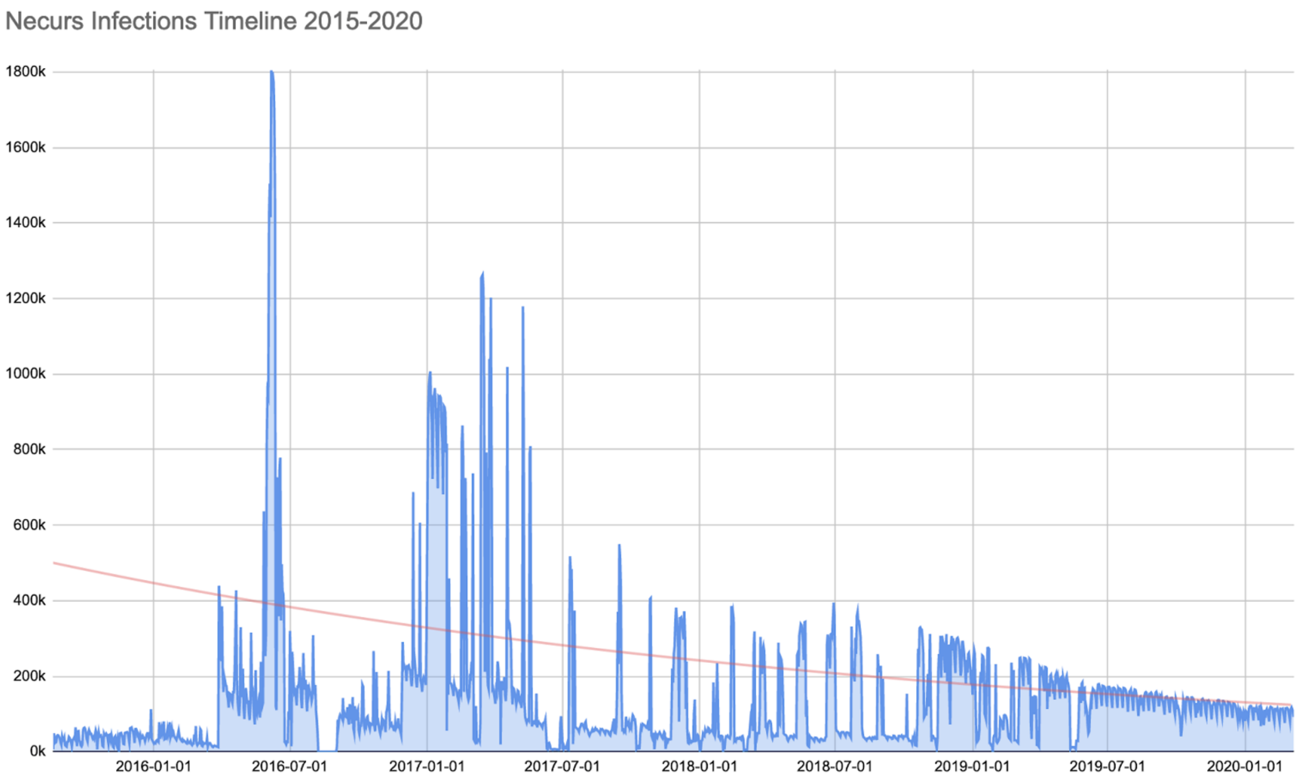
Its botnets appear to be closely controlled by a single group. During our investigation we have identified eleven Necurs botnets; of these, four are the most active and constitute approximately 95% of all infections. Since March 2019, the Necurs botnets' activity stalled but left an estimated 2 million infected systems in a dormant state waiting for the botnets to revive. It's not unusual for Necurs to stall operations from time to time, but it has never happened for such a long period of time until now.

## Infection Telemetry

Bitsight's unique ability to observe massive global infections is the reason why law enforcement and private sector organizations have worked with us over the years on significant disruption initiatives.

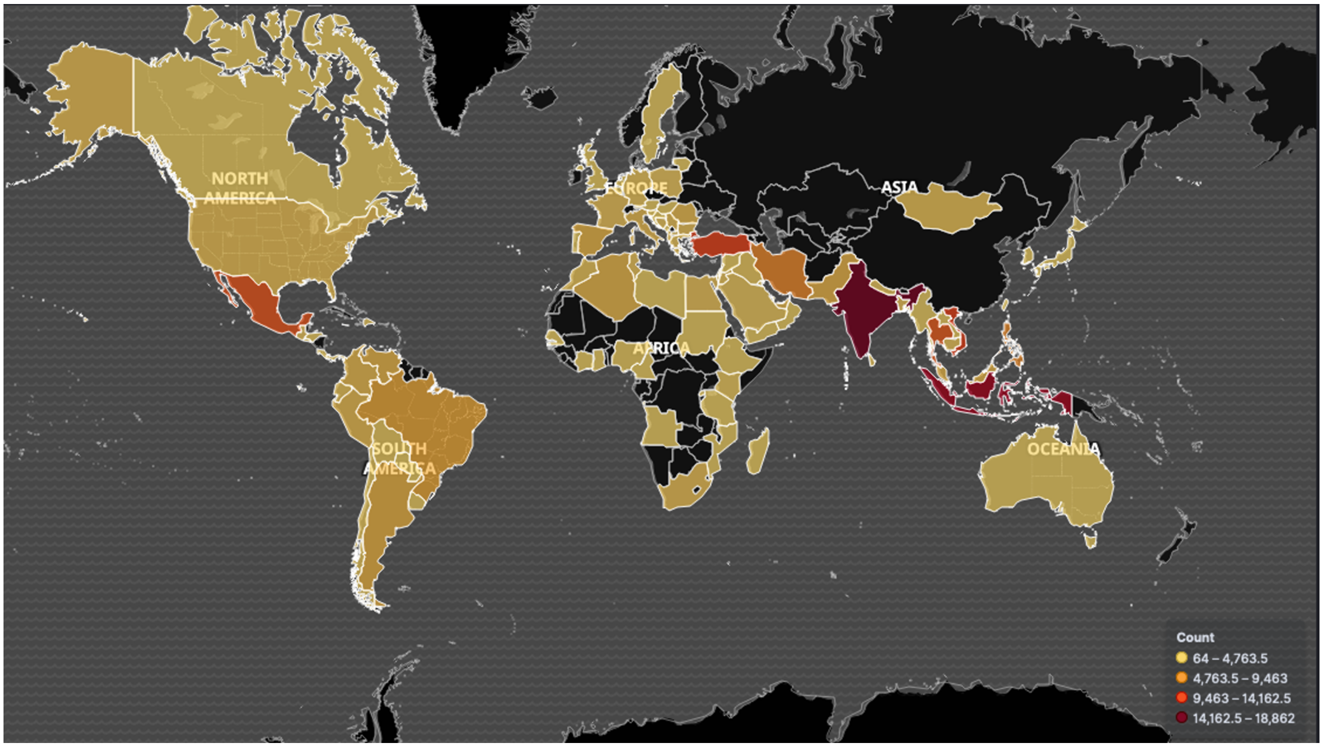
Back in 2016, we discovered that Necurs had around 1 million infected systems. Shortly after that post we had the opportunity to see a much bigger infection base of around 2 million infected systems in a 24 hour period. Measuring infections for Necurs is not as simple as for other malware; this is due to how the malware establishes communication with its command and control (C2, see below) and how our sinkholes collect this information. The communication from the infected machines would not reach out to us always, so only in rare occasions we have full visibility of all the botnets. On normal days of Necurs operation, our daily infection counters are below 50k infected systems when there are active C2s, and between 100k-300k when not. Even when under circumstances where we do receive a higher number of connections from infected systems, the daily unique observations continue to be an underestimate of the true size of the botnet, but it stills enables the ability to approximate those changes over time. After March 2019, when active C2s were last seen, we observed a slight decrease in infections overtime.

The following chart shows the evolution over the last years of how many infected systems reached out to our sinkholes:



*Necurs infections observed in the last years in Bitsight sinkholes*

The following map shows how a week of Necurs infection telemetry is dispersed geographically:



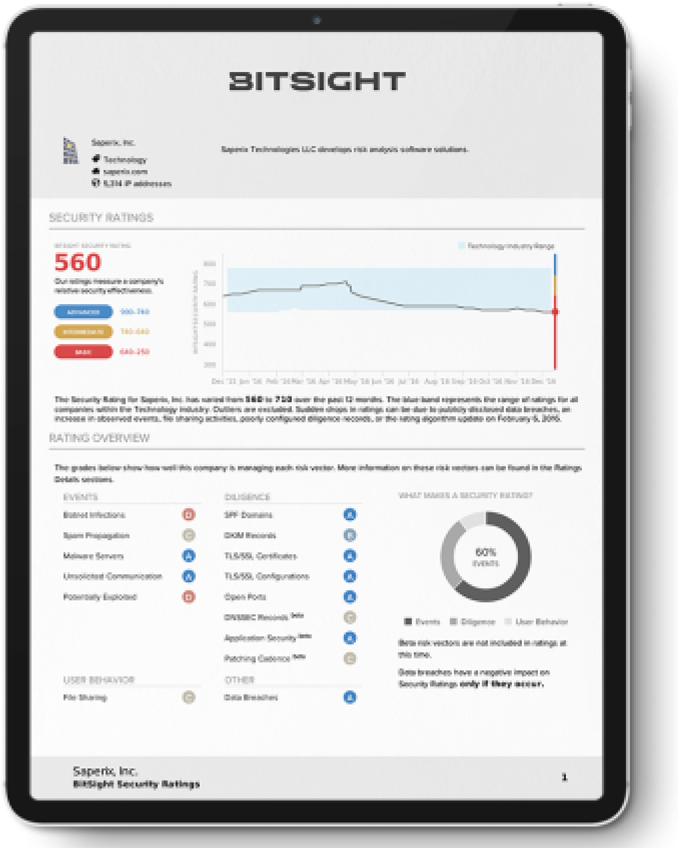
*Geographic distribution of Necurs infections*

The breakdown by countries for the first seven days of March 2020 is given by the following table where the infection counter is measured by distinct IP addresses reaching our sinkholes - as stated above the botnets are bigger and these numbers cover only a part of them:

| Country | Infections | % |
|---|---|---|
| India | 90563 | 13.59% |
| Indonesia | 69530 | 10.43% |
| Turkey | 51605 | 7.74% |
| Vietnam | 49190 | 7.38% |
| Mexico | 40129 | 6.02% |
| Thailand | 37081 | 5.56% |
| Iran | 32807 | 4.92% |
| Philippines | 24097 | 3.62% |
| Brazil | 16122 | 2.42% |
| Pakistan | 11311 | 1.70% |
| Argentina | 11289 | 1.69% |
| Spain | 10223 | 1.53% |
| Venezuela | 9825 | 1.47% |
| Algeria | 9806 | 1.47% |
| Malaysia | 8250 | 1.24% |

| | | |
|---|---|---|
| Colombia | 7832 | 1.18% |
| Italy | 7640 | 1.15% |
| Romania | | |

## Request your Security Rating Snapshot report to find out how secure your organization really is



BITSIGHT

Saperix, Inc.
Technology
saperix.com
5,314 IP addresses

Saperix Technologies LLC develops risk analysis software solutions.

SECURITY RATINGS

BITSIGHT SECURITY RATING

560

Our ratings measure a company's relative security effectiveness.

| | |
|---|---|
| ADVANCED | 900–740 |
| INTERMEDIATE | 740–640 |
| BASIC | 640–250 |

Technology Industry Range
BITSIGHT SECURITY RATING
800
700
600
500
400
300
Dec '15 Jan '16 Feb '16 Mar '16 Apr '16 May '16 Jun '16 Jul '16 Aug '16 Sep '16 Oct '16 Nov '16 Dec '16

The Security Rating for Saperix, Inc. has varied from **560** to **710** over the past 12 months. The blue band represents the range of ratings for all companies within the Technology industry. Outliers are excluded. Sudden drops in ratings can be due to publicly disclosed data breaches, an increase in observed events, file sharing activities, poorly configured diligence records, or the rating algorithm update on February 6, 2016.

RATING OVERVIEW

The grades below show how well this company is managing each risk vector. More information on these risk vectors can be found in the Ratings Details sections.

| EVENTS | | DILIGENCE | |
|---|---|---|---|
| Botnet Infections | D | SPF Domains | A |
| Spam Propagation | C | DKIM Records | B |
| Malware Servers | A | TLS/SSL Certificates | A |
| Unsolicited Communication | A | TLS/SSL Configurations | A |
| Potentially Exploited | D | Open Ports | A |
| | | DNSSEC Records beta | C |
| | | Application Security beta | A |
| | | Patching Cadence beta | C |
| USER BEHAVIOR | | OTHER | |
| File Sharing | C | Data Breaches | A |

WHAT MAKES A SECURITY RATING?

Beta risk vectors are not included in ratings at this time.

Data breaches have a negative impact on Security Ratings **only if they occur.**

Saperix, Inc.
**BitSight Security Ratings**
1

## Request your Security Rating Snapshot report to find out how secure your organization really is

Request your free Security Rating Snapshot to find the gaps in your security program and how you compare to others in your industry.

See Your Rating

| | | |
|---|---|---|
| Romania | 7191 | 1.08% |

| | | |
|---|---|---|
| UAE | 6916 | 1.04% |
| Peru | 6584 | 0.99% |
| US | 5757 | 0.86% |
| South Africa | 5519 | 0.86% |
| Serbia | 5293 | 0.79% |
| Bangladesh | 4963 | 0.74% |
| France | 4892 | 0.73% |
| Others | 132089 | 19.82% |

## Command and Control

For the Necurs infected systems to communicate with the botnet command and control (C2), the developers have implemented a layered approach using a mixture of a centralized and peer-to-peer (P2P) communication channels in order to prevent botnet disruption by law enforcement, network operators and researchers. Necurs communicates with its operators via the following:

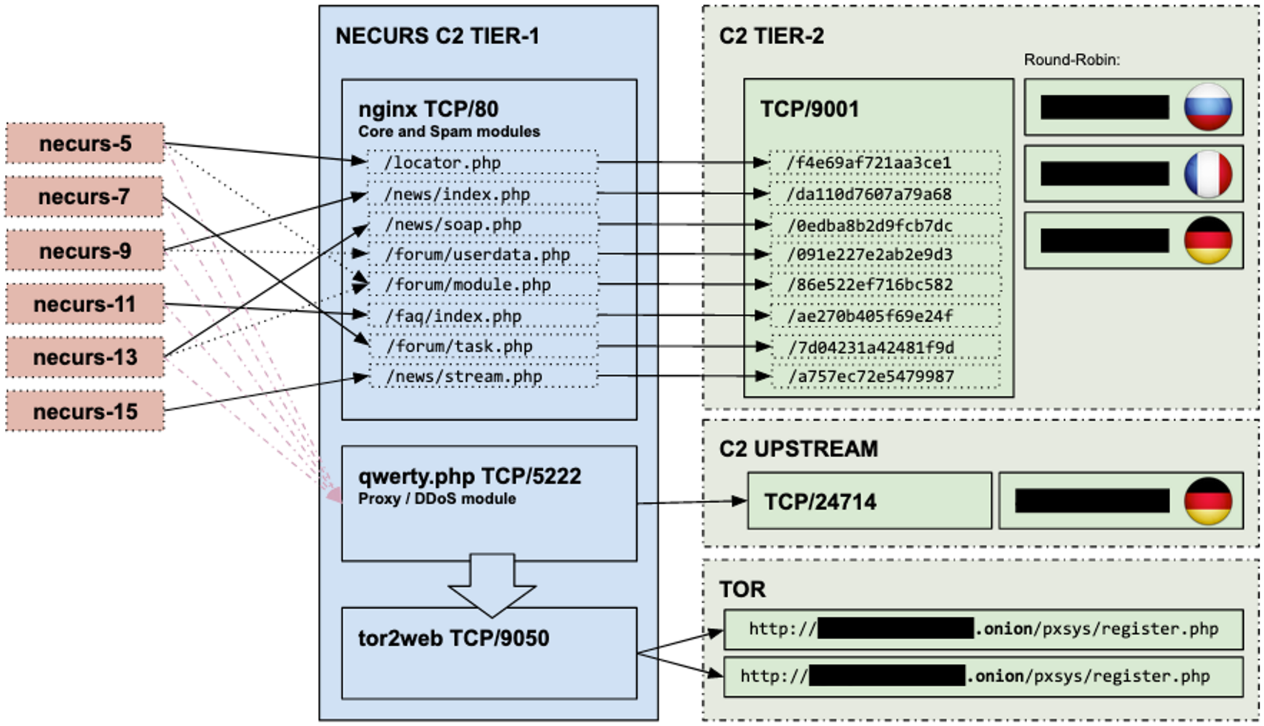
- As a primary communication mechanism, an embedded list of IPs and occasionally static domains are embedded in the malware sample itself.
- If they are not working, Necurs uses its domain generation algorithm (DGA):
    - A dummy DGA that produces domains to be used to see if the malware is running in a simulated environment.
    - A second DGA-like fetches .bit domains that are not generated algorithmically but hard-coded.
      The .bit TLD is an alternative DNS model, maintained by Namecoin, that uses a blockchain infrastructure and is harder to disrupt when compared with ICANN regulated TLDs.
    - The main DGA kicks in if none of the other methods were able to get an active C2. This DGA produces 2048 possible C2 domains every 4 days across 43 TLDs, including .bit. The DGA depends on the current date and a seed hardcoded in the binary. All domains are tried until one resolves and responds using the correct protocol.

- Even if all methods above fail, the C2 domain is retrieved from the P2P network that is always active and acts as the main channel to update C2s. An initial list of about 2000 peers is hardcoded in the binary but can be updated at any given time as needed. The peers in this list are known as supernodes: victim systems with elevated status within the infrastructure.

To make itself difficult to monitor there is another layer: the malware uses an algorithm that converts the IP addresses received through DNS to the real IP addresses of its servers. When connecting to that IP address, if it responds with the proper protocol the malware knows it’s communicating with an active C2.

The command and control complexity is completed with a tiered approach of the C2 infrastructure. When an infected system communicates with a C2, it is, in reality, communicating with multiple layers of C2 proxies; this is another way operators try to hide their core infrastructure and is common in more complex malware.

The first tier of C2 are cheap VPS in countries such as Russia, Ukraine, etc. that reverse proxy all communications to the C2 upstream in tier-2, that normally are hosted in Europe and sometimes Russia, until the communication reaches the backend. The following diagram shows the relationship between what is seen in the first and second tiers - other tiers are out of scope of this post:



*Necurs C2 flow between tier-1 and tier-2*

The diagram shows that the C2 have three main components that are aligned with the malware capabilities:

1. The main module is the core of Necurs. In the HTTP communication, the HTTP path could be used to differentiate each botnet. The tier-1 C2 reverse proxies all communication to a group of upstream C2 in tier-2 that are configured in nginx in a round-robin fashion.
2. The spam module is configured in the same way as the main module in a tier-1 C2, but uses different HTTP paths (dotted lines in the diagram above for paths /forum/userdata.php and /forum/module.php belong to the spam module).
3. The Proxy/DDoS module (see more here) also has its component in the C2 and a different upstream C2. It uses an upstream server and also two Tor hidden services to communicate with the bot operators.

These two C2 tiers are proxies to the backend C2 system, for network defenders only the first tier is really important and it’s enough to harden their networks against this threat.

## Conclusion

With this joint action we hope to further Bitsight’s mission of creating a safer Internet and digital ecosystem. We know in advance that Necurs was in idle mode for a while and was already been replaced by others (Emotet) but, nevertheless, there were still an estimated 2 million infected bots waiting for their master commands - and that could happen at any time if no action was taken.

A list of indicators of compromise is shared at the end of this post, composed by malware samples hashes, domains, C2 and supernodes IP addresses, all collected in a three-year period by Bitsight and our partners in regard to this operation. With this, we hope that researchers and network defenders can hunt and clean up Necurs infections in their networks in order to better eradicate it.

Happy hunting. Over and out.

## Read the Microsoft announcement here

### References

- https://www.bitsight.com/blog/monitoring-necurs-the-tip-of-the-iceberg
- https://www.bitsight.com/blog/necurs-proxy-module-with-ddos-features
- https://www.johannesbader.ch/2015/02/the-dgas-of-necurs/
- https://www.cert.pl/en/news/single/necurs-hybrid-spam-botnet/
- https://www.virusbulletin.com/virusbulletin/2014/04/curse-necurs-part-1
- https://www.virusbulletin.com/virusbulletin/2014/05/curse-necurs-part-2
- https://www.virusbulletin.com/virusbulletin/2014/06/curse-necurs-part-3
- https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/

### Indicators of Compromise

The following links allow you to download IOCs files in multiple formats - please note that DGA domains are not included:

## Get the Weekly Cybersecurity Newsletter

Subscribe to get security news and industry ratings updates in your inbox.

-
- *
  Read more
  By checking this box, I consent to sharing this information with BitSight Technologies, Inc. to receive email and phone communications for sales and marketing purposes as described in our privacy policy. I understand I may unsubscribe at any time.