EN

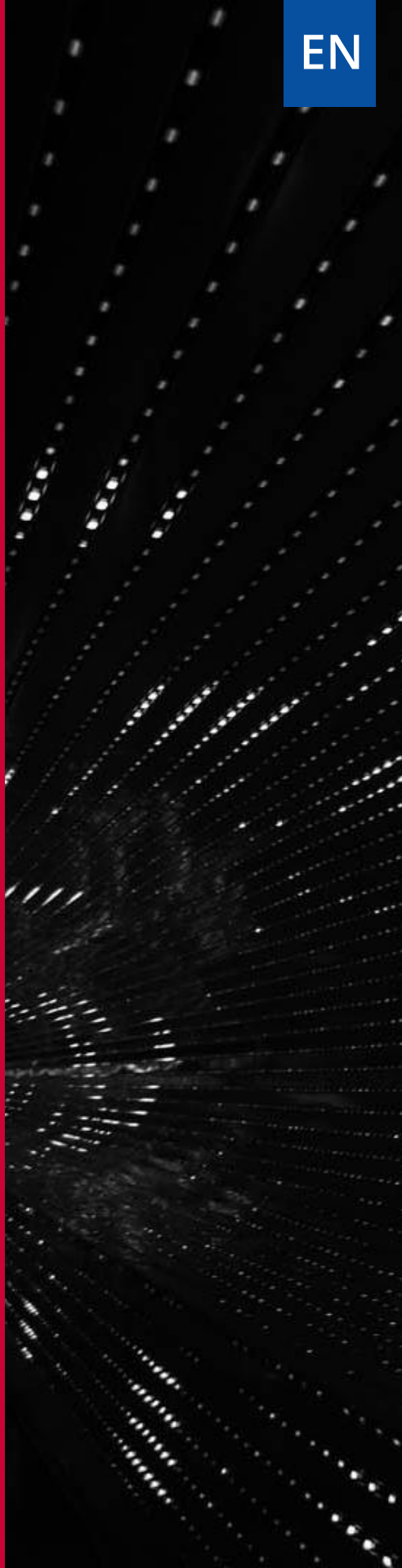
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

# Botnet

## ENISA Threat Landscape



# Overview

**A botnet is a network of connected devices infected by bot malware**. These devices are typically used by malicious actors to conduct Distributed Denial of Service (DDoS) attacks. Operating in a peer-to-peer (P2P)[1] mode or from a Command and Control (C2)[2] center, botnets are remotely controlled by a malicious actor to operate in a synchronised way to obtain a certain result.[3]

Technological advancements in distributed computing and automation have created an opportunity for malicious actors to explore new techniques and improve their tools and attack methods. Thanks to this, botnets operate in much more distributed and automated ways and are available from self-service and ready-to-use providers.

Malicious bots, referred as 'bad bots', are not only constantly evolving but people's skillsets and the bots' level of development are becoming highly specialised in certain applications, such as defence-providers or even evasions techniques.[4] From a different perspective, botnets provide a vector for cybercriminals to launch various operations from e-banking fraud to ransomware, mining cryptocurrencies and DDoS attacks.[5]

# Findings

## 7,7_ million IoT devices are connected to the Internet every day

Of these, 1 in 20 is estimated to be behind a firewall or similar network security tools.[6]

## 57%_ increase in the number of Mirai variants detected during 2019

Although Mirai variants are known to use brute-force attempts predominantly for compromising IoT devices, there was an increase in both brute-force (51%) and web exploitation (87%) attempts during 2019.[7]

## 300.000_ notifications of Emotet botnet traffic observed during 2019

This accounted for over 100.000 more victim alerts than same period in 2018. Researchers believed that there was a 913% increase in the number Emotet samples having compared the second halve of 2018 and 2019.[7]

## 60%_ of new rival botnet activity is associated with stealing credentials[9]

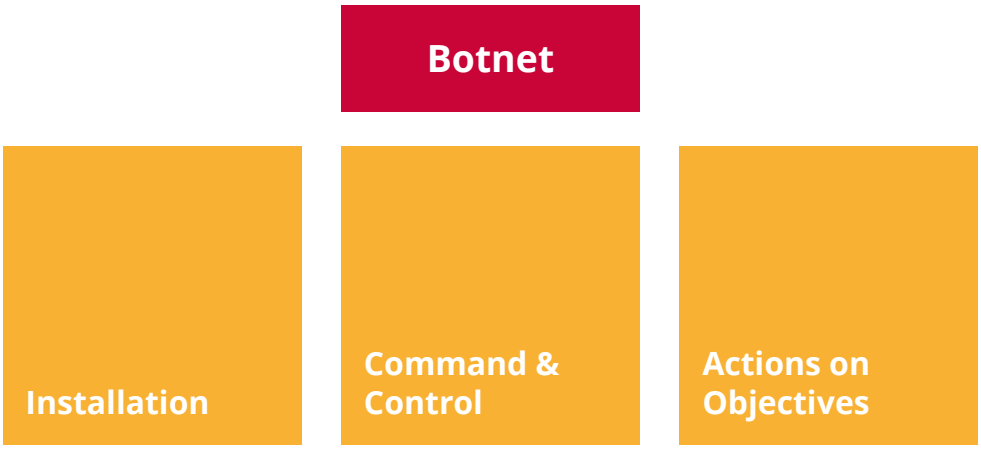
## 17.602_ fully functional botnet C2 servers found in 2019

71,5% increase compared with 2018.[5]

# Kill chain


*Step of Attack Workflow*

*Width of Purpose*




The Cyber Kill Chain® framework was developed by Lockheed Martin, adapted from a military concept related with the structure of an attack. To study a particular attack vector, use this kill-chain diagram to map each step of the process and reference the tools, techniques and procedures used by the attacker.

MORE INFORMATION

# Trends

## _Bots are big money

Bots are facilitating brute-force capabilities by luring victims into buying limited-edition items or items on promotional offers and subsequently reselling them at a higher price. This fact was identified by analysing a job posting in which the advertiser was looking for a software developer with experience of evading security defences, creating bots with evasion techniques (i.e. web scrapping, reCAPTCHA bypass, cookie generation, etc.) and willing to pay US$ 15.000 (ca. €12.750) for the right candidate.[4]

## _The bricking Silexbot

During June 2019, a security researcher[17] analysed a new bot sample developed to disrupt the functionalities of insecure IoT devices. In other words, this bot was designed to use known/default credentials of IoT devices to log-in and subsequently kill the device by deleting network configurations and adding an IP tables' rule to drop all connections. On top of the technical capabilities, an interesting point was the note left on the malware sample. The threat actor apologises for their activity and explains their actions as a way of preventing mass exploitation of insecure IoT devices to build botnets for malicious purposes.

## Echobot and its growing threat vector

During June 2019, a security researcher identified an updated version of Echobot. In this analysis, the researcher observed an x86 compiled sample leading to attack vectors used by this Mirai variant in 26 different incidents.[10] During August, another security researcher found an increase in Echobot, exploiting 50 different vulnerabilities including the 'command injection over HTTP' (CPAI-2016-0658 ).[25,26] In December 2019, another team detected an enhanced version of Echobot including 71 exploits. The newly added exploits were targeting old and new vulnerabilities and had a significant added capability of targeting Industrial Control System (ICS) devices. This included companies and devices such as Mitsubishi, Citrix NetScaler app-delivery controls, Barracuda web application firewall and endpoint administration tools.[27]

## Necurs on the fall while Emotet rises again

During January 2019, Necurs was observed moving into an amateur type of spam campaign, which made researchers think that the malicious actors behind it had a significant decrease in their skillset.[20] In contrast, Emotet's activity increased substantially since September 2019 and continued surging towards the end of 2019, dropping unique compiled binaries representing persistent delivery vector and communication mechanisms.[7] An analysis revealed a sharp increase in the distribution of Emotet by e-mail.[22]

# Trends

## _Retadup, the Botnet behind Monero-Mining has fallen

Retadup was mostly active as the Monero-mining worm that developed polymorphic capabilities.[23] It had infected Windows machines in Latin America. This bot had capabilities raging from mining to deploying custom code and downloaded files to the victims' machines (it was also observed distributing STOP ransomware[24]). A security researcher started monitoring the Retadup activity in March 2019 and noticed that the C2 protocol was designed in a simple way. The team identified a flaw in the protocol that enabled them to remove infections from the victim by taking over the C2 server. The infrastructure for this malicious activity was identified as being mostly in France. The botnet was taken down with the collaboration of the National Gendarmerie (France) and around 850.000 computers were disinfected.

## _Mirai is dead, long live Mirai

It might be because of the lack of skills and features in the original code that Mirai and its variants still dominate in the botnet families, and more than 20.000 unique samples were observed monthly during the first half of 2019. These variants use different techniques for compromising IoTs, from brute-forcing default hard-coded passwords to exploits.[6] There is also a broad diversity of system architectures targeted by these variants according to two security researchers. More statistics on Emotet activity presented in Figure 1.[7,18]

## _The P2P Roboto botnet

Roboto's activity was first observed during August 2019 by a security research team as a P2P botnet program. The first sample captured was a suspicious ELF file. During October the research team identified another sample (ELF file) which turns out to be the downloader of the previous sample. Upon further analysis, the research team discovered that Roboto botnet can support seven function, namely reverse shell, self-deactivation, process and network information gathering, bot information gathering, executing URL specified files, DDoS attacks and running system attacks. Interestingly, it seems that a DDoS attack is not its main use case according to the researcher. Unlike other botnets, this bot was spreading by exploiting the Webmin RCE vulnerability (CVE-2019-1507[28]).[11]

## _Mozi, another DHT based botnet

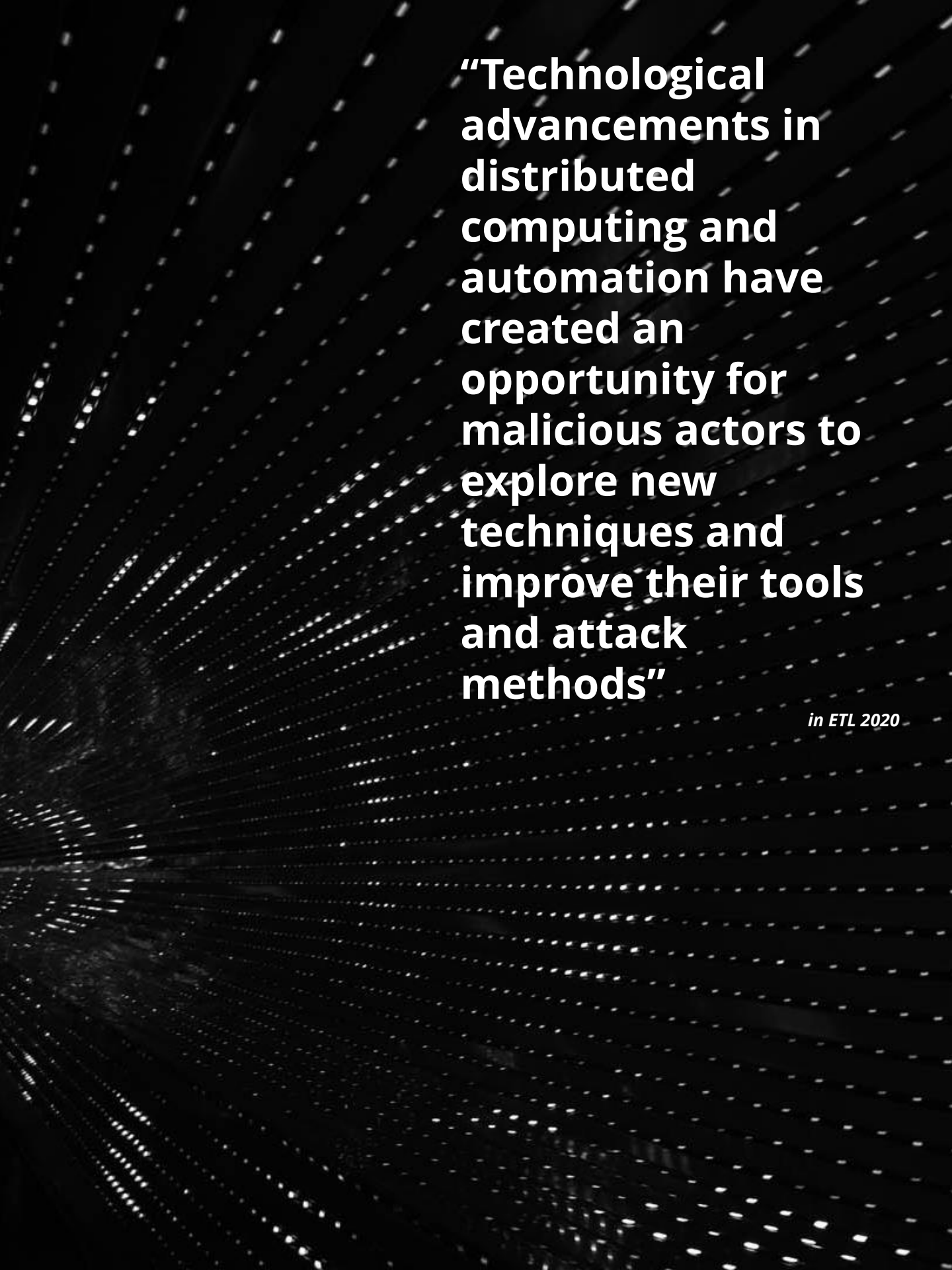
Named after its propagation filename, Mozi has been identified as a brand new DHT based botnet observed by a security researcher in September 2019. An initial analysis of the sample conducted by another security researcher[38] identified it as Gafgyt. However, that was because the sample partially reused the code from Gafgyt. This botnet spreads by using a handful of exploits and exploiting weak passwords for telnet. Analysis of its functionalities revealed that it could be capable of running DDoS attacks, information gathering, executing and updating sample/payload using a specified URL and executing commands.[29, 30]

# Trends

## _Statistics on Emotet activity

| Finding | Statistic |
|---|---|
| **Total number of ASn detected:** | 5.430 |
| **Total number of unique IPs detected:** | 120.764 |
| **Total countries participating:** | 193 |
| **Total emails sent:** | 10.935.346 |
| **Total distribution URLs:** | 4.726 |
| **Distinct RCPTs targeted:** | 8.052.961 |

Figure 1: Source: Spamhaus[5]



**“Technological advancements in distributed computing and automation have created an opportunity for malicious actors to explore new techniques and improve their tools and attack methods”**

***in ETL 2020***

# Findings

## Statistics and other relevant numbers

According to a security researcher, **7,7 million IoT devices are connected to the Internet every day** and only 1 in every 20 is estimated to be behind a firewall or similar network security tool.[6] This estimation reveals that **IoT devices are still vulnerable and susceptible to exploitation** by cybersecurity threats such as Mirai.

- During the first half of 2019, botnet activity and hosting C2 servers increased substantially.[32] This increase represented 7% of all botnet detections and 1,8% of C2s around the world. Financial services and their customers was the sector most often targeted.
- Thailand was the top country in terms of hosting C2 servers while Malaysia came second followed by the Philippines, Singapore and Indonesia.
- Based on Interpol research, the Andromeda botnet was the most dominant in terms of detection although it was dismantled in 2017.[33] Conficker[34] came second followed by Necurs[35], Sality[36] and Gozi[37].

During 2019, the number of Mirai variants detected increased by more than 57% compared with 2018 as depicted in Figure 2.

Although Mirai variants are known to use brute-force attempts predominantly for compromising IoT devices, during 2019 there was an increase in both brute-force (51%) and web exploitation (87%) attempts.

## __Mirai sample count

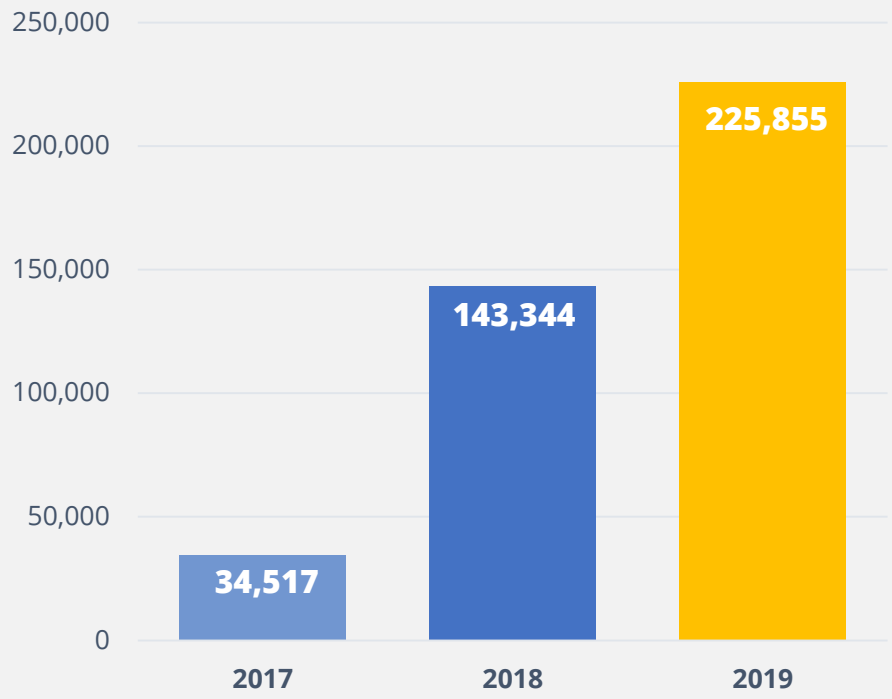



Figure 2: Source: NETSCOUT[7]

# Findings

## Statistics and other relevant numbers

- During 2019, a security researcher observed nearly 300.000 more notifications of Emotet botnet traffic and over 100.000 more victim alerts compared with the same period in 2018. The researcher believes that there was a 913% increase in the number of Emotet samples having compared the second halves of 2018 and 2019.[7,22]
- There was an increase in P2P botnet activity since Roboto and Mozi became active.[8]
- Linux based botnets were responsible for almost 97,4% of attacks.[8]
- The highest share of botnets were registered in the United States (58,33%) in Q4 2019. While this is an increase compared with Q3 2019 (47,55%), the total number of C2 servers almost halved. The United Kingdom was is in fourth place and jumped to second place with 14,29%, while China maintained the same position at 9.52%. The most significant decrease in C2 registered servers was in the Netherlands (from 45% to ~1%). For more information about botnet C2 servers distribution by country please consult Figure 3.[8]
- In 2019, LokiBot remained at the top of the list of credential stealing bots with an increase in the number of C2 activity by 74% compared with 2018. AZORult was in second position right behind LokiBot.[39]
- 17.602 botnet C2 servers were live during 2019, representing a 71,5% increase compared with 2018.[39]

# Distribution of botnet C&C servers by country

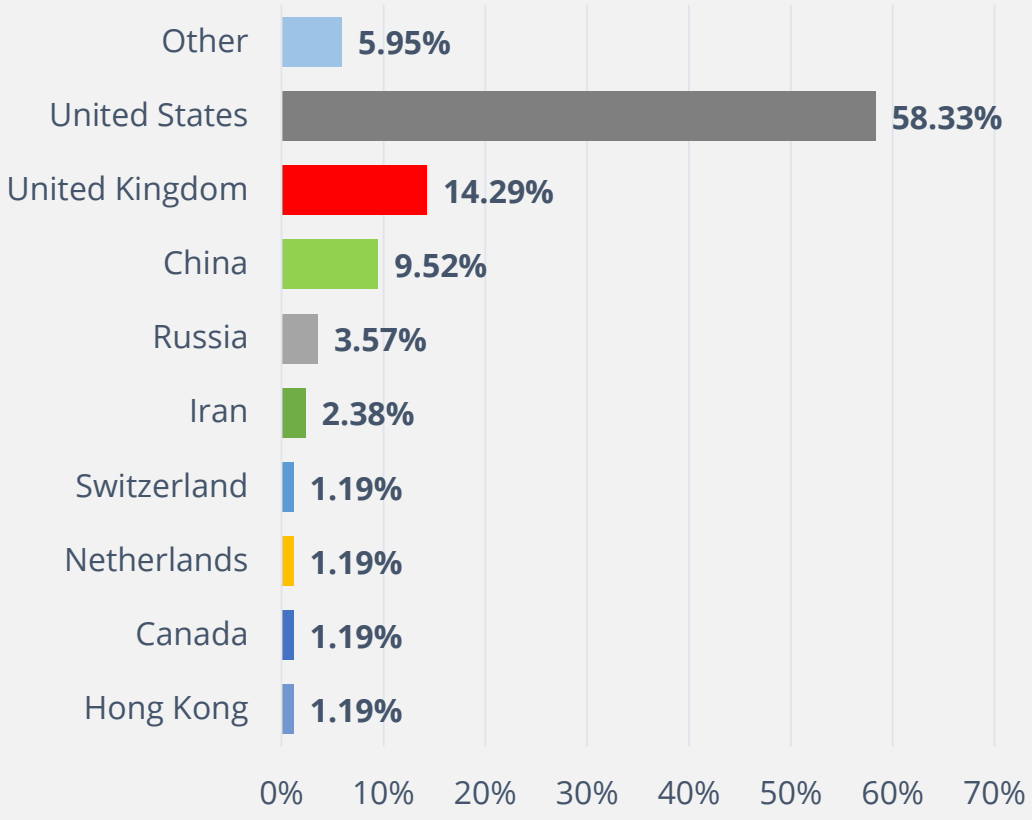



Figure 3: Source: Kapersky[8]

# Attack vectors

## The botnet attacks

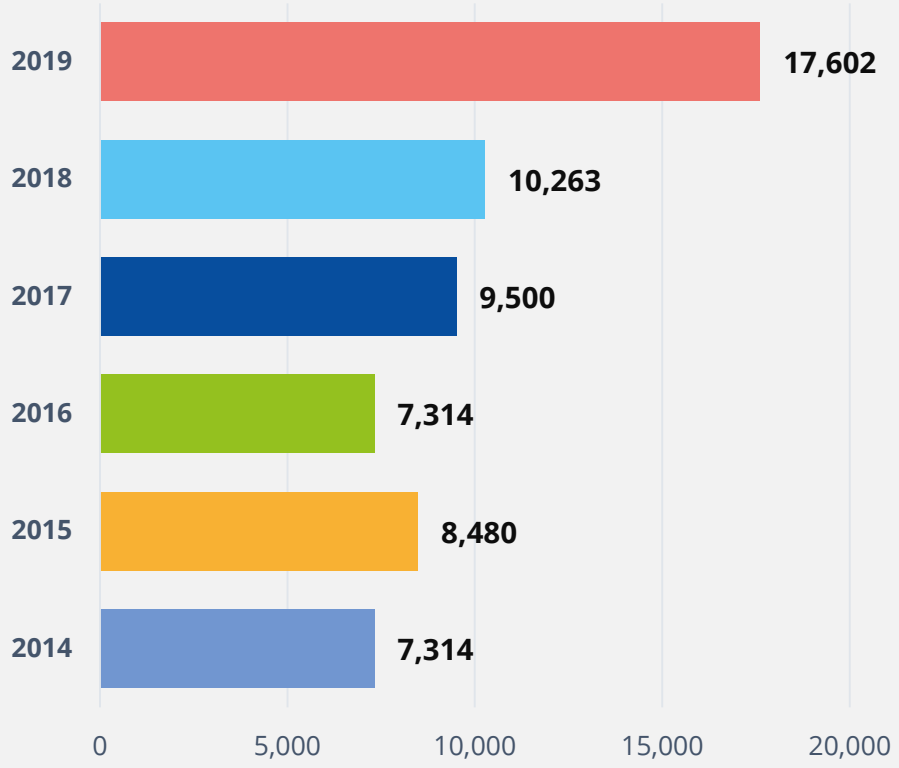
According to a security researcher, in 2019, nearly 60% of new rival botnet activity was associated with **stealing credentials**. As previously mentioned, LokiBot is the most active in this area. In addition to the credential-stealing activity, **e-banking and financial fraud** are other areas where botnet's presence is vast. Emotet and TrickBot are prime examples of this activity with an updated model covering not only e-banking fraud but also pay-per-install (PPI).[9]

Moreover, **Remote Access Trojans (RATs)** were among the most used tools in botnets C2 activities. During 2018, most of these activities were associated with Adwind, but in 2019, its activity was reduced and replaced by NanoCore.[5]

**Specific attack vectors were adopted** in 2019. Botnets use various attack vectors to reach their objectives. Infected machines or zombie networks are created by exploiting common vulnerabilities with brute-force and other common infection techniques.[10,11,12] Subsequently, the botmaster is capable of providing a platform for different attacks including the widespread spamming and malware campaign, stealing and reusing credentials, crypto-mining and DDoS.

Another example of an attack vector used in a botnet attack is the **'Triple Threat'**. In this technique, the targeted organisation is initially infected with Emotet malware. Then the Emotet malware delivers the TrickBot Trojan, targeting and exploring sensitive information. If the information is found and the targeted environment/network is in the attacker's list, Ryuk ransomware is delivered.[13]

# Number of botnet C2 servers observed between 2014 and 2019




Source: Spamhaus[5]

# Mitigation

## _ Proposed actions

One key aspect of having a solid defence is the concept of knowing the environment. This will help to identify malicious activity within the traffic based on the possible baseline (i.e. behavioural detections)[14] measured by a traffic monitoring tool.[4] Considering that substantial botnet traffic is associated with DDoS activity, mitigation techniques for DDoS threat also apply.

- Deploy border gateway protocol feeds with the capability to look for dTLDs (decentralised top-level domains) to block connections to IP addresses related to botnet C2 activity.[8]
- Understand and categorise vulnerabilities and implement a strong patching and updating practice.[15,16]
- Restrict or block cryptocurrency mining pools and monitor the environment for required users.[5]
- Deploy challenge based capabilities for required websites to check the origin of traffic (i.e reCAPTCHA).[16]
- Deploy strong password and authentication (2FA) policies on public-facing servers or infrastructure to avoid being a victim of weak password/authentication exploitation.[5]
- Deploy and configure network and application firewalls.


“The threat landscape is becoming extremely difficult to map. Not only attackers are developing new techniques to evade security systems, but threats are growing in complexity and precision in targeted attacks.”
in ETL 2020

# References


**1.** "Peer-to-peer (P2P)." Malwarebytes Labs https://blog.malwarebytes.com/glossary/peer-to-peer/

**2.** Monnappa K A. "Learning Malware Analysis." June 2018. O'reilly. https://www.oreilly.com/library/view/learning-malware-analysis/9781788392501/17a1735d-9583-4d86-9d1e-8b2735af5168.xhtml

**3.** "ASEAN Cyberthreat Assessment 2020." February 17, 2020. Interpol https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-highlights-key-cyberthreats-in-Southeast-Asia

**4.** "State of The Internet Security - DDoS and Application Attacks Report: Volume 5, Issue 1." 2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf

**5.** "Spamhaus Botnet Threat Report 2019." January 28, 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

**6.** "NETSCOUT Threat Intelligence Report: Powered by ATLAS - Findings from H1 2019." 2019.

**7.** "NETSCOUT Threat Intelligence Report - With key findings from the 15th Annual Worldwide Infrastructure Security Report (WISR) - Findings from H2 2019." 2019. NETSCOUT. https://www.netscout.com/threatreport

**8.** Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q4 2019." February 13, 2020. Kaspersky. https://securelist.com/ddos-report-q4-2019/96154/

**9.** Alina Dettmer. "What is Pay Per Install.?" October 26, 2017. Aye Studios. https://www.ayetstudios.com/blog/mobile-advertising/mobile-campaign-types/pay-per-install

**10.** Larry Cashdollar. "Latest Echobot: 26 Infection Vectors." June 13, 2019. Akamai. https://blogs.akamai.com/sitr/2019/06/latest-echobot-26-infection-vectors.html

**11.** "The awaiting Roboto Botnet." November 20, 2019. Netlab. https://blog.netlab.360.com/the-awaiting-roboto-botnet-en/

**12.** Asher Davila. "Home & Small Office Wireless Routers Exploited to Attack Gaming Servers." October 31, 2019. Paloalto. https://unit42.paloaltonetworks.com/home-small-office-wireless-routers-exploited-to-attack-gaming-servers/

**13.** "Triple Threat: Emotet deploys Trickbot to steal data & spread Ryuk." April 2, 2019. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

**14.** "Bots." Imperva. https://www.imperva.com/learn/application-security/what-are-bots/

**15**. Rebecca Carter. "Bot Mitigation Best Practices." October 19, 2018. DYN. https://dyn.com/blog/bot-mitigation-best-practices/

**16.** "What is a Botnet?" Veracode. https://www.veracode.com/security/botnet

**17.** "SIRT Advisory: Silexbot bricking systems with known default login credentials". June 26, 2019. Akamai.

**18.** "Mirai Botnet Continues to Plague IoT Space". September 10, 2019. Reversing Labs. https://blog.reversinglabs.com/blog/mirai-botnet-continues-to-plague-iot-space

**19.** The Shadowserver Foundation. https://www.shadowserver.org/

**20.** "As Necurs Botnet Falls from Grace, Emotet Rises" January 27, 2020. Threat Post. https://threatpost.com/as-necurs-botnet-falls-from-grace-emotet-rises/152236/

**21.** "Mirai malware, attacks Home Routers". December 14, 2016. ENISA. https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

**22.** "Estimating Emotet's size and reach". December 12, 2019. SPAMHAUS. https://www.spamhaus.org/news/article/791/estimating-emotets-size-%20-and-reach

**23.** "Monero-Mining RETADUP Worm Goes Polymorphic, Gets an AutoHotKey Variant". April 23, 2018. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-retadup-worm-goes-polymorphic-gets-an-autohotkey-variant/

**24.** "Meet Stop Ransomware: The Most Active Ransomware Nobody Talks About". September 20, 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/meet-stop-ransomware-the-most-active-ransomware-nobody-talks-about/

**25.** "Command Injection Over HTTP". July 26, 2016. Check Point. https://www.checkpoint.com/defense/advisories/public/2016/cpai-2016-0658.html/

**26.** "August 2019's Most Wanted Malware: Echobot Launches Widespread Attack Against IoT Devices". August 2019. Check Point. https://blog.checkpoint.com/2019/09/12/august-2019s-most-wanted-malware-echobot-launches-widespread-attack-against-iot-devices/

**27.** "Echobot Malware Now up to 71 Exploits, Targeting SCADA". December 18, 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits--targeting-scada

**28.** "CVE-2019-15107 Detail". NIST. https://nvd.nist.gov/vuln/detail/CVE-2019-15107

**29.** "What is a distributed hash table?". EDPresso. https://www.educative.io/edpresso/what-is-a-distributed-hash-table

**30.** "A Look into the Gafgyt Botnet Trends from the Communication Traffic Log". July 23, 2019. https://nsfocusglobal.com/look-gafgyt-botnet-trends-communication-traffic-log/

**32.** "ASEAN Cyberthreat Assessment 2020, Key Insights From The ASEAN Cybercrime Operations Desk" Interpol, 2020

**33.** "International team takes down virus-spewing Andromeda botnet". December 5, 2017. The Register. https://www.theregister.com/2017/12/05/international_team_takes_down_virusspewing_andromeda_botnet/

**34.** "The odd, 8-year legacy of the Conficker worm". November 21, 2016. WeLiveSecurity. https://www.welivesecurity.com/2016/11/21/odd-8-year-legacy-conficker-worm/

**35.** "The Necurs Botnet: A Pandora's Box of Malicious Spam". April 24, 2017. https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/

**36.** "WhitePaper: Sality: Story of a Peer to-Peer Viral Network". June 10, 2011. Broadcom.

**37.** "Botnet C&C: Gozi". FortiGuard Labs. https://fortiguard.com/encyclopedia/botnet/7630489

**38.** Virustototal. https://www.virustotal.com

**39.** "Spamhaus Botnet Threat Report 2019" 2020 . Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

# Related


READ THE REPORT

ENISA Threat Landscape Report
**The year in review**

A summary on the cybersecurity trends for the period between January 2019 and April 2020.


READ THE REPORT

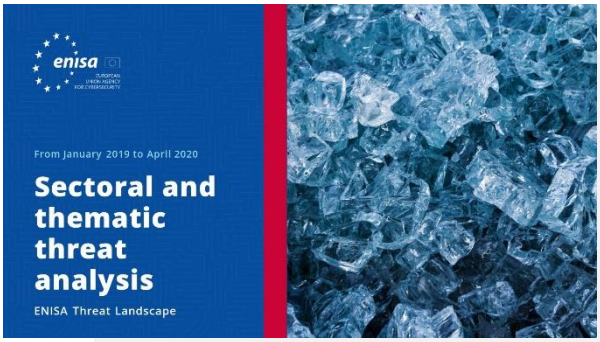
ENISA Threat Landscape Report
**List of Top 15 Threats**

ENISAs' list of the top 15 threats of the period between January 2019 and April 2020.


READ THE REPORT

ENISA Threat Landscape Report
**Research topics**

Recommendations on research topics from various quadrants in cybersecurity and cyber threat intelligence.




READ THE REPORT

ENISA Threat Landscape Report **Sectoral and thematic threat analysis**

Contextualised threat analysis between January 2019 and April 2020.


READ THE REPORT

ENISA Threat Landscape Report **Emerging trends**

Main trends in Cybersecurity observed between January 2019 and April 2020.


READ THE REPORT

ENISA Threat Landscape Report **Cyber Threat Intelligence overview**

The current state of play of cyber threat intelligence in the EU.

# About

## _ The agency

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

**Contributors**

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) and *all members of the ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) and Thomas Hemker.

**Editors**

Marco Barros Lourenço (ENISA) and Louis Marinos (ENISA).

**Contact**

For queries on this paper, please use enisa.threat.information@enisa.europa.eu.

For media enquiries about this paper, please use press@enisa.europa.eu.

## Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

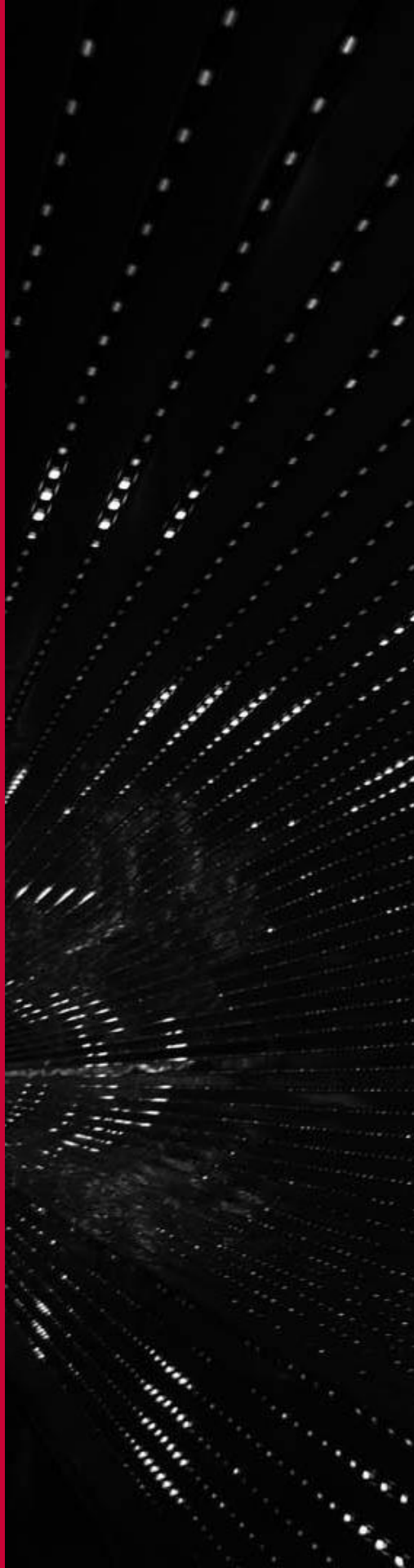
This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.




**ISBN:** 978-92-9204-354-4
**DOI:** 10.2824/552242



Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu



enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



https://www.enisa.europa.eu