



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

# HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

## **HC3 Intelligence Briefing** **\*\*\*\* Botnet Threat to the Healthcare** **Industry\*\*\***

**OVERALL CLASSIFICATION IS**

**TLP:WHITE**

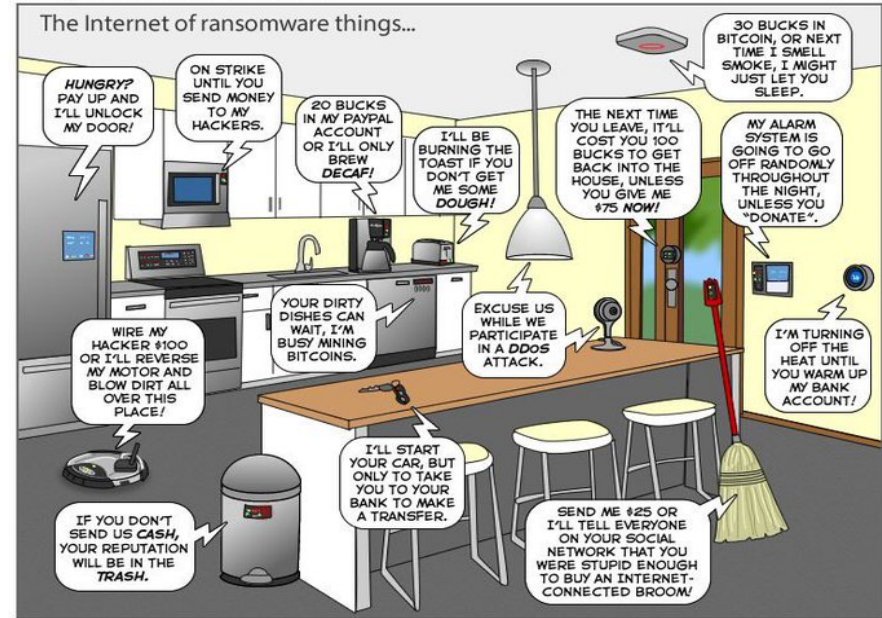
**January 16, 2020**



# Agenda

- Overview
- Botnet Breakdown
- Anatomy of Botnet
- Botnet Architecture
- Mirai
- Reaper/Echobot
- Emotet/The Gamut/ Necurs
- Future of IPv6 Security and IoT
- Mitigations
- Prevention
- Questions

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron! [www.patreon/joyoftech](http://www.patreon/joyoftech)

[Support.feelpc.com](http://Support.feelpc.com)

joyoftech.com

## Slides Key:



Non-Technical: managerial, strategic and high-level (general audience)



Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

# Overview



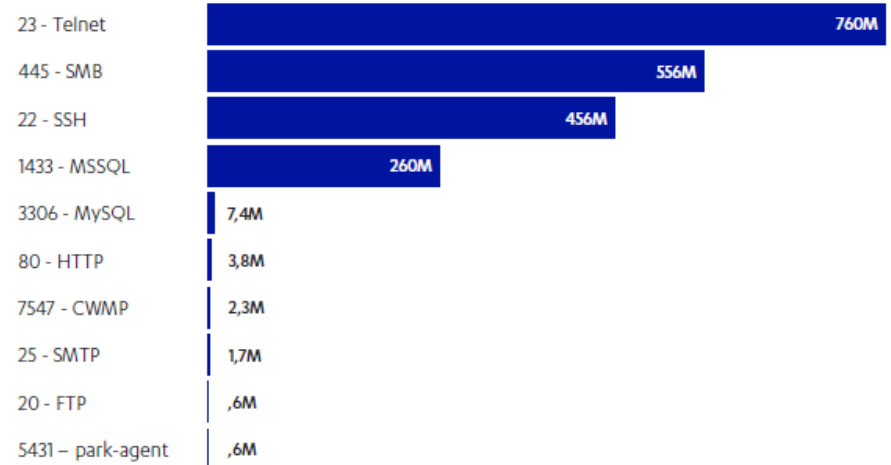
- Hackers are launching cyberattacks against SMB ports and IoT devices at a record pace, with the US facing the greatest number of hacking attempts, according to a recent report from F-Secure.
  - IoT sensor networks are characteristically different to conventional networks. Sensor devices are low powered and often use batteries as their primary source of energy.
  - Therefore, energy efficiency is a priority. These power restrictions mean that devices have limited processing capabilities, which often results in poor security
- F-Secure researchers set up a network of honeypots – decoy servers set up around the globe – to get a pulse of the current threat landscape. The report found these attempts have tripled in the past year: The honeypots measured a total of 2.9 billion events
  - Of those attacks, 2.1 billion were on the TCP port. Telnet, which is rarely used anymore outside of the realm of IoT devices, saw the greatest volumes during the period.
  - Primarily used on IoT devices. Mirai malware, which proliferated in 2018, is continuing to highly target these devices.
  - Mirai hackers have also created variants specifically engineer to infect enterprise IoT devices, which “allows attackers access to greater bandwidth connections than are available with consumer devices, affording them greater power for DDoS attacks.”

Total Global Honeypot Attacks Per Period



F-Secure

Top TCP Ports Targeted



F-Secure

F-Secure



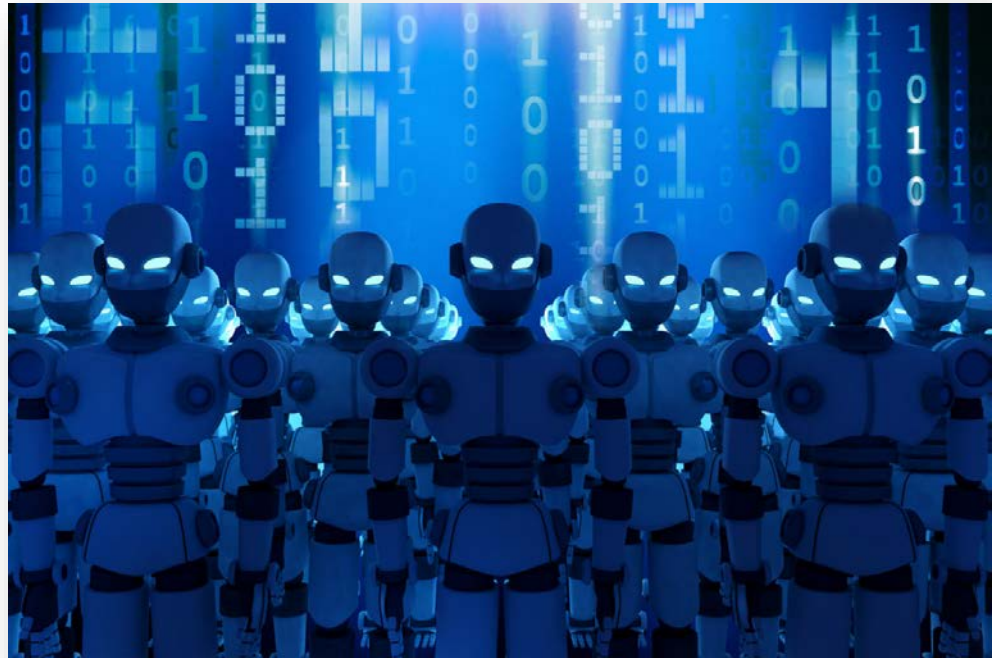
# Botnet Breakdown...



- A botnet is a collection of internet-connected devices that an attacker has compromised. Botnets act as a force multiplier for individual attackers, cyber-criminal groups and nation-states looking to disrupt or break into their targets' systems.
- Commonly used in distributed denial of service (DDoS) attacks, botnets can also take advantage of their collective computing power to send large volumes of spam, steal credentials at scale, or spy on people and organizations.

## Why botnets exist

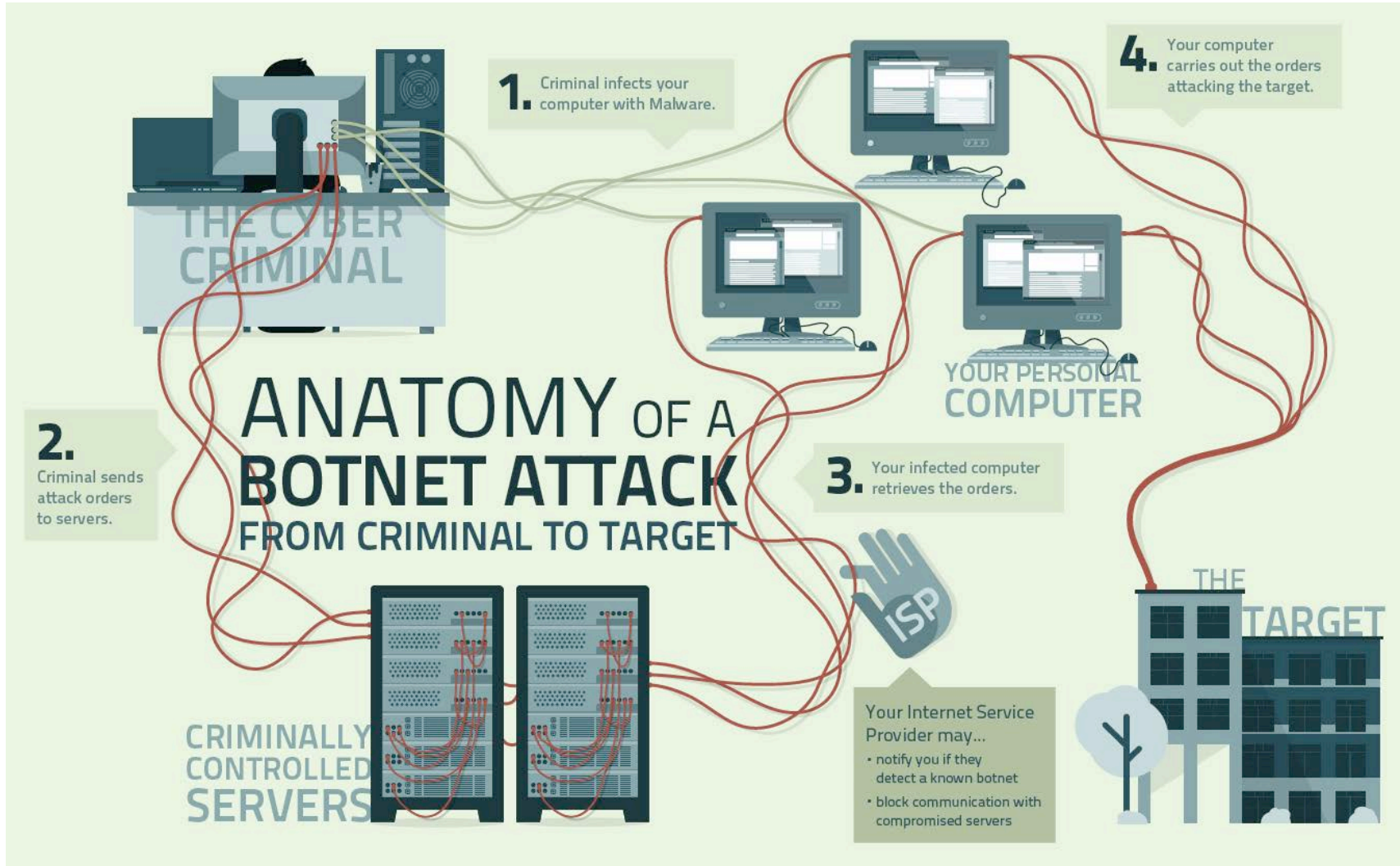
- Operating botnets has two distinct advantages.
  - First, the botmaster is hard to trace because the actual attacks are launched by bots that are distributed both on the network and geographically.
  - Second, the distributed network of bots allows the botmaster to instigate largescale automated attacks. Botnets made up of thousands of computers or devices allow attackers to send a vast number of emails, collect massive amounts of information, or disrupt access to a website quickly and efficiently.



CSO Online

CSO Online





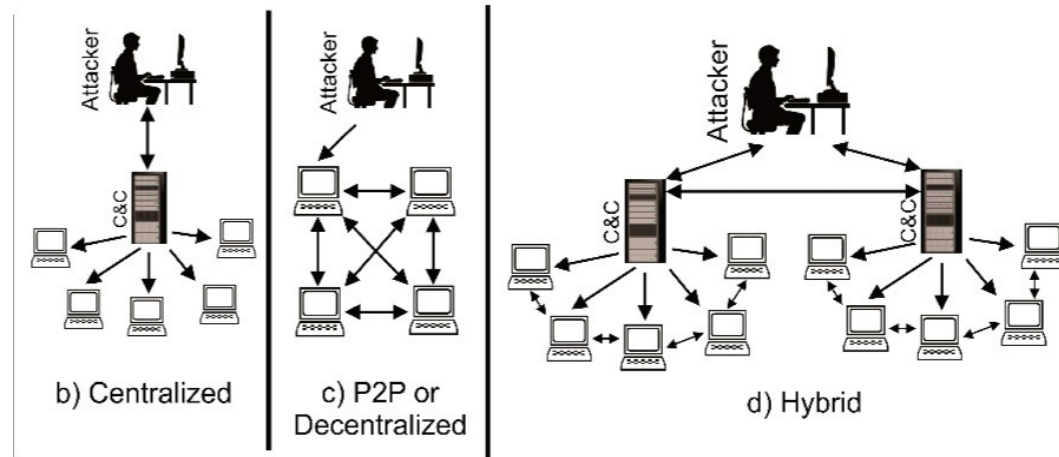
Cybersecurity Observatory



# Botnet Architectures



- **Centralized Architecture:** With centralized botnet architecture, the botmaster controls all the bots in a botnet from a single central hub referred to as the command and control server (C&C).
  - Here all the bots connect directly to the C&C server and all receive directives from it. Once the C&C server is identified, it is very easy to take down this type of botnet.
- **Decentralized Architecture:** With the decentralized botnet architecture, no single machine controls the bot in a botnet. There are several command and control servers which are connected and communicates with the bots.
  - With this type of botnet architecture every bot in the botnet is a control and command server as well as a zombie (bot). Detecting this type of botnet is very difficult as it has no central control.
- **Hybrid Architecture:** Hybrid architecture is a combination of both centralized and decentralized architecture. States that with hybrid architecture there are two types of bots.
  - The client bot and the servant bot. Monitoring and detection of botnets having hybrid architecture is harder than with centralized and decentralized architecture.



MDPI

# Mirai Malware



- Mirai caused widespread disruption during 2016 and 2017 with a series of large-scale DDoS attacks. According to, 65,000 devices were infected in 20 hours, and the botnet achieved a peak size of 600,000 nodes . ([Security and Communication Networks Volume 2019](#))
  - Mirai uses worm-based propagation, which is characterised by periods of scanning for vulnerable devices, reportedly targeting IoT-enabled cameras, routers, printers, and video recorders during its “rapid scanning phase”
- Since the Mirai botnet’s source code was leaked online three years ago, malicious actors have continuously experimented and created their own upgraded versions. ([Securing digital economy](#))
  - As of July 2019, the Mirai botnet has at least 63 confirmed variants and it is very possible others remain undiscovered.
  - IBM Security Intelligence reports that activity from Mirai variants almost doubled between 2018 and 2019.
  - AT&T Cybersecurity researcher reported that whenever they look at new IoT malware — it’s almost inevitably a new Mirai variant. Every day they see new Mirai variants with different payloads.



[The Hacker News](#)





## Reaper (aka IoTroop)

- In fall 2017, Check Point researchers said they discovered a new botnet, variously known as "IoTroop" and "Reaper," that's compromising IoT devices at an even faster pace than Mirai did. ([Checkpoint](#))
  - Mirai infected vulnerable devices that used default user names and passwords. Reaper goes beyond that, targeting at least nine different vulnerabilities from nearly a dozen different device makers, including major players like D-Link, Netgear and Linksys. It's also flexible, in that attackers can easily update the botnet code to make it more damaging.
  - According to research by Recorded Future, Reaper was used in attacks on European banks in 2019, including ABN Amro, Rabobank and Ing.



[FossBytes](#)

## Echobot

- Discovered in early 2019, Echobot is a Mirai variant that uses at least 26 exploits to propagate itself. Like many other botnets, it takes advantage of unpatched IoT devices, but also exploits vulnerabilities in enterprise applications such as Oracle WebLogic and VMware SD-WAN.
- Echobot was discovered by Palo Alto Networks, and [its report on the botnet](#) concludes that it is an effort to form larger botnets to execute larger DDoS attacks.



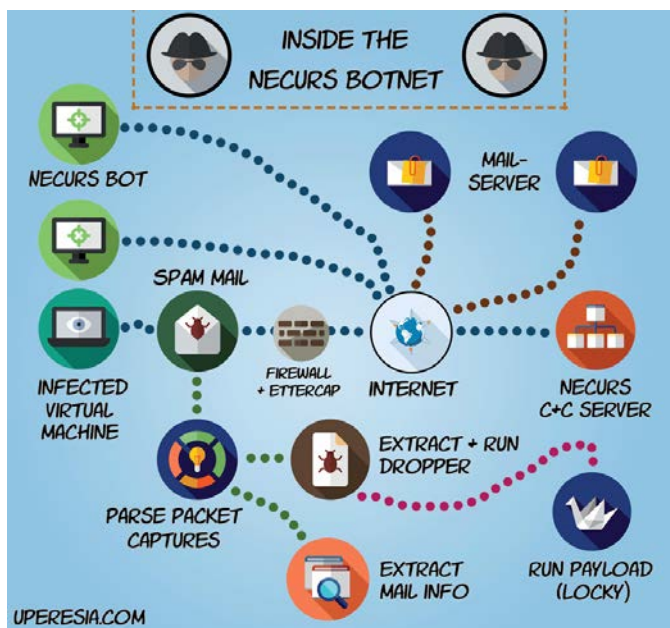
[Trojan Killer](#)



# Emotet, Gamut and Necurs

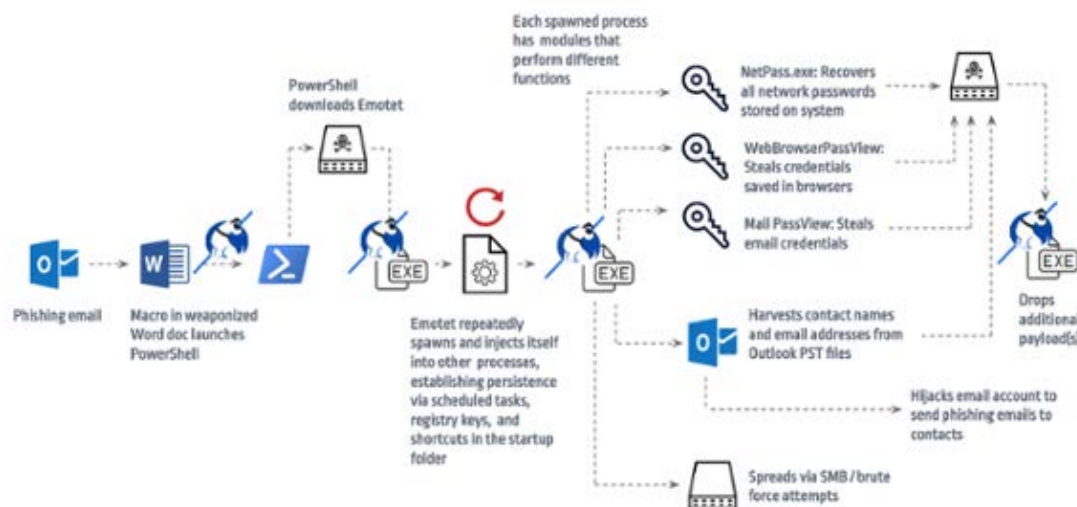


- The main purpose of these three botnets is to spew spam at high volume to deliver a malicious payload or get victims to perform a certain action.
  - **Emotet** can steal email from victims' mailboxes, which allows the attackers to craft convincing yet malicious messages to fool recipients. Attackers can also use it to steal SMTP credentials, useful to take over email accounts.
  - **Gamut** seems to specialize in spam emails that try to establish a relationship with the victims. This might be in the form of a dating or romance guise. In other campaigns, the actors behind the botnet send out messages hawking pharmaceuticals or job opportunities
  - **Necurs** first emerged in 2012 and has spread a variety of threats, ranging from Zeus to ransomware. While its activity has received far more attention in the past, Necurs appears to have faded into the background. However, this botnet is still very much active. In fact, the Necurs botnet is the primary distribution vehicle for a variety of scams, including digital extortion.



[uperesia.com](http://uperesia.com)

## Emotet Trojan: Attack Diagram



[CERT-PY](http://CERT-PY)

CSO online, CISCO



# Future of IPv6 Security and IoT



Network World

- IPv6 is an internet protocol defined by the Internet Engineering Task Force (IETF) and was created to replace the older IPv4 protocol over time.
  - As the number of internet users and connected devices grows across the globe, networks are increasingly providing IPv6 connectivity, and in many cases IPv6 and IPv4 are deployed together.
- Akamai's State of the Internet Security report notes that IPv6 still being seen as a minority of traffic, it's not a major selling point for a number of security tools.
- Botnets like Mirai gain new bots through automated scans of the IPv4 address space, and vulnerable devices are usually infected within a few minutes of connecting to the internet.
  - By contrast, scanning the IPv6 address space has been considered extremely difficult due to the sheer size. Nonetheless, for years, experts have been warning that undiscovered vulnerabilities in the IPv6 protocol, combined with the growth of IoT, could allow for massive botnet attacks.
- There is now at least one documented case of an IPv6 DDoS attack, which used a technique known as DNS amplification instead of a botnet
  - While it did not amount to a major incident, the question must be asked: could IPv6 result in more and bigger DDoS attacks over time?
  - The rise of IPv6 botnet attacks would present unique challenges that have no easy fix. For instance, the incredibly large number of IPv6 addresses (over 8,000 times more than IPv4) could allow attackers to overwhelm the memory of security systems designed to handle IPv4- based threats

## Securing Digital Economy





## Machine Learning

- **Supervised learning** is the category of machine learning algorithms that generates a function that maps inputs to desired outputs. These supervised machine learning algorithms are trained by examples of inputs and their corresponding outputs and then they are used to predict output for some future inputs.
  - In the context of botnet detection, supervised machine learning algorithms are used in implementing network traffic classification. These network classifiers are able to classify network traffic as malicious or non-malicious as well as identify traffic belonging to different botnets.
- **Unsupervised machine learning** is a type of machine learning in which training data has not been labeled. The machine learns by analyzing the data characteristics to construct the classifier. Unsupervised learning involves training data consists of a set of inputs without any corresponding output values. The goal in unsupervised learning approach to problem solving is to firstly discover groups of similar examples within the input data, where it is called clustering, to determine the distribution of data within the input space, known as density estimation.
  - In botnet detection, unsupervised machine learning algorithms are commonly used for the clustering of bot-related observations most popularly used unsupervised machine learning algorithms used in botnet detection are the K-means, X-means, and hierarchical clustering.



ARITEX

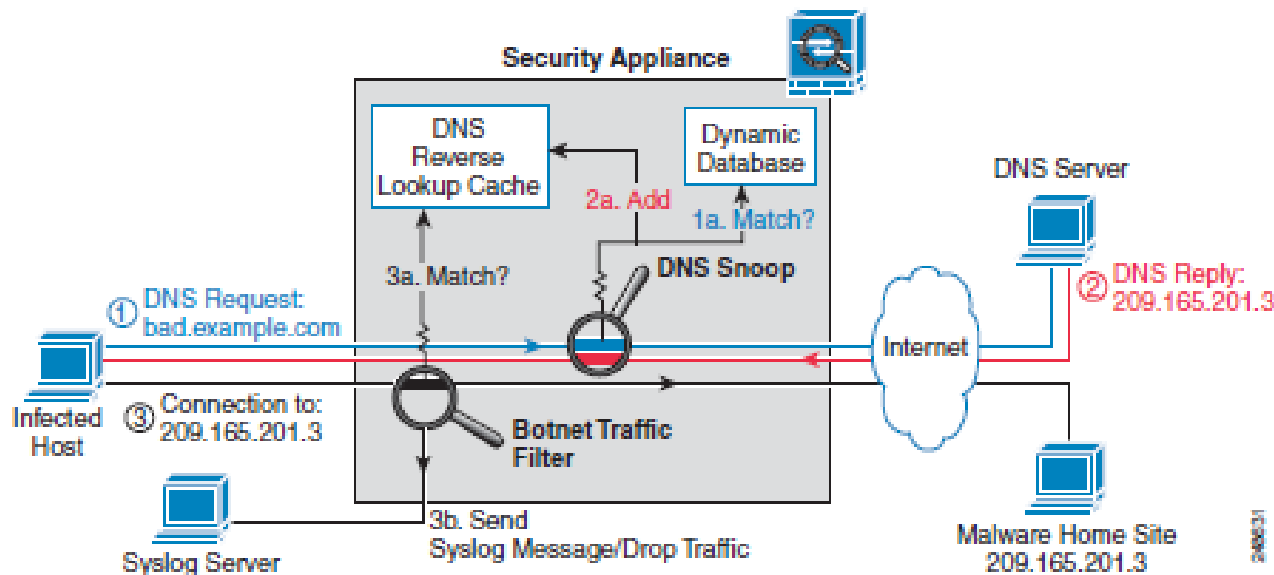
[Researchgate.net](https://www.researchgate.net)





## Filtering

- One of the complications when mitigating botnets is that malicious actors use IP-spoofing to make bad traffic appear to come from somewhere other than its actual place of origin. By filtering out bad traffic as it enters the provider's, providers can reduce the effectiveness of spoofing and therefore make DDoS attacks more difficult to carry out.
  - Due to the readily observable benefits of this practice, the Internet Engineering Task Force (IETF) has recognized ingress filtering as a best practice. It is worth noting that ingress filtering works better at network ingress points such as customer premises, whereas it is much more difficult at network exchange points.
- Finally, in a network setting, Access Control Lists (ACLs) are used to identify traffic flows based on parameters such as its source and destination, IP protocol, ports, EtherType, and other characteristics.
  - A common example is that traffic from a lower security interface cannot access a higher security interface. In some contexts, ACLs may be configured to account for the access privileges of individual users to further limit the attack vectors by which malware can infiltrate a network.



Securing Digital Economy

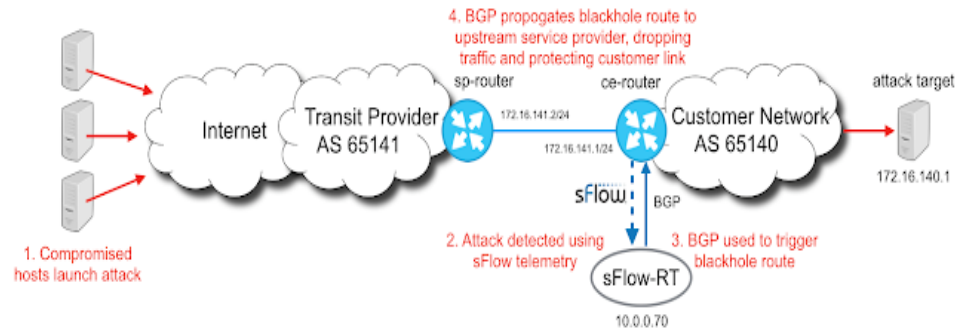


# Mitigations cont...



## Blackholing

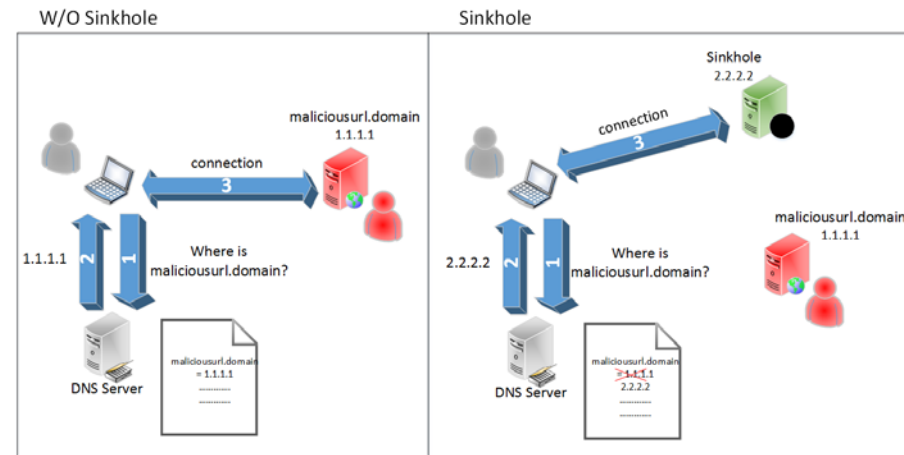
- Blackholing is a technique that drops all traffic headed toward a specific online destination. A common version of this technique is remotely triggered destination based blackholing (RTDBH) in which upstream networks, which are typically closest to the attack source, drop the malicious traffic before it reaches a potential victim.



SFLOW

## Sinkholing

- Sinkholing is a technique where traffic within a particular IP-range is sent to a designated server (the “sinkhole”) whereas traffic outside that IP-range continues as normal. The purpose of sinkholing is to capture botnets for both research and mitigation purposes.
- When malware caught in a sinkhole tries to communicate with command-and-control servers, security experts can track the IP addresses of machines the malware feeds information to, thus gaining insight into criminal activities.
  - Providers can also completely sever communications between the malware and the command-and-control servers.
  - Sinkholes are essential to large-scale takedowns of botnets, which use hundreds of thousands of internet-enabled systems in multiple countries throughout the world.



ENISA

## Securing Digital Economy





# Preventive Steps



2.M.A, 2.S.A	Basic Endpoint Protection Controls	NIST FRAMEWORK REF: PR. AT PR.IP-1, PR.AC-4,PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-3
9.M.A, 9.S.A	Medical Device Security	NIST FRAMEWORK REF: PR. PT, PR.MA

- Ensure all default passwords are changed to strong passwords. Default usernames and passwords for most devices can easily be found on the Internet, making devices with default passwords extremely vulnerable.
- Update IoT devices with security patches as soon as patches become available.
- Disable Universal Plug and Play (UPnP) on routers unless absolutely necessary.
- Purchase IoT devices from companies with a reputation for providing secure devices.

**Health Industry Cybersecurity Practices:**  
Managing Threats and Protecting Patients



Healthcare & Public Health  
Sector Coordinating Councils  
PUBLIC PRIVATE PARTNERSHIP

405(d) HICP

US-CERT



# Preventive Steps



2.S.A	Basic Endpoint Protection Controls	NIST FRAMEWORK REF: PR. AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-3
9.S.A	Medical Device Security	NIST FRAMEWORK REF: PR. PT

- Consumers should be aware of the capabilities of the devices and appliances installed in their homes and businesses. If a device comes with a default password or an open Wi-Fi connection, consumers should change the password and only allow it to operate on a home network with a secured Wi-Fi router.
- Understand the capabilities of any medical devices intended for at-home use. If the device transmits data or can be operated remotely, it has the potential to be infected.
- Monitor Internet Protocol (IP) port 2323/TCP and port 23/TCP for attempts to gain unauthorized control over IoT devices using the network terminal (Telnet) protocol.
- Look for suspicious traffic on port 48101. Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor.

**Health Industry Cybersecurity Practices:**  
Managing Threats and Protecting Patients



Healthcare & Public Health  
Sector Coordinating Councils  
PUBLIC PRIVATE PARTNERSHIP

405(d) HICP

US-CERT

# Questions

## Upcoming Briefs

- Zeppelin Ransomware
- Ryuk Update

## Previous HC3 briefs

- Internet of Things
- Emotet Update



## Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to [HC3@HHS.GOV](mailto:HC3@HHS.GOV).

## Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to [HC3@HHS.GOV](mailto:HC3@HHS.GOV) or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.





# References

- Attack Landscape H1 2019: IoT, SMB traffic abound

<https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/>

- Cisco: Email: Click with Caution

<https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf>

- International BOTNET and IOT Security Guide 2020

[https://securingdigiteconomy.org/wp-content/uploads/2019/11/CSDE\\_Botnet-Report\\_2020\\_FINAL.pdf](https://securingdigiteconomy.org/wp-content/uploads/2019/11/CSDE_Botnet-Report_2020_FINAL.pdf)

- Botnet Identification Using Machine Learning Techniques: A Survey

[https://www.researchgate.net/publication/334284867\\_Botnet\\_Identification\\_Using\\_Machine\\_Learning\\_Techniques\\_A\\_Survey](https://www.researchgate.net/publication/334284867_Botnet_Identification_Using_Machine_Learning_Techniques_A_Survey)

- Machine Learning in Cyber Security Domain – 9: Botnet Detection

<https://www.normshield.com/machine-learning-in-cyber-security-domain-9-botnet-detection/>

- A Graph-Based Machine Learning Approach for Bot Detection

<https://arxiv.org/pdf/1902.08538.pdf>

- Heightened DDoS Threat Posed by Mirai and Other Botnets

<https://www.us-cert.gov/ncas/alerts/TA16-288A>

- New Mirai Variant Adds 8 New Exploits, Targets Additional IoT Devices

<https://unit42.paloaltonetworks.com/new-mirai-variant-adds-8-new-exploits-targets-additional-iot-devices/>





# References

- A New IoT Botnet Storm is Coming

<https://research.checkpoint.com/2017/new-iot-botnet-storm-coming/>

- Machine learning for identifying botnet network traffic

<https://vbn.aau.dk/ws/portalfiles/portal/75720938/paper.pdf>

- Modelling the Spread of Botnet Malware in IoT-Based Wireless Sensor Networks

<https://www.hindawi.com/journals/scn/2019/3745619/>

- What is a botnet?

<https://www.pandasecurity.com/mediacenter/security/what-is-a-botnet/>

- What is a botnet? When armies of infected IoT devices attack

<https://www.csoonline.com/article/3240364/what-is-a-botnet.html>

- The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

<https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html>

