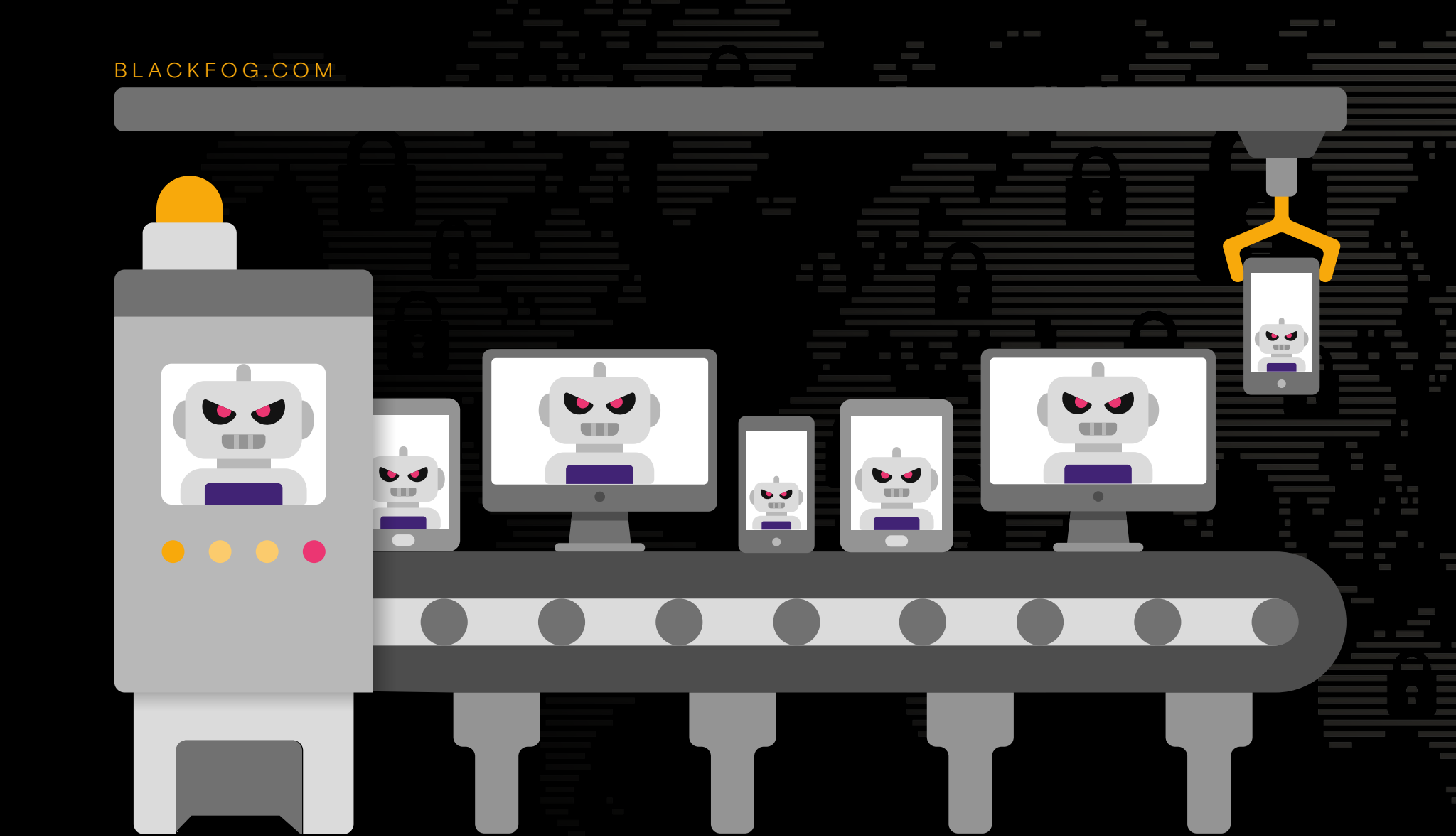
BLACKFOG™

Botnets: From IRC to IoT

A GUIDE FOR MSPS & CYBERSECURITY LEADERS



Contents

Overview 3

1. What is a Botnet? 4
2. Botnets in the Media 6
3. IRC Botnets 8
4. HTTP Botnets 9
5. P2P Botnets 10
6. Mobile Botnets 11
7. IoT Botnets 12
8. The Concept of Bot Shops and Install for Install (I4I) 13
9. How Can Botnet Activities Be Mitigated? 15

Frequently Asked Questions 17

Stop Data Theft with BlackFog 20

Botnets have become a significant threat to cybersecurity, with their ability to carry out a wide range of malicious activities, including Distributed Denial-of-Service (DDoS) attacks, spam email campaigns, cryptocurrency mining, data theft, and the spread of malware. In this article, we will explore the different types of botnets, their functionalities, and provide examples of notorious botnets that have caused significant damage.

1

What is a Botnet?

A botnet is a network of compromised computers or devices, often referred to as "zombies" or "bots," that are controlled by a malicious actor known as a "botmaster" or "bot herder."

The devices in a botnet can include personal computers, servers, mobile devices, and even Internet of Things (IoT) devices like smart cameras, routers, and appliances. Cybercriminals create botnets by infecting large numbers of devices with malware, which allows them to remotely control the devices without the knowledge or consent of their owners. This malware can spread through various means, such as phishing emails, malicious websites, or unpatched software vulnerabilities.

Once a device is compromised and becomes part of a botnet, the botmaster can use it to carry out a variety of malicious activities.

Types of Malicious Activity:

Botnet Attack Type	Description
Distributed Denial-of-Service (DDoS) attacks	Botnets can flood targeted websites or networks with a massive amount of traffic, overwhelming them and rendering them inaccessible to legitimate users.
Spam and phishing campaigns	Botnets can be used to send out large volumes of spam emails or phishing messages designed to trick recipients into revealing sensitive information or downloading additional malware.
Credential stuffing attacks	Botnets can automatically test large lists of stolen usernames and passwords across multiple websites to gain unauthorized access to user accounts.
Cryptocurrency mining	Botmasters can use the collective computing power of a botnet to mine cryptocurrencies, generating profits at the expense of the compromised devices' owners.
Data theft	Botnets can be used to steal sensitive information, such as financial data, personal information, or intellectual property, from compromised devices or networks.
Extortion	Botnets can be used to carry out extortion schemes, such as threatening to launch DDoS attacks against a target unless a ransom is paid or using stolen data to blackmail individuals or organizations.

2

Botnets in the Media

Botnets often receive less media attention compared to threats like ransomware due to the difficulty in attributing and tracking their activities. If a botnet were to take down a website, for example, it would be incredibly challenging to determine who was responsible based solely on the network traffic generated by the attack. Unless a person or group comes forward and claims responsibility, the true culprits behind the attack often remain unknown. The distributed nature of botnets, with the controlling party hidden behind layers of compromised devices, makes pinpointing the origin of an attack an enormous challenge.

In contrast, ransomware attacks often have distinct characteristics that make them easier to track and attribute to specific threat actors. Ransomware typically leaves behind unique indicators, such as the specific file extension used to encrypt targeted files, or the presence of ransom notes containing distinguishable language and demands. These calling cards allow security researchers to connect attacks to known cybercriminal groups or individuals. Botnets, on the other hand, lack these types of clear branding elements, making it more difficult to link their activities to specific entities.

The effects of a successful ransomware attack are often more immediately visible and disruptive than those of a botnet. When ransomware strikes, the consequences are apparent: files become encrypted, ransom demands are issued, and business operations are disrupted.

In comparison, the impact of a botnet attack, such as taking a website offline through a DDoS attack or quietly stealing data, may be less immediately apparent or attributable to the botnet itself.

Analyzing botnet activity also presents unique challenges compared to investigating ransomware incidents. Ransomware attacks typically generate a concentrated burst of activity, providing security researchers with ample network logs and data to analyze.

Botnets, however, operate in a more distributed and piecemeal fashion over an extended period, making their traffic patterns harder to isolate and study.

3

IRC Botnets

IRC (Internet Relay Chat) botnets are one of the earliest types of botnets, utilizing IRC servers for command and control (C&C) communication between the botmaster and the compromised devices. IRC is a protocol that facilitates real-time text messaging, making it an ideal platform for controlling botnets. The botmaster can issue commands to the bots through specific IRC channels, instructing them to perform various malicious activities.

ID	Value	Description
1	*BOT_COMPNICK*	Use computer name as nick name
2	*BOT_SECLOGIN*	Enable login only by channel messages
3	*BOT_RANDNICK*	Assign random nickname to bot
4	*BOT_MELSERVER*	Melt original server file
5	*BOT_TOPICCMD*	Execute topic commands
6	*DO_SPEEDTEST*	Do speedtest on startup
7	*DO_AVKILL*	Enable AV software disabling
8	*DO_STEALTH*	Enable stealth mode
9	*AS_ENABLED*	Enable Autostart
10	*AS_SERVICE*	Install as service
11	*IDENTD_ENABLED*	Enable the server
12	*CDKEY_WINDOWS*	Get Windows CD keys
13	*SPAM_AOL_ENABLED*	Enable AOL spamming
14	*SNIFFER_ENABLED*	Enable sniffer
15	*INST_POLYMORPH*	Polymorph on installation

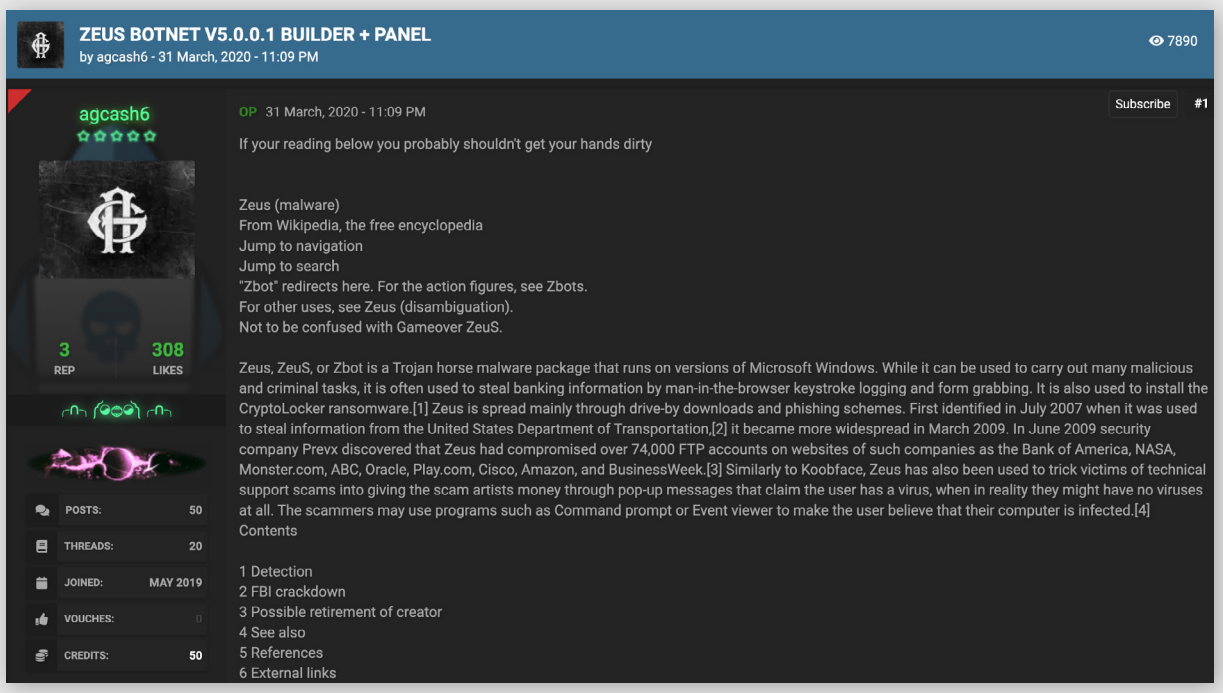
The different parameters that Agobot accepts

One example of an IRC botnet is Agobot, a modular botnet that has been used for DDoS attacks, keylogging, and data theft. Agobot's source code was leaked in 2004, leading to the development of numerous variants and inspiring the creation of other IRC botnets. The modular nature of Agobot allows botmasters to easily add or remove functionalities, making it highly adaptable to different malicious purposes.

4

HTTP Botnets

As cybersecurity measures evolved, botnet operators shifted towards using HTTP or HTTPS protocols for C&C communication. HTTP botnets are harder to detect and block because they blend in with legitimate web traffic. Botmasters can create web-based control panels to manage their bots, issue commands, and monitor their activities.



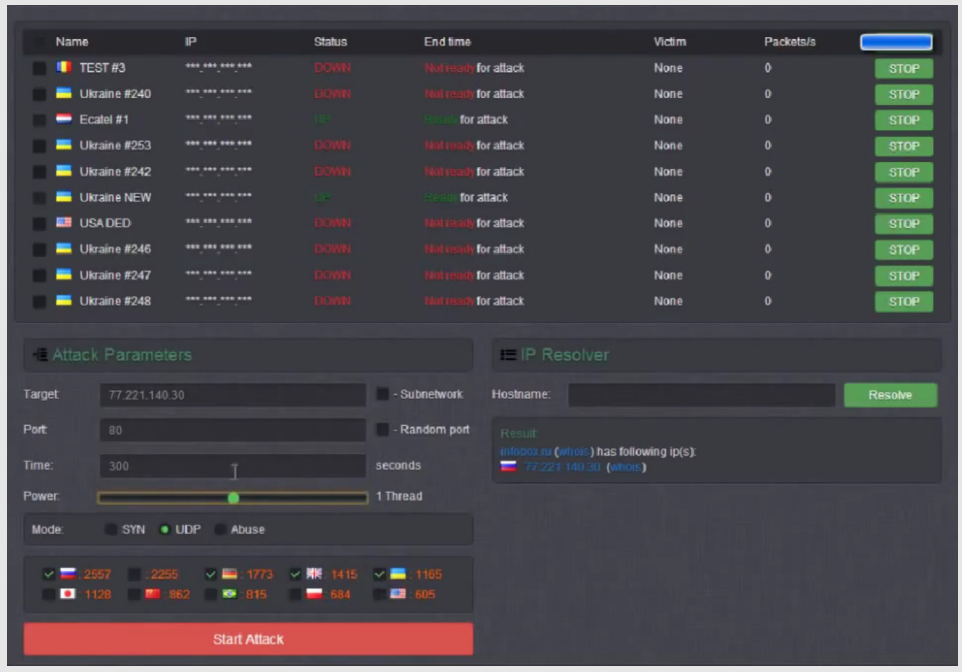
An old version of Zeus Bot being shared on a cybercrime forum

The Zeus botnet, also known as Zbot, is a notorious example of an HTTP botnet. Zeus is primarily designed to steal banking credentials and other sensitive information from infected computers. It uses techniques like keystroke logging and form grabbing to capture user input and send it back to the botmaster. The Zeus botnet has been responsible for significant financial losses worldwide, with some estimates suggesting that it has caused damages exceeding $100 million.

5

P2P Botnets

Peer-to-Peer (P2P) botnets have emerged as a more resilient alternative to centralized botnets. In a P2P botnet, there is no central C&C server; instead, the bots communicate directly with each other, forming a decentralized network. This architecture makes P2P botnets more difficult to take down, as there is no single point of failure. Even if some bots are discovered and removed, the remaining bots can continue to operate and maintain the botnet's functionality.



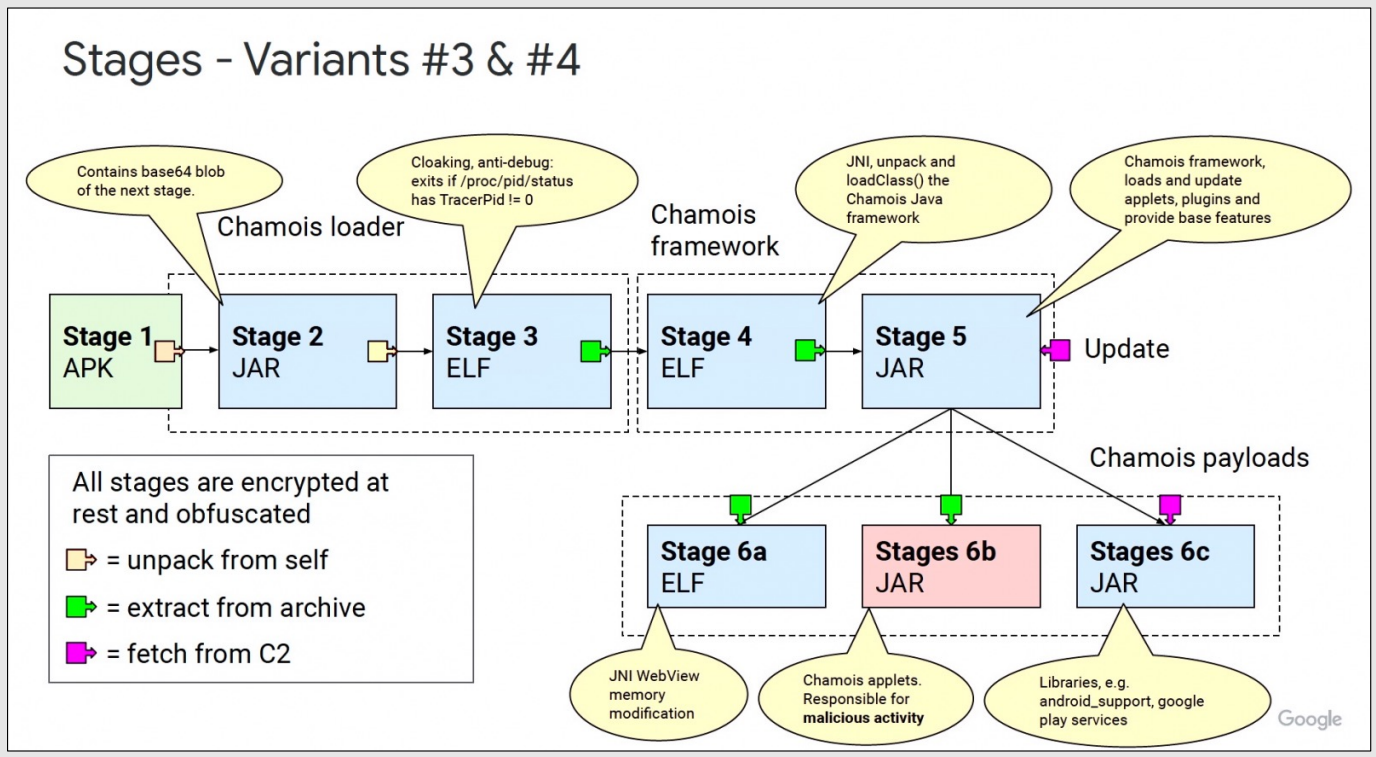
The user interface for Storm botnet

The Storm botnet is a prime example of a P2P botnet that has caused significant damage. It uses the Overnet P2P protocol for C&C communication and has been used for various malicious activities, including spam email campaigns and DDoS attacks. At its peak, the Storm botnet was estimated to have infected millions of computers worldwide, making it one of the largest botnets ever created.

6

Mobile Botnets

With the proliferation of mobile devices, such as smartphones and tablets, botnet operators have started targeting these devices to expand their botnets. Mobile botnets often spread via malicious apps or SMS messages, exploiting vulnerabilities in mobile operating systems or tricking users into installing malware.



A technical explanation of how Chamois botnet functions

The Chamois botnet is an example of an Android botnet that has infected millions of devices worldwide. Chamois uses infected devices for ad fraud, generating fake clicks on advertisements to earn money for the botmasters. It also has the capability to install additional malware on the compromised devices, further expanding its malicious potential.

7

IoT Botnets

IoT has introduced a new attack surface for botnet operators. IoT devices, such as smart cameras, routers, and home appliances, often have weak security measures and default credentials, making them easy targets for compromise. Once infected, these devices can be used to carry out DDoS attacks, mine cryptocurrencies, or spread malware to other devices.

Search Results

Thread / Author	Forum	Replies	Views	Last Post [asc]
[TUT] How to Setup Mirai Botnet works 100% [1 2 3 4] Prix1337	Botnets and Botting	56	1,964	14 hours ago Last Post: dzig
[Help] Mirai Botnet decyption	Botnets and Botting	0	55	Mar 12, 2024 04:17 AM Last Post: decyption
[Help] Vps for mirai botnet SIM-5186353	Botnets and Botting	11	145	Mar 9, 2024 12:34 AM Last Post: FunkyPigeon174
mirai botnet benddd1230	Botnets and Botting	1	171	Feb 23, 2024 11:51 AM Last Post: SIM-5186353
[Help] Mirai botnet setup SIM-5186353	Botnets and Botting	2	57	Feb 21, 2024 09:35 PM Last Post: SIM-5186353
The best Botnet for DDOS? Mirai alternatives? gloomez	Blackhat Training	2	142	Feb 21, 2024 06:28 AM Last Post: LaDullahan
[World] Mirai Botnet Variant 'Pandora' Hijacks Android TVs for Cyberattacks BiNBo	News and Happenings	3	164	Dec 23, 2023 10:30 PM Last Post: CryptedNetwork
Mirai Botnet is still alive and kicking ChickenSoupFortuneTeller	Botnets and Botting	4	439	Dec 23, 2023 10:28 PM Last Post: CryptedNetwork
Mirai Botnet Detected? [1 2] Prix1337	Botnets and Botting	15	283	Oct 24, 2023 11:25 AM Last Post: Kayfoxz

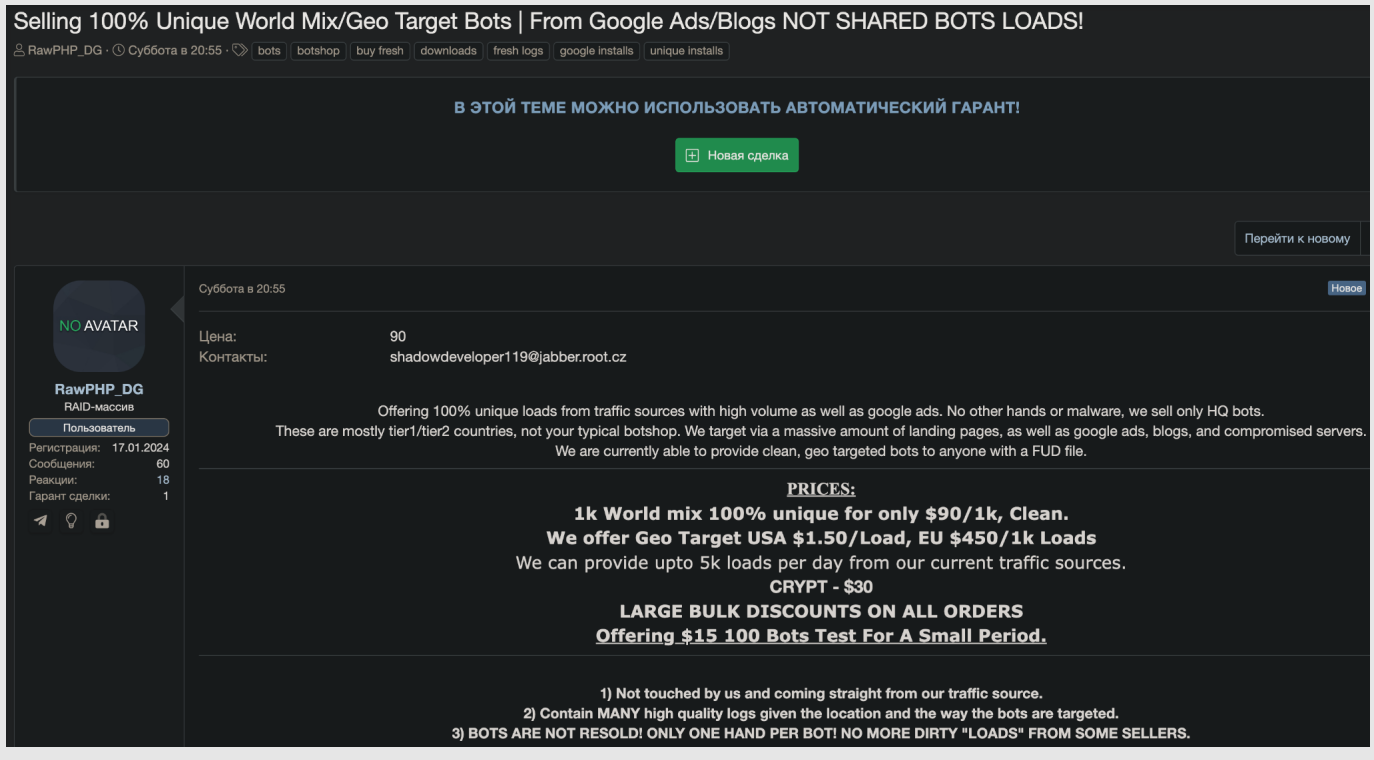
Discussions posted on a cybercrime forum surrounding Mirai

The Mirai botnet is a notorious example of an IoT botnet that has caused significant disruption. Mirai targets IoT devices with default or weak credentials, infecting them and using them to carry out large-scale DDoS attacks. In 2016, the Mirai botnet was used to launch a massive DDoS attack against the DNS provider Dyn, causing widespread internet outages and affecting major websites like Twitter, Netflix, and Reddit.

8

The Concept of Bot Shops and Install for Install (I4I)

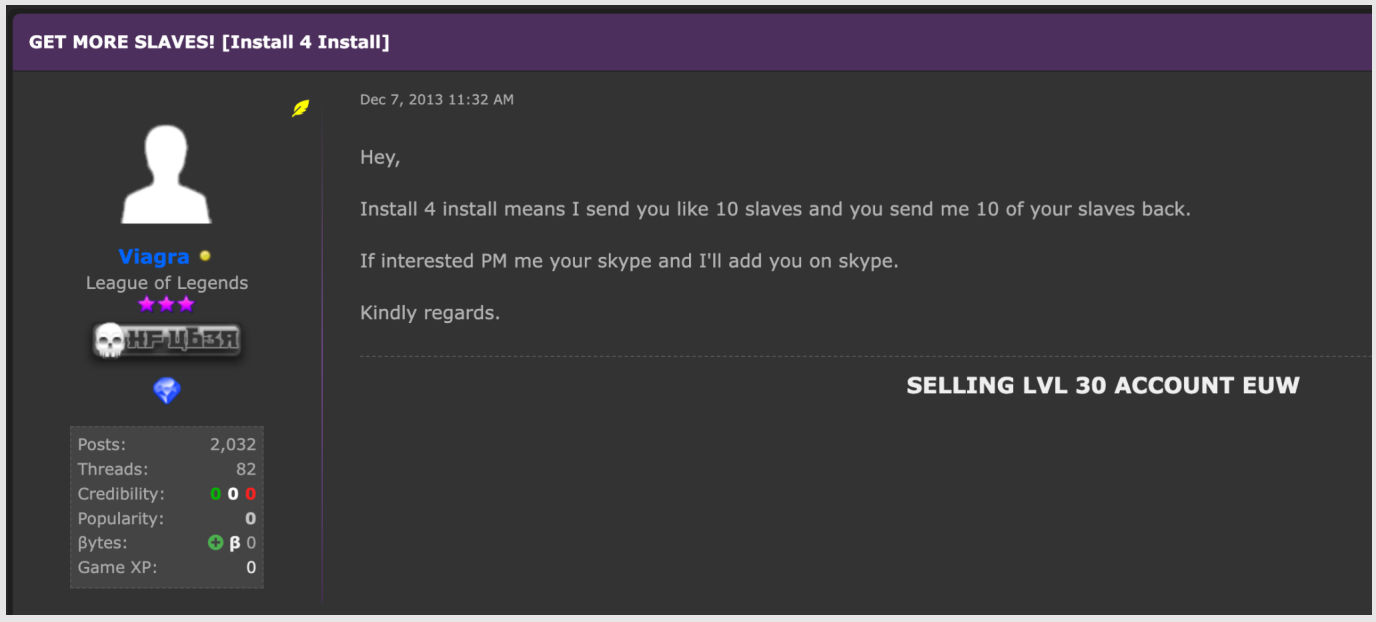
The cybercriminal underground has seen the rise of “bot shops” - online marketplaces where botnet operators can sell or rent access to their networks of compromised devices. These bot shops have made it easier for less technically skilled criminals to carry out attacks and malicious activities, as they no longer need to build and maintain their own botnets.



An example of a bot shop on a cybercrime forum

Customers of bot shops can purchase access to a certain number of bots for a specified period, often paying based on the size of the botnet and the duration of access. Some bot shops even offer different tiers of service, with higher-priced packages providing access to more powerful or stealthier bots.

Another concept that has emerged in the botnet ecosystem is “Install for Install” (I4I). In this arrangement, botnet operators collaborate to grow their respective networks by exchanging infections. When one operator’s botnet infects a new device, it will also install the malware of their partner’s botnet, and vice versa. This mutual exchange helps both operators expand their botnets without the need for additional resources or infrastructure.



An example of a cybercriminal offering I4I

I4I agreements can be particularly beneficial for smaller botnet operators who may struggle to compete with larger, more established players in the market.

By partnering with other operators, they can rapidly increase the size and reach of their botnets, making them more attractive to potential buyers or renters.

9

How Can Botnet Activities Be Mitigated?

Mitigating the threat posed by botnets requires a multi-faceted approach because there is no one-size-fits-all solution. The specific strategies and tools used will depend on the type of attack being carried out by the botnet and the unique characteristics of the affected organization or individual.

For example, if a botnet is being used to conduct DDoS attacks, mitigation efforts may focus on implementing traffic filtering and rate limiting techniques to block the malicious traffic while allowing legitimate requests to pass through. This can be achieved through the use of specialized DDoS mitigation services or by configuring firewalls and intrusion prevention systems (IPS) to detect and block the attack traffic.

In the case of botnets being used for spam or phishing campaigns, mitigation may involve deploying advanced email filtering solutions that can identify and block malicious messages based on their content, sender reputation, or other characteristics. This can be combined with user education initiatives to help individuals recognize and avoid falling victim to these scams.

If a botnet is being used for data theft or exfiltration, mitigation efforts may focus on implementing strong access controls, encryption, and monitoring solutions to prevent unauthorized access to sensitive information and detect any suspicious activities. This can include measures such as multi-factor authentication, network segmentation, and anti data exfiltration (ADX) tools.

It is important to note that a botnet is often just a means of delivery and not an actual attack type. To effectively mitigate the threat posed by botnets, organizations and individuals must first identify the specific type of attack they are facing. Once the attack type has been identified, targeted research can be conducted to determine the most appropriate mitigation strategies and tools for that particular scenario.

FREQUENTLY ASKED QUESTIONS

Here are some frequently asked questions that will help with the comprehension of botnets:

1

What types of devices can be part of a botnet?

Botnets can include various devices, such as personal computers, servers, mobile devices, and IoT devices like smart cameras, routers, and appliances.

2

What are some common activities carried out by botnets?

Botnets can be used for a wide range of malicious activities, including distributed DDoS attacks, spam email campaigns, cryptocurrency mining, data theft, credential stuffing attacks, and extortion.

3

How have botnets evolved over time?

Botnets have evolved from using IRC for C&C communication to utilizing HTTP/HTTPS protocols, P2P architectures, and targeting mobile devices and IoT devices. These changes have made botnets more resilient and harder to detect and take down.

4

What are “bot shops” and “Install for Install” (I4I) in the context of botnets?

Bot shops are online marketplaces where botnet operators can sell or rent access to their networks of compromised devices. I4I is an arrangement where botnet operators collaborate to grow their networks by exchanging infections, installing each other’s malware on newly infected devices.

Stop Data Theft with BlackFog

As we highlighted earlier, some botnets will engage in data theft and exfiltrate information from infected devices to use or sell on cybercrime forums and networks. Something that we're able to do at BlackFog is prevent data exfiltration from a device or network with our ADX technology.

BlackFog's ADX solution uses advanced AI algorithms and behavioral analytics to detect and block suspicious outbound traffic in real-time, without relying on signature-based detection methods that can easily be evaded.

This lightweight, user-centric approach allows our technology to run on endpoints, mobile devices, and IoT devices, ensuring comprehensive protection across your entire digital ecosystem.

Click here to arrange a demo and find out how we can help you!

BLACKFOG™

ABOUT BLACKFOG

BlackFog is the leader in on-device data privacy, data security and ransomware prevention. Our behavioral analysis and anti data exfiltration (ADX) technology stops hackers before they even get started. Our cyberthreat prevention software prevents ransomware, spyware, malware, phishing, unauthorized data collection and profiling and mitigates the risks associated with data breaches and insider threats. BlackFog blocks threats across mobile and desktop endpoints, protecting organizations data and privacy, and strengthening regulatory compliance.

All contents copyright © 2024 BlackFog, Inc. All rights reserved. The BlackFog logo and name are trademarks of BlackFog, Inc. All other trademarks are the property of their respective owners.

Except as specifically stated herein, none of the material may be copied, reproduced, distributed, republished, downloaded, displayed, posted, or transmitted in any form without authorized, prior written permission from BlackFog, Inc. Permission is granted for you to make a single copy of this document solely for informational uses within your organization, provided that you keep intact all copyright and other proprietary notices. No other use of the information provided is authorized.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The information contained in this document represents the current view of BlackFog, Inc. on the issues discussed as of the date of publication.
