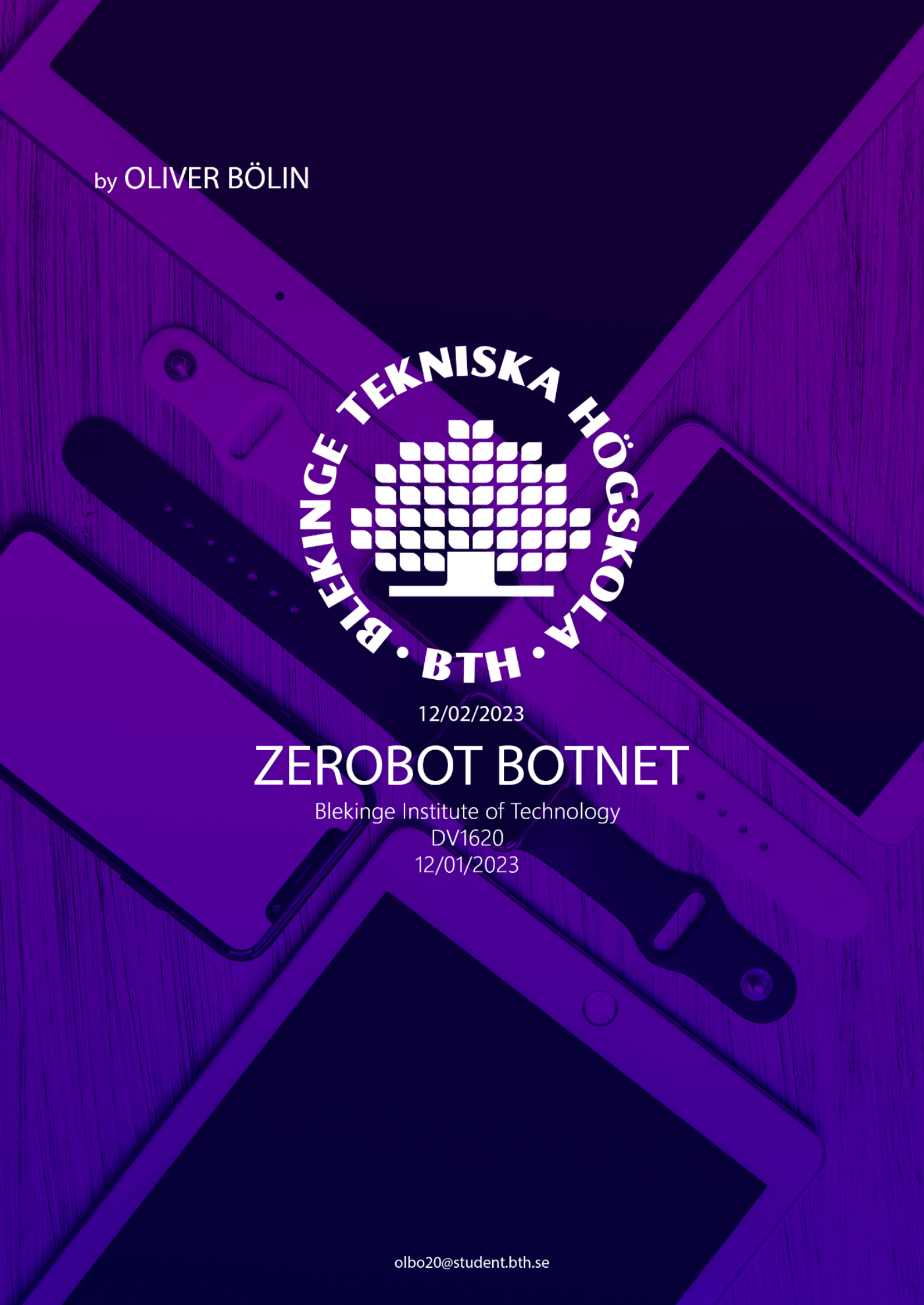
by OLIVER BÖLIN



12/02/2023

ZEROBOT BOTNET

Blekinge Institute of Technology
DV1620
12/01/2023

olbo20@student.bth.se

1. Botnets

A botnet is a collection of Internet-connected devices, each of which is running one or more bots. Bots are typically created by infecting the device with malware, which allows the attacker to control the device remotely. The threat actors can then use the botnet to perform a variety of malicious activities, such as launching distributed denial-of-service (DDoS) attacks, sending spam, or stealing sensitive information. The increased targeting of Internet of Things (IoT) devices by threat actors can be attributed to their lack of robust security measures.

Botnets can be very large, with some containing tens of thousands of infected devices. They are often used for illicit activities and are a major security concern for organisations and individuals. An analysis of recent trends reveals that operators are utilising a diverse range of malware distributions and objectives, as well as modifying existing botnets to increase their operational scale and augment the number of devices within their infrastructure. [1]

2. Zerobot

The Zerobot botnet, a self-perpetuating Go-lang malware primarily spread through IoT and web application vulnerabilities, has been identified as an evolving threat by the Microsoft Defender for IoT research team. The botnet, also referred to as ZeroStresser by Microsoft, is continually updated with new exploits and capabilities.

The Microsoft team has been monitoring Zerobot for several months and has observed multiple updates to the malware. Additionally, in December 2022, a domain associated with Zerobot was among several seized by the FBI in relation to DDoS-for-hire services.[1]

3. Technical Abilities

The latest version of Zerobot now boasts 21 vulnerability attacks, including the ability to exploit vulnerabilities in Apache and Apache Spark (namely CVE-2021-42013 and CVE-2022-33891), as well as newly added DDoS attack capabilities. Zerobot doesn't really stick out from other botnets in the sense that it uses command injection exploits. The unique thing about Zerobots exploit codes that makes it more advanced, is that they have created different commands to download files on the host, and after that kill other malware/botnets present on the host. After that Zerobot uses commands such as *history -c* and deletes the bash_history file to clean up the terminal history. [2]

Table1. Common Vulnerabilities and Exposures that Zerobot uses

CVE	Vulnerability type	Affected software/device
CVE-2014-8361	Improper Input Validation	Software (Realtek SDK), Router (D-Link)
CVE-2016-20017	Command Injection	Router (D-Link)
CVE-2017-17215	Improper Input Validation	Router (Huawei HG532)
CVE-2018-10561/10562	Authentication and Command Injection	Router (Dasan GPON)
-	Command Injection	Router (Sapido RB-1732)
CVE-2020-10987	Command Injection	Router (Tenda AC15 AC1900)
CVE-2020-25506	Command Injection	Router (D-Link DNS-320)
CVE-2020-7209	Command Injection	Software (LinuxKI)
-	Command Injection	Software (PHP 8.1.0-dev)
CVE-2021-35395	Command Injection and Out-of-bounds Write	Software (Realtek Jungle SDK)
CVE-2021-36260	Command Injection	IP camera (Hikvision)
CVE-2021-41773	Path Traversal	Software (Apache HTTP server)
CVE-2021-42013	Path Traversal	Software (Apache HTTP server)
CVE-2021-46422	Command Injection	Router (Telesquare SDT-CW3B1)
CVE-2022-1388	Missing Authentication for Critical Function	Firewall (F5 BIG-IP)
CVE-2022-22965	Command Injection	Software (Spring MVC/Spring WebFlux)
CVE-2022-25075	Command Injection	Router (Totolink A3000RU)
CVE-2022-26186	Command Injection	Router (Totolink N600R)
CVE-2022-26210	Command Injection	Router (Totolink A830R)
CVE-2022-30525	Command Injection	Firewall (Zyxel USG FLEX-series)
CVE-2022-34538	Command Injection	IP camera (Digital Watchdog DW MEGApix)
CVE-2022-37061	Command Injection	Thermal sensor camera (FLIR AX8)

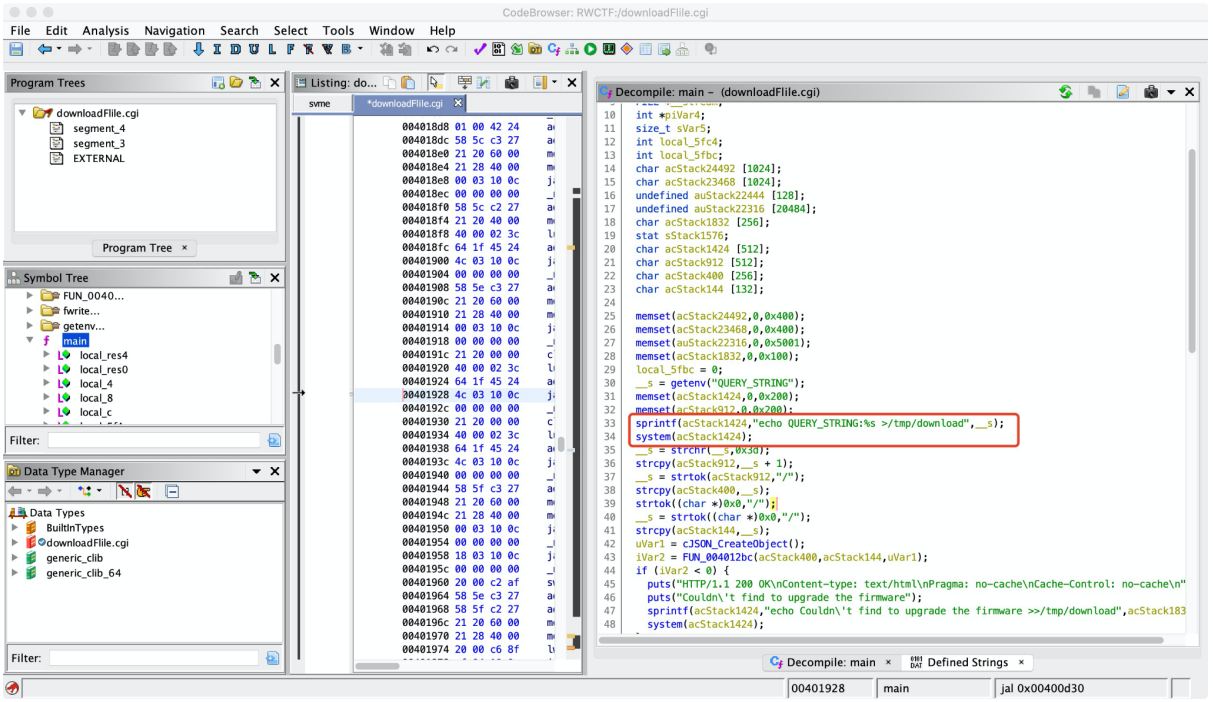
Examples of targeted vulnerabilities

CVE-2021-42013 (Path Traversal)

This vulnerability is used on Apache HTTP server 2.4.49 and 2.4.50, The vulnerability is a path traversal issue that could allow an attacker to access files on the server that are outside of the intended directory structure. By mapping the URLs to the files outside the directories configured by Alias-like directives, this vulnerability would not make the files outside protected by default configurations. Zerobot could be using a CGI script to allow for remote code execution.

CVE-2022-25075 (Command injection)

TOTOLink A3000RU discovered a command injection vulnerability in its “Main” function. This allows Zerobot to execute arbitrary commands by using the QUERY_STRING parameter



When the target becomes a zombie

The botmaster chooses if the Command & Control (C&C) server should make the bot a zombie or continue spreading to other hosts. If it spreads, Zerobot doesn’t only target unpatched devices, it also uses brute-force over SSH and telnet (23 or 2323) for spreading. But if it’s to remain dormant. It waits until a payer gives the botmaster a host to DDoS.

The threat

Adding some weight to the threat, cybercriminals might know if they have infected a host who might be sellable, says Botezatu, director of threat research at BitDefender.
Meaning the botnet can spread and the threat actor can sell off enslaved zombies to the highest bidder. Otherwise turn them into spamming bots to carry out DDoS attacks. The consequences of falling victim to such an attack can be severe, as the botmaster can gain access to sensitive information, steal personal data, and cause financial harm. Moreover, the infected devices can also be used to launch attacks on other systems, which can lead to widespread damage. [3]

The DDOS

The latest version of Zerobot, 1.1, has added seven more DDoS attack techniques by utilizing protocols such as UDP, ICMP, TCP, SYN, ACK, and SYN-ACK, showcasing its constant evolution and swift implementation of new capabilities.

UDP is a connectionless protocol that allows for the transmission of data without the need for establishing a connection beforehand. In a UDP DDoS attack, an attacker will send large amounts of UDP packets to a target, overwhelming its resources and causing it to become unavailable.
ICMP is a network-level protocol that is used for various purposes, such as checking the status of a network or troubleshooting issues. In an ICMP DDoS attack, an attacker will send large numbers of ICMP packets, such as ping requests, to a target, overwhelming its resources and causing it to become unavailable.
TCP is a reliable, connection-oriented protocol that is commonly used for transmitting data over the internet. In a TCP DDoS attack, an attacker will establish many connections to a target, consuming its resources and causing it to become unavailable. [4][5][6]

Previously undisclosed and new capabilities are the following:

Attack method	Description
UDP_RAW	Sends UDP packets where the payload is customizable.
ICMP_FLOOD	Supposed to be an ICMP flood, but the packet is built incorrectly.
TCP_CUSTOM	Sends TCP packets where the payload and flags are fully customizable.
TCP_SYN	Sends SYN packets.
TCP_ACK	Sends ACK packets.
TCP_SYNACK	Sends SYN-ACK packets.
TCP_XMAS	Christmas tree attack (all TCP flags are set). The reset cause field is “xmas”.

4. Countermeasures

The severity of the threat posed by botnets has led to increased efforts by security organisations and governments to monitor and disrupt them. However, the constant evolution of cyber threats means that organisations and individuals must remain vigilant and proactive in defending against them. The best mitigation to reduce the risk of becoming a victim of a zerobot attack, is to keep software and systems up-to-date, and to be mindful of suspicious emails, links, and downloads.

Other mitigation methods include monitoring your network for unusual activities, using SNMP, NetFlow, SFlow, BGP, IPFIX can help detecting if a host has been infected. Using Network intrusion Detection Systems can also help to block traffic if a unusual amount starts to flood out.

5. Sources

1. https://www.microsoft.com/en-us/security/blog/2022/12/21/microsoft-research-uncovers-new-zerobot-capabilities/ 2022-12-21, Microsoft Security
2. https://cujo.com/the-zerobot-botnet-vulnerabilities-targeted-and-exploits-used-in-detail/, 2023-01-03, CUJOAI
3. https://techmonitor.ai/the-age-of-ambient/zerobot-botnet-enterprise-iot, 2023,01-25, TECHMONITOR
4. https://www.akamai.com/glossary/what-is-udp-flood-ddos-attack, unknown date, Akamai
5. https://www.netscout.com/what-is-ddos/icmp-flood, unknown date, Netscout
6. https://www.imperva.com/learn/ddos/syn-flood/, unknown date, imperva