1. Understanding Malware Types

Before jumping into the tools, you need to classify what you are looking for.

Type	Key Characteristic	Behavior
Virus	Requires human action	Attaches to a legitimate file and spreads when executed.
Worm	Self-replicating	Spreads across networks automatically without human intervention.
Trojan	Deceptive	Disguises itself as legitimate software to gain access.
Ransomware	Extortion	Encrypts files and demands payment for the decryption key.

---

2. Using VirusTotal (Static Analysis)

You don't need a live file to practice; you can use **File Hashes** (digital fingerprints).

1. **Find a Hash:** Go to a site like the MalwareBazaar to find a recent MD5 or SHA256 hash.
2. **Upload to VirusTotal:** Paste the hash into the **"Search"** tab.
3. **Analyze Detection:** Look at the "Detection" tab. It shows how many antivirus engines (e.g., Kaspersky, Microsoft, CrowdStrike) flagged it.
4. **Analyze Behavior:** Switch to the **"Behavior"** or **"Relations"** tabs. Note down:
    - **IP Addresses:** What servers is the malware talking to?
    - **Registry Keys:** What settings is it changing to stay hidden?

---

3. The Malware Lifecycle

To fulfill hint #5, remember this general flow:

1. **Delivery:** Email phishing, infected USB, or malicious download.
2. **Execution:** The user clicks the file or a vulnerability is exploited.
3. **Persistence:** The malware ensures it stays active after a reboot (modifying startup folders).
4. **Propagation:** (For worms) Scanning the network for other victims.
5. **Objective:** Stealing data, encrypting files, or spying.

---

4. Prevention Methods

To wrap up your report (Hint #7), include these standard defenses:

- **EDR/Antivirus:** Real-time scanning and behavioral blocking.
- **Network Segmentation:** Keeping infected machines away from critical servers.
- **Patch Management:** Closing the holes that malware uses to get in.
- **User Training:** Teaching people not to click on "Free_Giftcard.exe."

---

5. Deliverable: Malware Classification Report Template

To complete your task, fill out this brief template for one sample you find:

Sample Name/Hash: [Enter Hash Here]

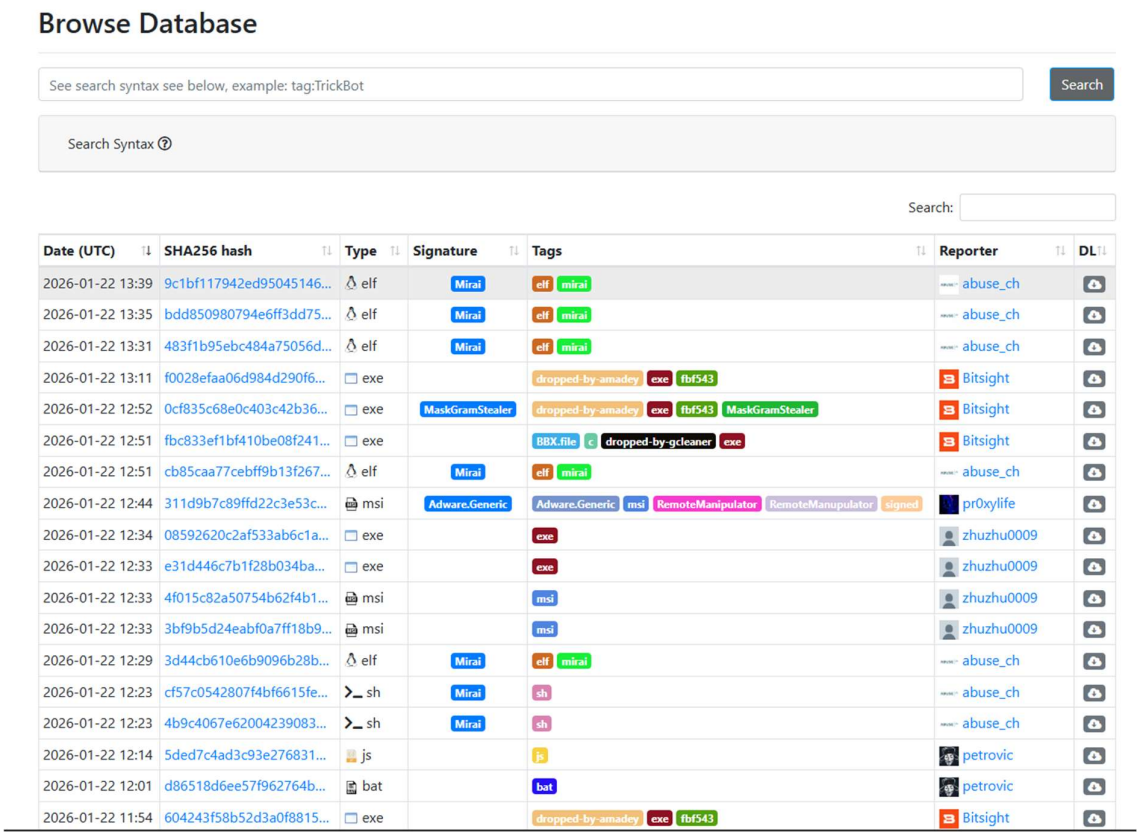
Primary Classification: (e.g., Trojan/Ransomware)

Detection Rate: [X]/90 Engines

Observed Behavior: Modified HKLM\Software\Microsoft\Windows\CurrentVersion\Run for persistence.

Spread Method: Likely via Phishing attachment.

Recommended Prevention: Email filtering and endpoint protection.



Mirai

Vendor detections: **6**

Intelligence 6 | IOCs | YARA 4 | File information | Comments | Actions

SHA256 hash:	9c1bf117942ed950451466f5694e9a6d55757689d95f1303c6a5689b8adec9ec
SHA3-384 hash:	c9bcd320f4c470032da4fc0fb4c0c91800d37aed9e77f8ae0c3c1d4e4ebc19f2867732777ba0bcacefdfb3d2854f09be
SHA1 hash:	e3bb0c1297740c6cff6b4896871d5072a429558a
MD5 hash:	ea8ed3fe40a1c573e32ac1860883967a
humanhash:	gee-batman-floor-triple
File name:	arm6
Download:	download sample
Signature	Mirai Alert
File size:	141'776 bytes
First seen:	2026-01-22 13:39:23 UTC
Last seen:	*Never*
File type:	elf

MIME type:	application/x-executable
ssdeep	3072:7OgCUoKGgaX5AAUrevayMGw3Oouv7oCVpufuTI:7OjfuaXSAGIaARouMApufuT
TLSH	T19CD3F856F8819B11D5C111BAFE1E128E37231B7CE2DE72029D246F747B8A8BB0E3B515
telfhash	t15701b1ea5b7c17f91ac0d244919e653c33c272b91e3538b58c7ba54666414d6b025438
TrID	50.1% (.) ELF Executable and Linkable format (Linux) (4022/12) 49.8% (.O) ELF Executable and Linkable format (generic) (4000/1)
Magika	elf
Reporter	abuse_ch
Tags:	elf mirai

Intelligence

File Origin

# of uploads:	1
# of downloads:	15
Origin country:	DE

Vendor Threat Intelligence

ACCE Mirai_Botnet_XOR_Lookup +

ClamAV +

FileScan.IO Malicious +

Kaspersky OpenTIP Unknown +

Kunai Sandbox +

Intezer Mirai −

Malware family:	Mirai Alert
Verdict:	Malicious
Link:	https://analyze.intezer.com/analyses/2af1f08e-0bfb-4e1c-b692-063ad0bab88a

Joe Sandbox +

Nucleon Malprob Malware +

CERT.PL MWDB +

ReversingLabs TitaniumCloud +

Spamhaus Hash Blocklist Suspicious file +

Hatching Triage mirai +

VirusTotal +

YARA Signatures

MalwareBazaar uses YARA rules from several public and non-public repositories, such as YARAhub and Malpedia. Those are being matched against malware samples uploaded to MalwareBazaar as well as against any suspicious process dumps they may create. Please note that only results from TLP:CLEAR rules are being displayed.

Rule name:	ELF_Mirai Alert
Author:	NDA0E
Description:	Detects multiple Mirai variants

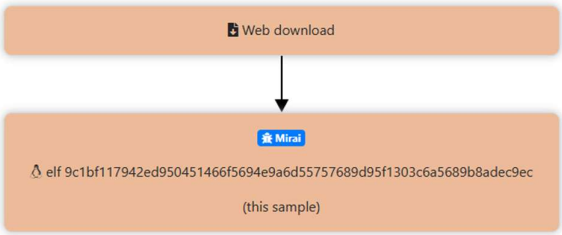
Rule name:	ELF_Toriilike_persist Alert
Author:	4r4
Description:	Detects Torii IoT Botnet (stealthier Mirai alternative)
Reference:	Identified via researched data

Rule name:	Mal_LNX_Mirai_Botnet_ELF Alert
Author:	Phatcharadol Thangplub
Description:	Use to detect Mirai botnet, and there variants.

Rule name:	unixredflags3 Alert
Author:	Tim Brown @timb_machine
Description:	Hunts for UNIX red flags

File information

The table below shows additional information about this malware sample such as delivery method and external references.



	URLhaus	https://urlhaus.abuse.ch/url/3760872/
	Delivery method	Distributed via web download