## Malware

Malware (malicious software) includes various programs designed to disrupt, damage, or gain unauthorized access to computer systems, commonly categorized into ransomware, viruses, worms, Trojans, spyware, and adware. Key threats include data theft, system disruption, and financial extortion, often spread via phishing or malicious websites.

## Types of Malware

| Malware Type | Description |
|---|---|
| **Ransomware** | Encrypts data and demands payment for decryption. |
| **Virus** | Replicates by attaching to legitimate programs. |
| **Worm** | Self-replicates and spreads across networks without human help. |
| **Trojan Horse** | Disguises itself as legitimate software to steal data. |
| **Spyware** | Secretly monitors user activity and collects information. |
| **Adware** | Displays unwanted, often malicious, advertisements. |
| **Rootkit** | Provides unauthorized, hidden access to a system. |
| **Botnet** | A network of infected devices controlled by a bot herder. |
| **Keylogger** | Records keystrokes to steal passwords and sensitive data. |
| **Fileless Malware** | Operates in memory, leaving no files for traditional antivirus to scan. |
| **Cryptojacking** | Uses device resources to mine cryptocurrency without consent. |

## Upload known malware samples (hashes) to VirusTotal

### 1. Hash Lookup and Initial Detection

Instead of uploading a physical file (which can be risky or unnecessary if the sample is already known), you search for its **SHA-256, SHA-1, or MD5 hash**.

- **Detection Tab:** This gives you the "verdict." Look for the ratio (e.g., 50/72). If top-tier engines like Kaspersky, CrowdStrike, or Microsoft flag it, you’re dealing with a confirmed threat.
- **Malware Naming:** Pay attention to the labels (e.g., Win32/Emotet.C). Different vendors use different naming conventions, but the core family name usually remains consistent.

## 2. Deep Dive: Behavior and Lifecycle

The **Behavior** and **Details** tabs are where the real learning happens regarding how malware operates.

- **Registry Keys & File System:** Look for "Files Created" or "Registry Keys Set." Malware often modifies these to ensure **persistence** (staying active after a reboot).
- **Network Communications:** Check for contacted IP addresses or domains. This shows the **Command and Control (C2)** phase where the malware checks in with the attacker for instructions.
- **Process Tree:** Observe which processes are spawned. Many samples will "hollow out" a legitimate process (like explorer.exe) to hide their activity.

## 3. Understanding the Spreading Mechanism

By looking at the "Bundled Files" or "Dropped Files" in the report, you can infer how it spreads:

- **Droppers:** Small files designed solely to download the "heavy" payload.
- **Worm-like behavior:** If the behavior report shows scans for local network vulnerabilities (SMB/Port 445), it's designed to spread laterally across a network.

**4. Prevention and Mitigation**

**Based on the indicators of compromise (IoCs) found in the report, you can identify how to stop it:**

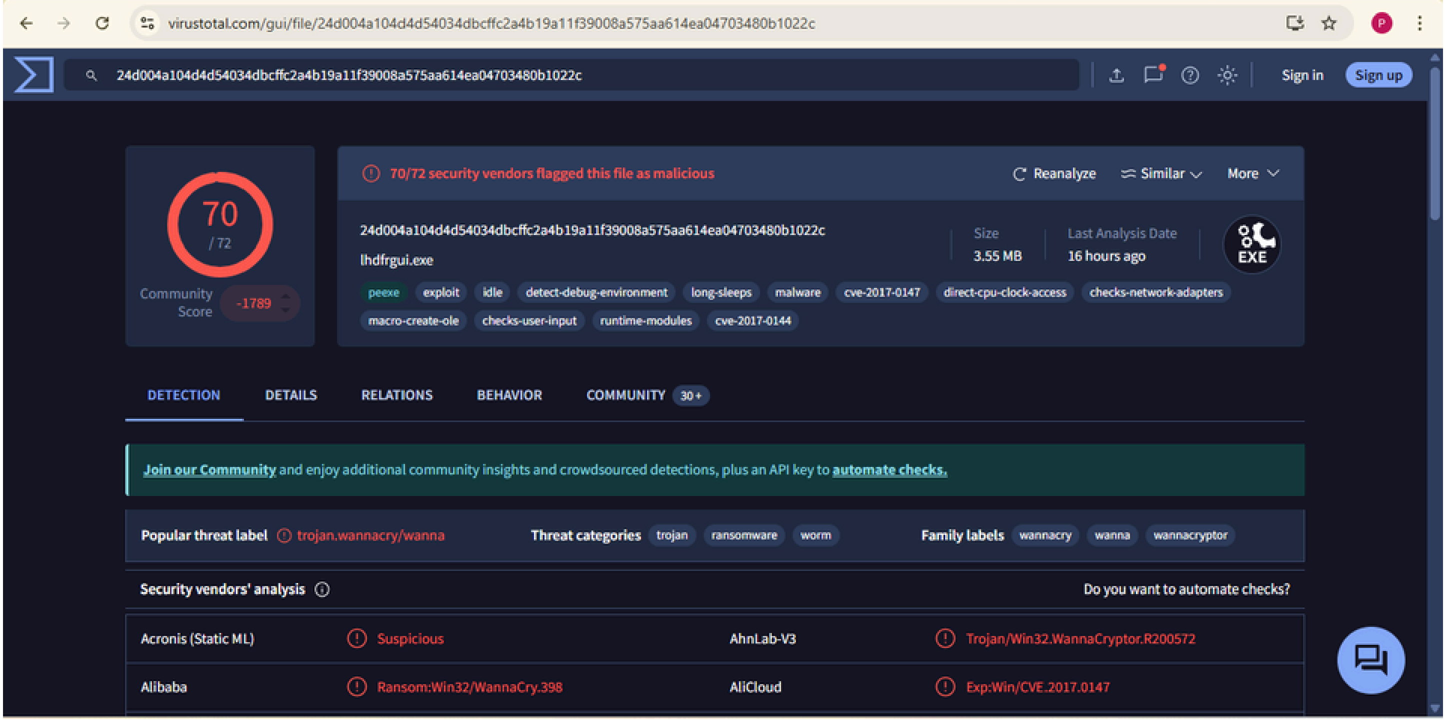
| Phase | Prevention Method |
|---|---|
| Initial Access | Email filtering (SPF/DKIM/DMARC) and User Training. |
| Execution | Endpoint Detection & Response (EDR) and disabling Macros. |
| Persistence | Hardening OS configurations and monitoring "Run" registry keys. |
| Exfiltration | Firewall rules blocking known malicious IPs/C2 domains. |

## 1. The Sample (Hash Lookup)

Instead of searching for a dangerous file, we will use its SHA-256 hash:

**24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c**

If you paste this into the VirusTotal search bar, you'll see a detection rate of nearly 100% (66/72+ engines).



virustotal.com/gui/file/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

70/72 security vendors flagged this file as malicious

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
lhdfrgui.exe

Size 3.55 MB
Last Analysis Date 16 hours ago

peexe exploit idle detect-debug-environment long-sleeps malware cve-2017-0147 direct-cpu-clock-access checks-network-adapters macro-create-ole checks-user-input runtime-modules cve-2017-0144

Community Score -1789

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.wannacry/wanna
Threat categories trojan ransomware worm
Family labels wannacry wanna wannacryptor

Security vendors' analysis

Do you want to automate checks?

| | | | |
|---|---|---|---|
| Acronis (Static ML) | Suspicious | AhnLab-V3 | Trojan/Win32.WannaCryptor.R200572 |
| Alibaba | Ransom:Win32/WannaCry.398 | AliCloud | Exp:Win/CVE.2017.0147 |

## 2. Analyze Detection Reports

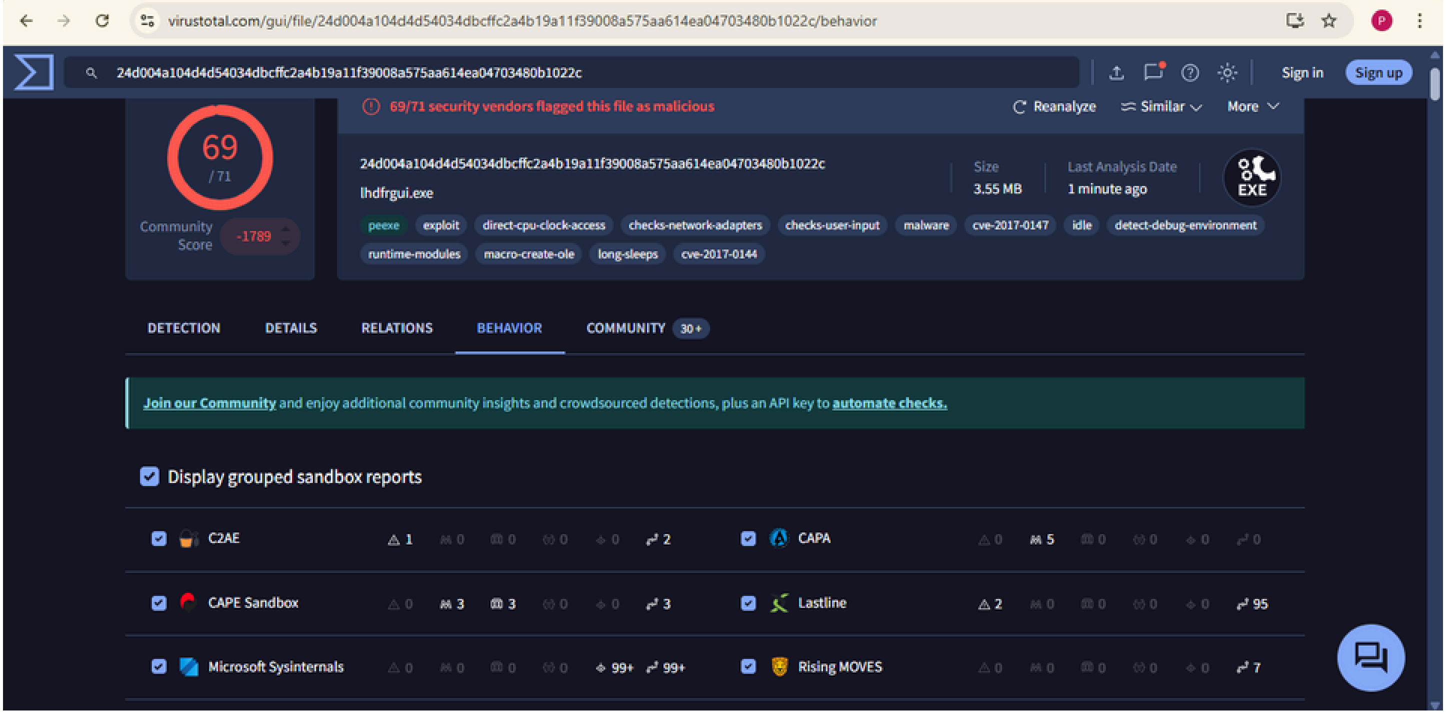
- **Verdict:** Almost every vendor labels it as Ransom:Win32/WannaCrypt or Trojan.WCRY.

- **Popular Threat Label:** This tells you the specific family. In a real-world scenario, knowing it's "WannaCry" tells you immediately that it exploits the SMB protocol.

### 3. Observe Behavior Indicators

Under the Behavior tab, you will see a list of "sandboxed" actions. Key indicators for WannaCry include:

- **Registry Modifications:** It creates keys in \CurrentVersion\Run to ensure it starts every time the computer boots (Persistence).
- **Shell Commands:** You'll see it running vssadmin.exe delete shadows /all /quiet.
  - *Why?* It is deleting "Shadow Copies" (Windows' built-in backups) so the victim cannot easily restore their files.
- **DNS Requests:** It tries to contact a very long, gibberish domain (the famous "Kill Switch" domain).



virustotal.com/gui/file/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c/behavior

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

69/71 security vendors flagged this file as malicious

69 / 71

Community Score -1789

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
lhdfrgui.exe

Size 3.55 MB

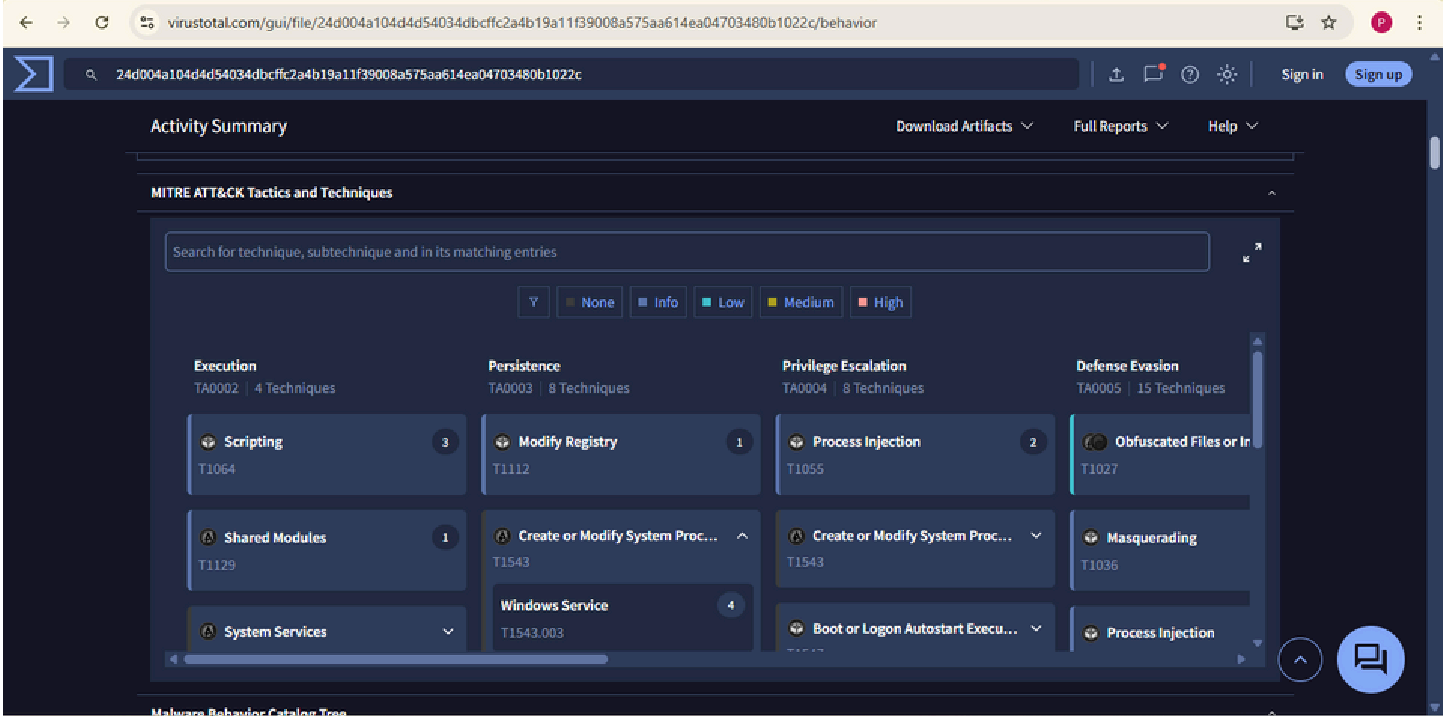
Last Analysis Date 1 minute ago

peexe exploit direct-cpu-clock-access checks-network-adapters checks-user-input malware cve-2017-0147 idle detect-debug-environment runtime-modules macro-create-ole long-sleeps cve-2017-0144

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

☑ Display grouped sandbox reports

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ C2AE | 1 | 0 | 0 | 0 | 0 | 2 | ☑ CAPA | 0 | 5 | 0 | 0 | 0 | 0 |
| ☑ CAPE Sandbox | 0 | 3 | 3 | 0 | 0 | 3 | ☑ Lastline | 2 | 0 | 0 | 0 | 0 | 95 |
| ☑ Microsoft Sysinternals | 0 | 0 | 0 | 0 | 99+ | 99+ | ☑ Rising MOVES | 0 | 0 | 0 | 0 | 0 | 7 |


virustotal.com/gui/file/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c/behavior
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Sign in
Sign up
Activity Summary
Download Artifacts
Full Reports
Help
Search for technique, subtechnique and in its matching entries
None
Info
Low
Medium
High

MITRE ATT&CK Tactics and Techniques

Execution
TA0002 | 4 Techniques
- Scripting 3 T1064
- Shared Modules 1 T1129
- System Services

Persistence
TA0003 | 8 Techniques
- Modify Registry 1 T1112
- Create or Modify System Proc... T1543
  - Windows Service 4 T1543.003

Privilege Escalation
TA0004 | 8 Techniques
- Process Injection 2 T1055
- Create or Modify System Proc... T1543
- Boot or Logon Autostart Execu...

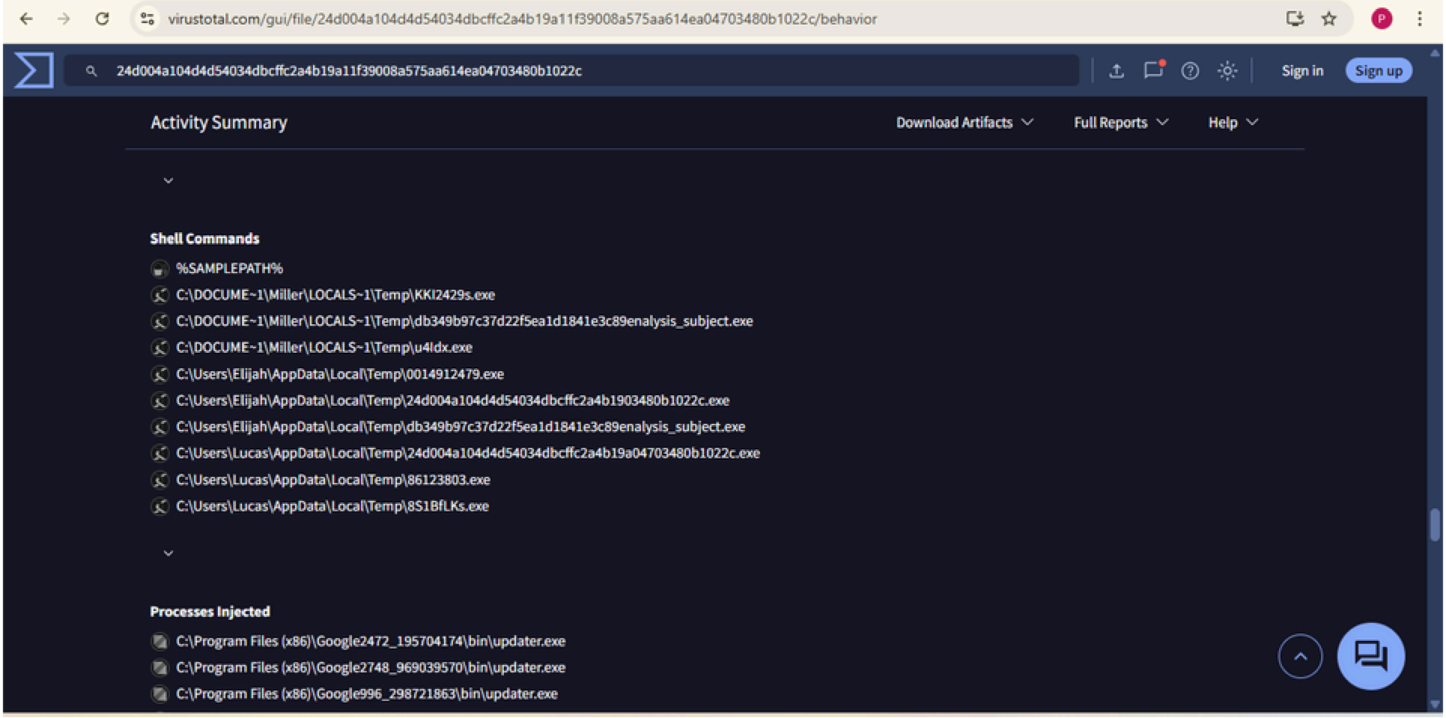
Defense Evasion
TA0005 | 15 Techniques
- Obfuscated Files or In T1027
- Masquerading T1036
- Process Injection

Malware Behavior Catalog Tree

## 4. Understand Malware Lifecycle

The WannaCry lifecycle follows a distinct path:

1. **Infection:** It enters via the EternalBlue exploit (MS17-010).
2. **Persistence:** It copies itself to the system folder and sets a registry key.
3. **Preparation:** It checks for a "Kill Switch" domain; if the domain is *not* registered, it proceeds.
4. **Execution:** It starts encrypting files and deleting backups.
5. **Extortion:** It drops a @WanaDecryptor@.exe file to show the ransom note.

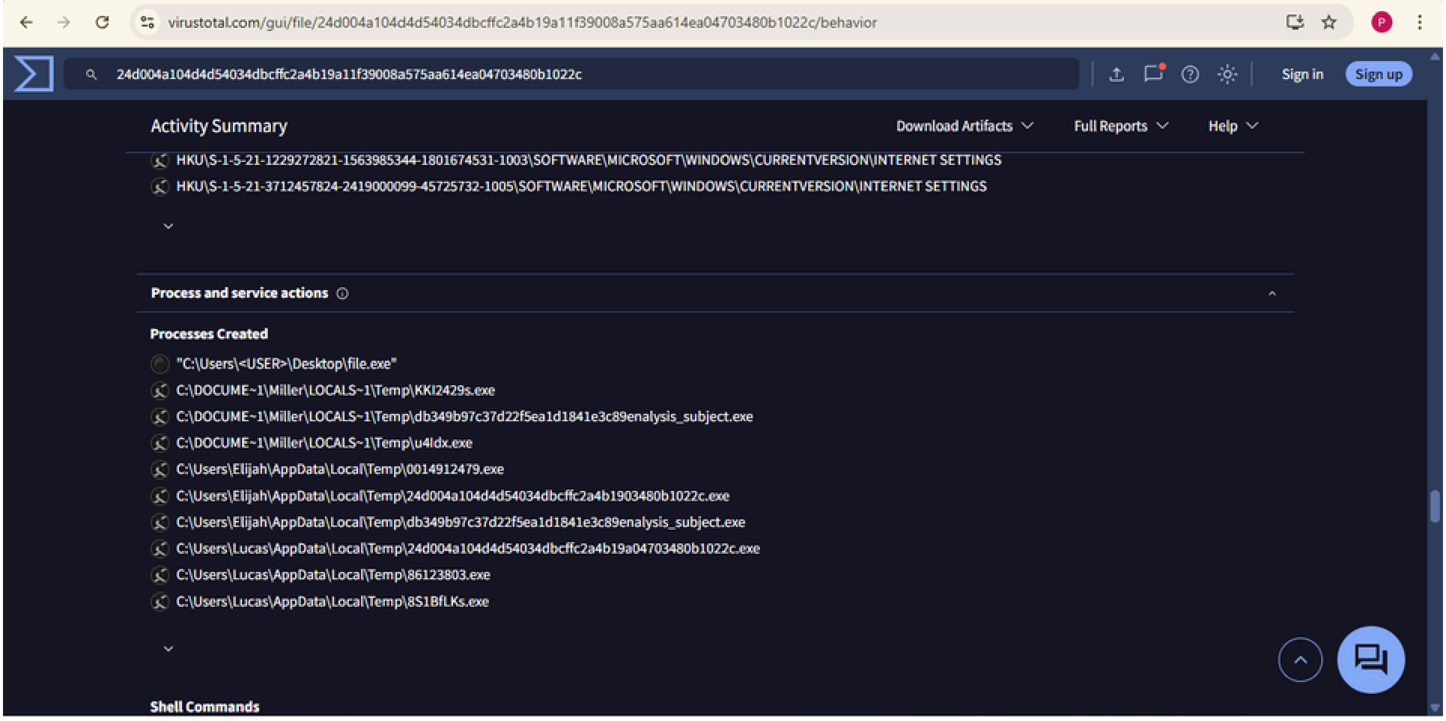

virustotal.com/gui/file/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c/behavior
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Sign in
Sign up
Activity Summary
Download Artifacts
Full Reports
Help

Shell Commands

```
%SAMPLEPATH%
C:\DOCUME~1\Miller\LOCALS~1\Temp\KKI2429s.exe
C:\DOCUME~1\Miller\LOCALS~1\Temp\db349b97c37d22f5ea1d1841e3c89enalysis_subject.exe
C:\DOCUME~1\Miller\LOCALS~1\Temp\u4ldx.exe
C:\Users\Elijah\AppData\Local\Temp\0014912479.exe
C:\Users\Elijah\AppData\Local\Temp\24d004a104d4d54034dbcffc2a4b1903480b1022c.exe
C:\Users\Elijah\AppData\Local\Temp\db349b97c37d22f5ea1d1841e3c89enalysis_subject.exe
C:\Users\Lucas\AppData\Local\Temp\24d004a104d4d54034dbcffc2a4b19a04703480b1022c.exe
C:\Users\Lucas\AppData\Local\Temp\86123803.exe
C:\Users\Lucas\AppData\Local\Temp\8S1BfLKs.exe
```

Processes Injected

```
C:\Program Files (x86)\Google2472_195704174\bin\updater.exe
C:\Program Files (x86)\Google2748_969039570\bin\updater.exe
C:\Program Files (x86)\Google996_298721863\bin\updater.exe
```



virustotal.com/gui/file/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c/behavior
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Sign in
Sign up
Activity Summary
Download Artifacts
Full Reports
Help

```
HKU\S-1-5-21-1229272821-1563985344-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
HKU\S-1-5-21-3712457824-2419000099-45725732-1005\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
```

**Process and service actions**

**Processes Created**

```
"C:\Users\<USER>\Desktop\file.exe"
C:\DOCUME~1\Miller\LOCALS~1\Temp\KKI2429s.exe
C:\DOCUME~1\Miller\LOCALS~1\Temp\db349b97c37d22f5ea1d1841e3c89enalysis_subject.exe
C:\DOCUME~1\Miller\LOCALS~1\Temp\u4ldx.exe
C:\Users\Elijah\AppData\Local\Temp\0014912479.exe
C:\Users\Elijah\AppData\Local\Temp\24d004a104d4d54034dbcffc2a4b1903480b1022c.exe
C:\Users\Elijah\AppData\Local\Temp\db349b97c37d22f5ea1d1841e3c89enalysis_subject.exe
C:\Users\Lucas\AppData\Local\Temp\24d004a104d4d54034dbcffc2a4b19a04703480b1022c.exe
C:\Users\Lucas\AppData\Local\Temp\86123803.exe
C:\Users\Lucas\AppData\Local\Temp\8S1BfLKs.exe
```

**Shell Commands**

## 5. How Malware Spreads

WannaCry is a Worm. Unlike a standard virus that needs you to click an email attachment, a worm spreads automatically.

- It scans the local network for other computers with Port 445 (SMB) open.
- Once it finds a vulnerable machine, it "jumps" to it and starts the cycle again.

## 6. Identify Prevention Methods

Based on these findings, we can build a defense:

- **Patch Management:** Install the MS17-010 security update.
- **Network Hardening:** Disable SMBv1 (an outdated, insecure protocol).
- **Segmentation:** Block Port 445 at the network perimeter so the worm can't enter from the internet.

## 7. Findings

**Sample:** WannaCry Ransomware Detection: Critical (Confimred by 60+ engines).

**Primary Impact:** File encryption and deletion of system backups. Spread Method: Automated worm-like propagation via SMB vulnerability (EternalBlue). Key IoCs: File extensions changed to .WNCRY, presence of tasksche.exe, and attempts to delete shadow copies.