Rhysida using Oyster Backdoor to deliver ransomware

threatdown.com/blog/rhysida-using-oyster-backdoor-to-deliver-ransomware/

Business, Threats

In a recent attack, Rhysida used a new variant of the Oyster backdoor, also known as Broomstick.

July 24, 2024

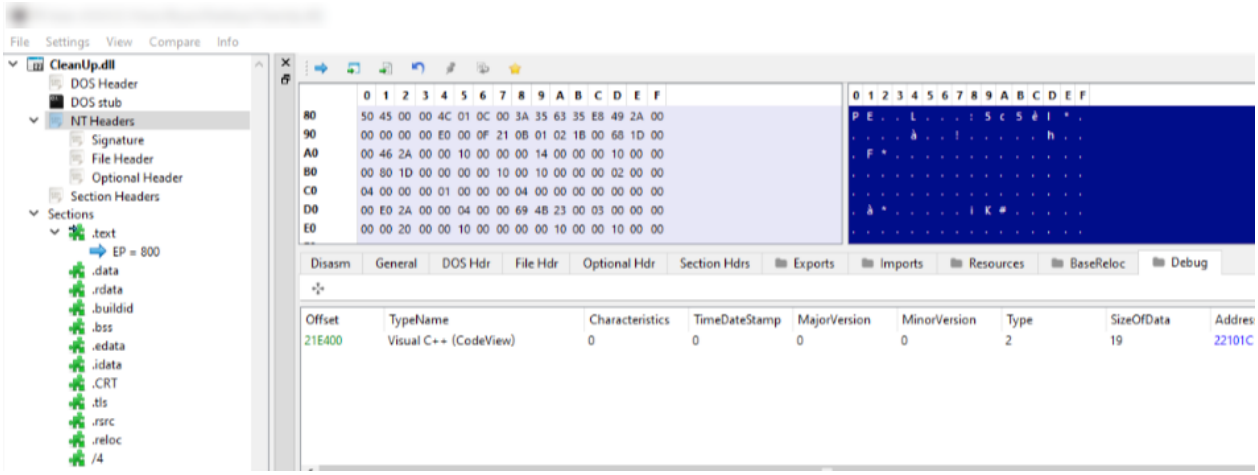
Bill Cozens

On July 10, 2024, a prominent private school was struck by the Rhysida ransomware gang.

As part of the attack, Rhysida used a new variant of the Oyster backdoor, also known as Broomstick. This is an updated version of a new Oyster campaign first discovered by Rapid7 in late June 2024 that uses SEO-poisoned search results to trick users into downloading malicious installers. These installers masquerade as legitimate software, such as Google Chrome and Microsoft Teams, but instead drop the Oyster backdoor.

Let's dive more into the incident and how Rhysida used Oyster as part of its attack.

Technical details and tactics

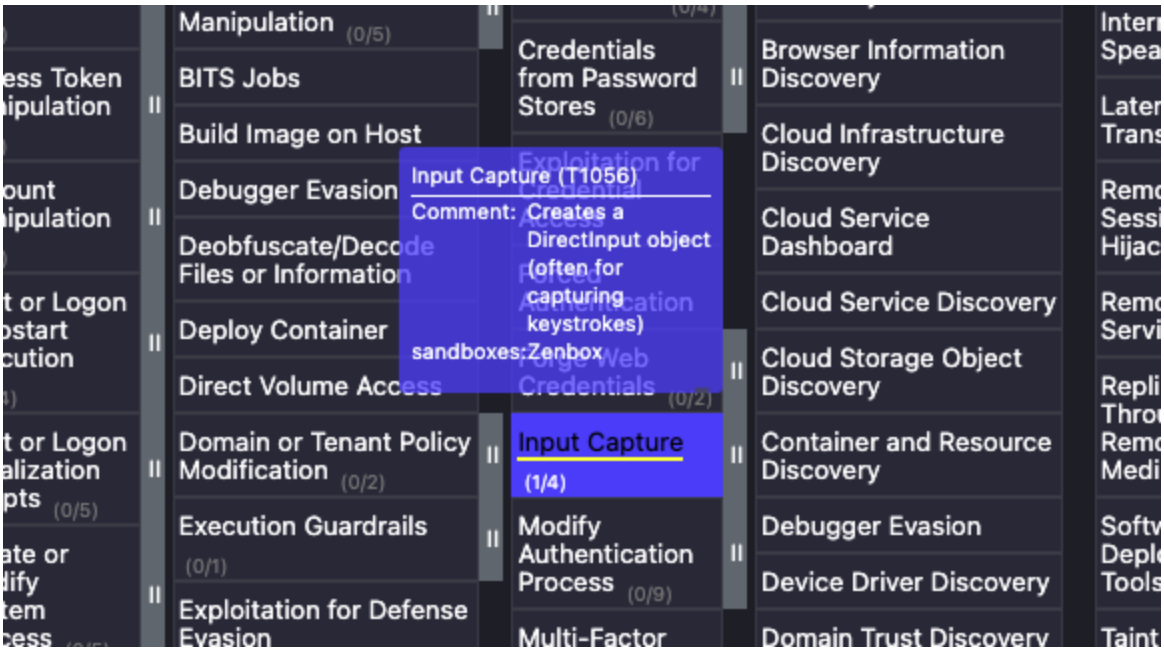


Raw data contents of CleanUp.dll

On July 10, an Oyster backdoor was deployed on a customer endpoint, likely originating from a malicious IP scanner distributed via malvertising. The malicious DLL associated with this attack communicates with `codeforprofessionalusers[.]com`, which ThreatDown researchers identified as an Oyster command and control (C2) server.

One of the notable tactics, techniques, and procedures (TTPs) observed includes input capture (T1056), which enabled the theft of administrative credentials to the clients' hypervisors. The specific malware tasks and malicious directories identified in this incident, which have since been added to ThreatDown detections, include:

- **Task:** `{59B44DEF-E91D-491A-97D8-1F48D6A5F961}` – System32\Tasks\OppCleanTp executing `CleanUp.dll`
- **Malicious directories and files:**
  - `C:\Users\[REDACTED]\AppData\Roaming\IwJnK`
  - `C:\Users\[REDACTED]\AppData\Roaming\ZBrAO`
  - `C:\WINDOWS\system32\Tasks\OppCleanTp`
  - `C:\Users\[REDACTED]\AppData\Local\Temp\CleanUp.dll`



Input capture (T1056) is among the DLL's TTPs

Using stolen SSH credentials, attackers accessed NAS devices and VMware hypervisors—thus bypassing ThreatDown Endpoint Protections' (EP) real-time protection layer—before deploying Rhysida ransomware. Because the customer relied solely on EP instead of EDR or MDR, they could also not see any suspicious activity alerts generated from this event.

This ransomware encrypted VMDK files on the hypervisor and potentially other critical data on the NAS devices. The attackers also encrypted local backups, necessitating the use of offsite backups for recovery.

Indicators of Compromise (IoCs)

VirusTotal link:
https://www.virustotal.com/gui/file/0a7fd836d36ed8e8e9aa7bc41fdc9242333e8469059dec8886b7d935f3651679/behavior

- **File Hashes:**
  SHA-256:
  `0a7fd836d36ed8e8e9aa7bc41fdc9242333e8469059dec8886b7d935f3651679`
- **Domains:**
  `codeforprofessionalusers.com`
- **IP Addresses:**
  `173.46.80[.]206`

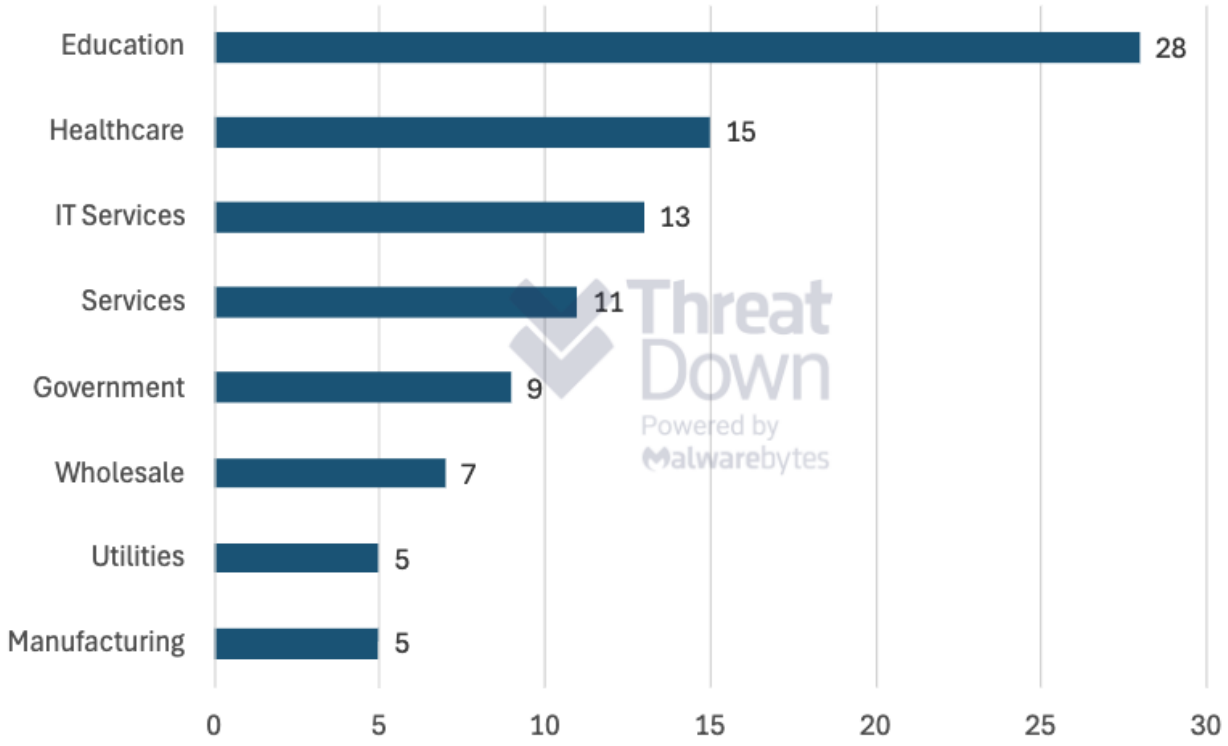
- **Files and Directories:**
  - `C:\Users\[REDACTED]\AppData\Roaming\IwJnK`
  - `C:\Users\[REDACTED]\AppData\Roaming\ZBrAO`
  - `C:\WINDOWS\system32\Tasks\OppCleanTp`
  - `C:\Users\[REDACTED]\AppData\Local\Temp\CleanUp.dll`

The infected endpoints exhibited numerous outbound web connections to known Rhysida C2 servers, including `173.46.80[.]206`.

How to prevent Rhysida ransomware

Rhysida has made a big name for itself in a short amount of time, with over 107 confirmed attacks since it emerged on the scene in June 2023.

While it looks like Rhysida will attack anyone it thinks is an easy target, it has a disproportionate interest in the education sector, which accounts for about 30% of its victims —about ten times the average for most ransomware groups.



Known Rhysida ransomware attacks by industry, June 2023 – June 2024

We recommend the organizations across all sectors follow a few best practices to prevent (and recover) from ransomware attacks from every angle. That includes:

- **Don’t get attacked twice**. Once you’ve isolated the outbreak and stopped the first attack, you must remove every trace of the attackers, their malware, their tools, and their methods of entry, to avoid being attacked again.

- **Block common forms of entry**. Create a plan for patching vulnerabilities in internet-facing systems quickly; disable or harden remote access like RDP and VPNs; use endpoint security software that can detect exploits and malware used to deliver ransomware.
- **Detect intrusions**. Make it harder for intruders to operate inside your organization by segmenting networks and assigning access rights prudently. Use EDR or MDR to detect unusual activity before an attack occurs.
- **Create offsite, offline backups**. Keep backups offsite and offline, beyond the reach of attackers. Test them regularly to make sure you can restore essential business functions swiftly.

Purpose-built for organizations with small (to non-existent) security teams that lack the resources to address all security alerts, the ThreatDown Elite Bundle includes award-winning technologies and 24x7x365 expert-managed monitoring and response from the ThreatDown MDR team.

Talk to an MDR expert today.

business mdr edr ransomware