

Ransomware Spotlight: Water Ouroboros | Trend Micro (GB)

Archived: 2026-04-05 13:35:47 UTC

Technical Details

The ransomware accepts the following arguments:

| Argument | Details |
|-------------------------------------|---|
| c {username}:{password} | A required argument that specifies the username and password to access the contact page |
| -a, -attach, --attach | Enables logging |
| -A, -no-aggressive, --no-aggressive | Disables the deletion of backups and recovery |
| -E, -no-extension, --no-extension | Disables appending of extension to files |
| -m, -min-size, --min-size | Specifies the minimum file size for encryption (in bytes) |
| {File or Path to encrypt} | Encrypts a specific file or directory |

Table 1. The arguments accepted by the Water Ouroboros ransomware

It encrypts fixed, removable, and network drives. It also executes the following commands:

- wmic.exe shadowcopy delete
- bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
- wbadmin.exe delete systemstatebackup -keepVersions:3
- wbadmin.exe delete systemstatebackup
- bcdedit.exe /set {default} recoveryenabled No
- vssadmin.exe delete shadows /all /quiet
- wbadmin.exe delete catalog-quiet
- notepad.exe {Drive}:\Contact Us.txt

During encryption, Water Ouroboros appends the following extension to the file name of the encrypted files:

- {original filename}.{original extension}.locked

The ransomware contains a list of strings or extensions to determine which files to avoid for encryption:

- 386
- adv
- ani
- bat
- bin
- cab
- cmd
- com
- cpl
- cur
- deskthemepack
- diagcab
- diagcfg
- diagpkg
- dll

- drv
- exe
- hlp
- hta
- icl
- icns
- ico
- ics
- idx
- key
- ldf
- lnk
- lock
- mod
- mpa
- msc
- msi
- msp
- msstyles
- msu
- nls
- nomedia
- ocx
- pdb
- prf
- ps1
- rom
- rtp
- scr
- shs
- spl
- sys
- theme
- themepack
- wpxF

Certain variants avoid encrypting files with the specified strings or extensions in their file path.

The following are the ransom notes dropped during infection:

- {Encrypted Directory}\Contact Us.txt
- {Drive}:\Contact Us.txt

Figure 1. The Water Ouroboros ransom note

During the encryption routine, it generates and exports the encryption keys and generates the ransom note. It directs the victim to a password-protected Onion domain (TOR website):

- [https://hivecust6vhekztbqgdnkks64ucehqacge3dij3gyrrdp57zoq3ooqdf.\[.\]onion/](https://hivecust6vhekztbqgdnkks64ucehqacge3dij3gyrrdp57zoq3ooqdf.[.]onion/)

It also warns the victim of the impending disclosure of their stolen data on the Hive Leaks site:

- <https://hiveleakdbtmp76ulyhi52eag6c6tyc.onion/>

From the function *App_ExportKey()*, it uses standard Go crypto functions to generate RSA keys. A key file is then exported.

It generates a random key for the encryption process using the *RTLGenRandom* API, which is initially saved in memory. This key is then used to encrypt the files via a custom encryption implementation.

The key is subsequently encrypted via GoLang's implementation of RSA, using a list of public keys embedded in the binary. The encrypted key is then saved as .key on the encrypted drive.

Finally, the generated key is wiped from memory, ensuring that the encrypted key is the only copy available for decryption.

Infection chain and techniques

Initial Access

- Water Ouroboros exploits public-facing Oracle WebLogic application using known vulnerabilities (CVE-2019-2725, CVE-2017-10271, CVE-2019-2729).
- It comes bundled in a software installer package (Drive-by Compromise).

Execution

- Water Ouroboros performs remote command execution on the compromised server.
- It downloads and executes crack software and key generators on multiple endpoints.

Persistence

- Water Ouroboros uses a compromised admin account to maintain access to the target's machine.
- It disables security services by modifying the registry.

Privilege

- Water Ouroboros employs credential dumping via registry hives to access sensitive OS credentials.

Lateral Movement

- Water Ouroboros uses Remote Desktop Protocol (RDP) and Server Message Block (SMB) to access other systems within the network.

Discovery

- Water Ouroboros discovers networks and accounts using tools like AdFind.
- It performs credential discovery via PassView or Registry Hive Dumping.

Exfiltration

- Water Ouroboros transfers files over the C&C channel to external IP addresses.
- It uses storage software tools for exfiltration.

Defense Evasion

- Water Ouroboros disables security tools and services.
- PCHunter and ProcessHacker are disabled via a valid account RDP or Remote Access Tools (RATs).

Credential Dumping

- Water Ouroboros dumps credentials using HackTool PassView or Registry Hive.

Collection

- Water Ouroboros transfers malicious tools and scripts to compromised systems.

Command and Control

- Water Ouroboros communicates with C&C servers using web protocols.
- It uses the SharpRhino RAT.

Impact

- Water Ouroboros encrypts data.
- It drops ransom notes to notify the user of file encryption and potential data leaks.
- It inhibits system recovery by deleting volume shadow copies and disabling recovery measures.

MITRE tactics and techniques

| Initial Access | Execution | Defense Evasion | Credential Access | Discovery | Lateral Movement | Exfiltration | Command and Control | Impact |
|--|---|--|---|--|---|---|---|---|
| <p>T1190 - Exploit Public-Facing Application</p> <p><i>Water Ouroboros exploits Oracle Weblogic Remote Command Execution resulting in outbound network traffic to a remote host.</i></p> <p>T1189 - Drive-by Compromise User</p> <p><i>downloads cracked software, indicating potential malware infection through untrusted sources.</i></p> <p>T1078 - Valid Accounts</p> <p><i>Water Ouroboros maintains malicious activity using a</i></p> | <p>T1059.003</p> <p><i>- Command and Scripting Interpreter: Windows Command Shell</i></p> <p><i>Water Ouroboros employs the command line to execute and decompress an archive file containing a ransomware binary.</i></p> | <p>T1562.001</p> <p><i>- Impair Defenses: Disable or Modify Tools</i></p> <p><i>Water Ouroboros modifies the registry to disable the Qualys agent security service.</i></p> | <p>T1003.002</p> <p><i>- OS Credential Dumping: Security Account Manager (SAM)</i></p> <p><i>Water Ouroboros performs credential dumping via the Registry hive using the reg command to save the SAM database.</i></p> | <p>T1595.002 - Active Scanning: Vulnerability Scanning</p> <p><i>Water Ouroboros conducts vulnerability scanning from specific IP addresses, indicating preparation for exploitation.</i></p> <p>T1087 - Account Discovery</p> <p><i>Water Ouroboros used AdFind tool to perform account, remote system, and group discovery.</i></p> <p>T1018 - Remote System Discovery</p> <p><i>Water Ouroboros continues using AdFind to discover other computers on the network.</i></p> | <p>T1021.001 - Remote Services: Remote Desktop Protocol</p> <p><i>Water Ouroboros uses RDP for remote access and lateral movement.</i></p> <p>T1021.002 - Remote Services: SMB/Windows Admin Shares</p> <p><i>Water Ouroboros uses SMB to transfer files or remotely access systems, indicating lateral movement.</i></p> | <p>T1041 - Exfiltration Over Command and Control Channel</p> <p><i>Water Ouroboros performs suspected data exfiltration over an outbound SMB connection.</i></p> | <p>T1105 - Ingress Tool Transfer</p> <p><i>Water Ouroboros transfers and uses scripts and discovery tools on the compromised system.</i></p> <p>T1071.001 - Application Layer Protocol: Web</p> <p><i>Water Ouroboros employs HTTP/HTTPS protocols to make requests to various C&C servers.</i></p> | <p>T14 - Encrypted Impact</p> <p><i>The per execrans binar on th</i></p> <p>T14 - Inhibit Recovery</p> <p><i>Water Our dele sha and boot reco mea hind reco</i></p> <p>T11 - Service to server potential evade detection</p> |

| Initial Access | Execution | Defense Evasion | Credential Access | Discovery | Lateral Movement | Exfiltration | Command and Control | Imp |
|-----------------------------|-----------|-----------------|-------------------|--|------------------|--------------|---------------------|-----|
| <i>compromised account.</i> | | | | T1069.002 - Permission Groups Discovery: Domain Trusts <i>Water Ouroboros further uses AdFind to enumerate domain trusts and organizational units.</i> | | | | |

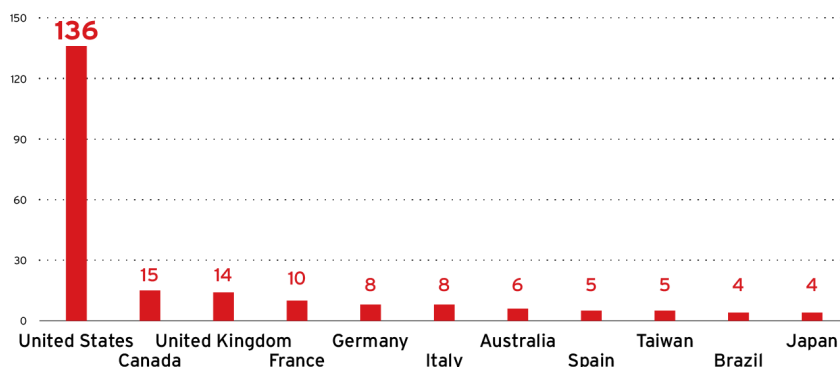
Summary of malware, tools, and exploits used

Security teams can look for the presence of the following tools and exploits that are typically used in Water Ouroboros attacks:

| ATTACK TOOL | MITRE TTP |
|------------------|----------------------------|
| SharpRhino | |
| Storage Software | Exfiltration |
| PCHunter | Discovery, Defense Evasion |
| ProcessHacker | Discovery, Defense Evasion |
| AdFind | Lateral Movement |

Top affected countries, industries, and business sizes

The US bore the overwhelming impact of Water Ouroboros attacks, experiencing nearly ten times as many incidents (136) as the next most-targeted country, Canada. The UK, France, Germany, and Italy also ranked among the group's primary targets.



©2025 TREND MICRO [open on a new tab](#)

Figure 6. The distribution of countries (top 10) targeted by the Water Ouroboros Sources: Water Ouroboros leak site data and Trend open-source intelligence (OSINT) research (Oct. 2023- Feb. 2025)

Companies in the construction, IT, manufacturing, and healthcare industries experienced the highest number of attacks. However, Water Ouroboros targeted a wide range of sectors, demonstrating a broad and diverse attack strategy.

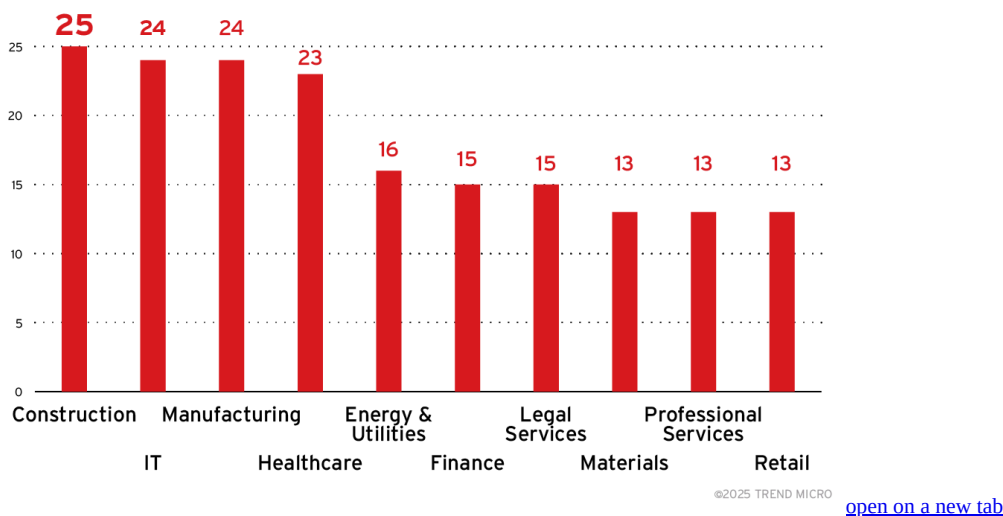
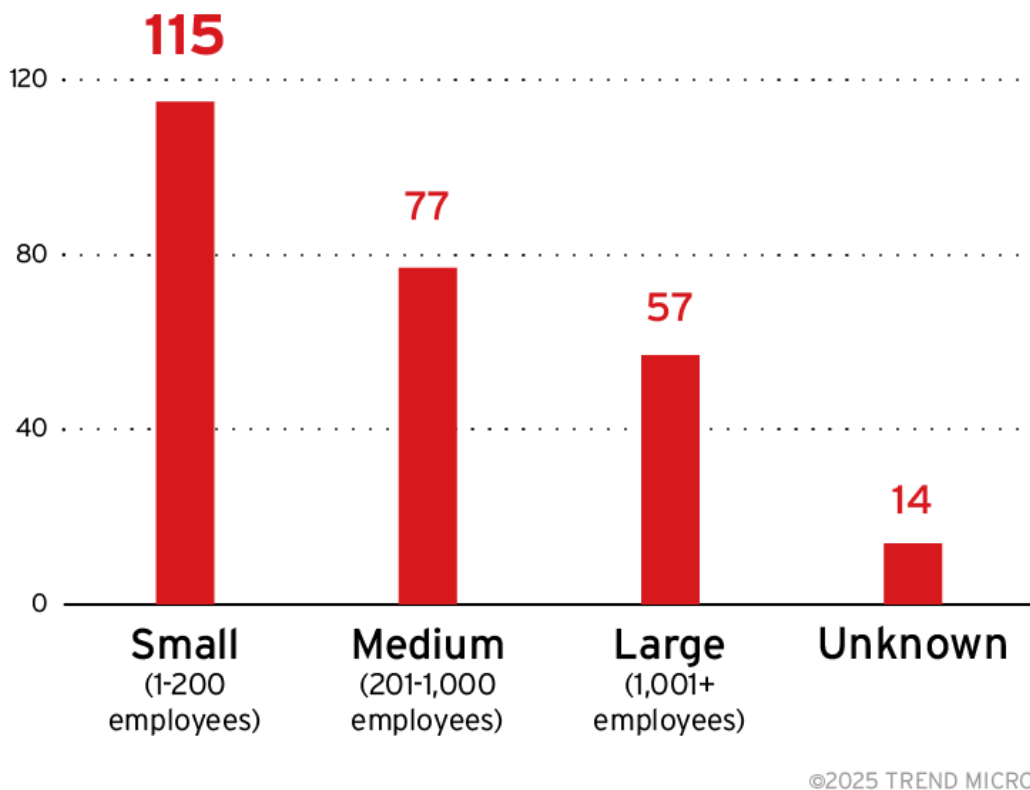


Figure 7. A breakdown of the top 10 industries targeted by Water Ouroboros ransomware attacks Sources: Water Ouroboros leak site data and OSINT research (Oct. 2023- Feb. 2025)

The threat actor launched attacks against organizations of all sizes but appeared to prefer targeting small and medium-sized businesses (1–200 and 201–1,000 employees, respectively), likely due to their limited cybersecurity resources.



[open on a new tab](#)

Figure 8. A breakdown of the sizes of the organizations targeted by Water Ouroboros ransomware attacks Sources: Water Ouroboros leak site data and OSINT research (Oct. 2023- Feb. 2025)

Trend Vision One™

[Trend Vision One™](#)[open on a new tab](#) is a cybersecurity platform that simplifies security and helps enterprises detect and stop threats faster by consolidating multiple security capabilities, enabling greater command of the enterprise's attack surface, and providing complete visibility into its cyber risk posture. The cloud-based platform leverages AI and threat intelligence from 250 million sensors and 16 threat research centers around the globe to provide comprehensive risk insights, earlier threat detection, and automated risk and threat response options in a single solution.

Trend Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Vision One customers can access a range of Intelligence Reports and Threat Insights within Vision One. Threat Insights helps customers stay ahead of cyber threats before they happen and allows them to prepare for emerging threats by offering comprehensive information on threat actors, their malicious activities, and their techniques. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and effectively respond to threats.

Trend Micro Vision One Intelligence Reports App [IOC Sweeping]

- *Hunters International (Hive Ransomware Rebranding)*
- *New Ransomware-as-a-Service Group: Hunters International seen in multiple LAR Companies*
- *SharpRhino – New Hunters International RAT*

Trend Vision One Threat Insights App

Hunting queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

```
Hunters International Ransomware Detection  
malName:*RUTHENS* AND LogType: detection
```

More hunting queries are available for Trend Vision One customers with [Threat Insights Entitlement enabled](#)[open on a new tab](#).

Recommendations

Water Ouroboros, a Ransomware-as-a-Service (RaaS) operation, demonstrates how threat actors can employ existing ransomware infrastructures while introducing new capabilities to evade detection and enhance efficiency. Despite being a relatively new group, Water Ouroboros has already targeted multiple industries worldwide, underscoring the persistent and evolving threat posed by ransomware operations.

The increasing reliance on vulnerability exploitation as an initial infection vector highlights the importance of timely patching and proactive security measures. Organizations should prioritize securing public-facing applications, as seen in Water Ouroboros' exploitation of Oracle WebLogic vulnerabilities. Additionally, threat actors are placing greater emphasis on data exfiltration rather than encryption, reinforcing the need for robust data security and incident response strategies.

To protect systems against Water Ouroboros and similar ransomware threats, organizations should implement a comprehensive security strategy that systematically allocates resources to establish strong defenses. The following best practices can help mitigate ransomware risks:

Audit and inventory

- Take an inventory of assets and data
- Identify authorized and unauthorized devices and software
- Make an audit of event and incident logs

Configure and monitor

- Manage hardware and software configurations
- Grant admin privileges and access only when necessary to an employee's role
- Monitor network ports, protocols, and services
- Activate security configurations on network infrastructure devices such as firewalls and routers
- Establish a software allow list that only executes legitimate applications

Patch and update

- Conduct regular vulnerability assessments
- Perform patching or virtual patching for operating systems and applications
- Update software and applications to their latest versions

Protect and recover

- Implement data protection, backup, and recovery measures
- Enable multifactor authentication (MFA)

Secure and defend

- Employ sandbox analysis to block malicious emails
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network
- Detect early signs of an attack such as the presence of suspicious tools in the system
- Use advanced detection technologies such as those powered by AI and machine learning

Train and test

- Regularly train and assess employees on security skills
- Conduct red-team exercises and penetration tests

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-
-
-
- - [The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructure](#)news article
 - [Complexity and Visibility Gaps in Power Automatenews article](#)
 - [Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2](#)news article
 - [Azure Control Plane Threat Detection With TrendAI Vision One™](#)news article
 - [The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026](#)predictions
 - [Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision One](#)news article
 - [The Road to Agentic AI: Navigating Architecture, Threats, and Solutions](#)news article