THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Water Hydra

Threat Actor Malware

Description

Water Hydra

CATEGORY

Malware

SEVERITY

High

Platforms

Windows & Linux

IMPACT

- Data Breaches
- Financial Loss
- Reputation Damage
- System Compromise
- Operational Disruption

Water Hydra is a sophisticated and elusive threat actor group known for its advanced cyber espionage and cyberattack capabilities. This group is characterized by its ability to adapt and evolve its tactics, techniques, and procedures (TTPs) to bypass even the most robust security measures. Water Hydra typically targets government agencies, critical infrastructure, and high-profile private sector organizations, often for purposes of political espionage or economic gain. The group is adept at exploiting zero-day vulnerabilities, spear-phishing, and deploying advanced malware that remains undetected for long periods.

Indicator of compromise

SHA-256

bf9c3218f5929dfeccbbdc0ef421282921d6cbc06f270209b9868fc73a080b8c

f1e2f82d5f21fb8169131fedee6704696451f9e28a8705fca5c0dd6dad151d64

64d0fc47fd77eb300942602a912ea9403960acd4f2ed33a8e325594bf700d65f

df0495d6e1cf50b0a24bb27a53525b317db9947b1208e95301bf72758a7fd78c

37647fd7d25efcaea277cc0a5df5bcf502d32312d16809d4fd2b86eebcfe1a5b

5c5764049a7c82e868c9e93c99f996efdf90c7746ade49c12aa47644650bf6cb

237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d

22ee095fa9456f878cfaff8f2a4871ec550c4e9ee538975c1bbc7086cde15ede

1ea0e878e276481a6faeaf016ec89231957b02cb55c3dd68f035b82e072e784b

18d87c514ff25f817eac613c5f2ad39b21b6e04b6da6dbe8291f04549da2c290

SHA-1

d41c5a3c7a96e7a542a71b8cc537b4a5b7b0cae7

3d89ad31cd13e4df562cb2eff8ef47edd9cf4329

c645b97a3753a08e642d57505f9fc0371714945c

bcc38633af6087c2fc5aefc868f8af1c374b95b9

d5742907e488ec04daec5042173e4090fe67925d

1c720c17e40d0e5864ad0e68676d0da30c25882b

2a4062e10a5de813f5688221dbeb3f3ff33eb417

943ba988d033ac64d59896868886dabbad9aa326

8ed384e6071a10d800f1f507ef561719271f662f

c562a7bd1d5e72248a1eae7b47d1dc18db8432c0

MD-5

409e7028f820e6854e7197cbb2c45d06

fb354f3d703ad29439b9bb01e9a8d5dc

550364af89288538a095df9fe4988bee

9db59da59f731692011dfa302fe2f627

1dc385972231a936352505a9e651055f

b0fd6015481f21321da77a910cdf6ce1

c56b5f0201a3b3de53e561fe76912bfd

fb282263a6bee8b3d8864c0b41e7b6e4

8ecf22eef5f008f8017f48adbd72dca0

afe012ed0d96abfe869b9e26ea375824

Remedation

1. Establish continuous monitoring of network traffic and system activity to detect and respond to suspicious behavior quickly.
2. Regularly update employees on the latest security practices and threat intelligence.
3. Deploy advanced threat detection tools such as intrusion detection systems (IDS) and security information and event management (SIEM) solutions.
4. Apply all necessary security patches, especially for zero-day vulnerabilities exploited by Water Hydra.
5. Block all IOCs on your XDR, EDR and other security tools.

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Secure your byte world

https://threatcure.net/

info@threatcure.net

+1 (832) 271 2738