

Inspect the evidence behind the intelligence.

EVIDENCE FROM OHIIHO RESEARCH

OHIIHO Research publishes primary observations from controlled environments, with the analysis and evidence needed to examine the conclusions.

ACCESS VALIDATION

One exposed profile, one month

The study maps how access is validated and reused in the hostile activity reaching a single edge-appliance profile. For defenders, the value is in the behavior behind the volume.

[FortiBleed](#), June 24, 2026.

AI-ENABLED CAPABILITY

72 hours in one documented case

An operator dependent on agentic assistance obtained tooling to create and manage remote access. The analysis follows the workflow and the artifacts it produced.

[It Built the Business](#), June 12, 2026.

POST-ACCESS BEHAVIOR

Encryption and propagation together

The analyzed Sorry-worm sample ran file encryption and SSH propagation concurrently in the same process. That relationship gives defenders a combined behavior to investigate.

[Inside Sorry-worm](#), May 1, 2026.



CYBER ARSENAL: CRIMEWARE RECOVERED FROM LIVE SESSIONS

CYBER ARSENAL

24 crimeware tools, dissected for defenders

Webshells, grabbers, and crackers dropped by real operators during live sessions, catalogued with detection signatures, the weaknesses of the tools themselves, and the backdoors their own distributors planted.

[Browse the Cyber Arsenal](#).

[Explore OHIIHO Research](#) →

From a captured Redis sequence to defensive content.

HYDRA BOT V5 | REDIS ACTIVITY OBSERVED FROM THE TARGET SIDE

One connection delivered artifacts associated with four Redis abuse patterns within 4.4 seconds. Four module-loading attempts followed, from about 10 seconds to the final attempt at 26.5 seconds.

0-4.4 s

Artifacts for four abuse patterns arrive over one TCP connection

About 10-26.5 s

Four module-loading attempts follow; none succeeds

All exploitation techniques were attempted; none succeeded against the sensor. The timing describes the observed sequence, not HIIH detection latency. Sequence, not to scale.

What the analysis used

Commands in sequence, a recovered stager, related artifacts, and infrastructure references.

What defenders can inspect

NIDS rules, YARA, Sigma, and IOC content, with hunting and hardening guidance. Review the reasoning and validate the material for your environment.

NIDS rules

YARA

Sigma

IOCs

requirepass

blocks all five vectors

bind 127.0.0.1

no external access

ACL deny

@admin · @dangerous

non-root

limits cron and SSH paths

firewall

block 6379 from the Internet

One prerequisite, unauthenticated Redis; one setting closes all five vectors. OHIIHO Research, September 1, 2026.

[Read the report and defensive content →](#)