INDICATOR SHARING

Shared Threat Intel - Modified Elephant APT

○○○ TLP:WHITE

Feb 11, 2022

A decade of persistent malicious activity targeting groups and individuals in India, including those involved in the Bhima Koregaon case, has been uncovered by SentinelLabs and the UK-based security firm

Health-ISAC is sharing these IOCs to increase sector awareness. Organizations are encouraged to ingest these IOCs manually if no automatic ingestion systems are implemented. For Health-ISAC members who have implemented the Health-ISAC Indicator Threat Sharing (HITS) program, the IOCs related to this alert have been automatically imported into your environment.

Threat Indicator(s)

SHA256:
b665efe9b3dd575e17631146706d6a950d642aa7b7401ac794480c2bb557594

c
828de55ffbfb1c1b6ffcbb56b838486dbaecc9b41a0d111fcca290978ed05e95

Domain(s):
new-agency.us

SHA1:
3fb6567e5bdd12252fdcfb867f1d5d603a2a3b29
9b0ffbdd1fa0018b96e6ba8bfaeb839e971e983f

MD5:
c14e101c055c9cb549c75e90d0a99c0a
0330921c85d582deb2b77a4dc53c78b3
b822d8162dd540f29c0d8af28847246e
0a3d635eb11e78e6397a32c99dc0fd5a

Alert ID e16ba10f

View Alert

Tags Modified Elephant APT

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Share Threat Intel For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP “Share Threat Intel” Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity related entities.

Turn off Categories For guidance on disabling this alert category, please visit the Knowlege Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.