INFORMATIONAL

HC3: Threat Profile - FIN11

TLP:WHITE

Jun 14, 2023

On June 14, 2023, the Health Sector Cybersecurity Coordination Center (HC3) shared a report "FIN11."

FIN11 is a cybercriminal group that has been active since at least 2016, originating from the Commonwealth of Independent States (CIS). While the group has historically been associated with widespread phishing campaigns, the group has shifted towards other initial access vectors. FIN11 often runs high-volume operations mainly targeting companies in various industries in North America and Europe for data theft and ransomware deployment, primarily leveraging CL0P (aka CLOP). The group has targeted pharmaceutical companies and other health care targets during the COVID-19 pandemic and continues to target the health sector. The group is behind multiple high-profile, widespread intrusion campaigns leveraging zero-day vulnerabilities. It is likely that FIN11 has access to the networks of far more organizations than they are able to successfully monetize, and choose if exploitation is worth the effort based on the location of the victim, their geographical location, and their security posture. This Threat Actor Profile provides information associated with FIN11, including recent campaigns, associated malware, CVEs exploited, and TTPs.

Please see the attached report for details.

Release Date
1686801599

Alert ID 49cf07e4

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags FIN11, HC3

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

For Questions and/or Comments

Please email us at contact@h-isac.org

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 Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

Knowledge Base

Check out our Knowledge Base for HITS integration documentation. https://health-isac.cyware.com/webapp/user/knowledge-base/f4b0c136/

Download Health-ISAC’s Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**