SHINY SCORPION C2 breached

Release date: July 13, 2023

The Federal Bureau of Investigation (FBI) has infiltrated SHINY SCORPION's command and control and seized what appears to be their victim database.

PRELIMINARY FINDINGS

FBI and Cybersecurity and Infrastructure Security Agency (CISA) advise SHINY SCORPION ransomware victims to examine the attached database. FBI and CISA provide this binary file raw, before full analysis has been completed, in the interest of immediately reducing the damage from this campaign.

Based on its findings so far, FBI developed a script that parses the ransomware's config binary. This should assist victims in identifying whether their infection was part of this campaign.

UNVERIFIED FINDINGS

FBI authorized release of these unverified findings based on potential ransomware source code discovered during the operation:

- Heavy use of steganography and ROT13 "cipher" in inter-actor communication
- Leverage Brute Ratel C4 during exploitation phase
- Include library for RSAES-PKCS1-v1_5, application not yet found
- Use of RC4 cipher for encrypting C2 communication

FILES

The following files should accompany this Cybersecurity Advisory

Victim database

Raw binary from malicious host, use caution.

`клиенты.db` - SHA256:
`71d1d994a329520e077a4a47be3443a183cc894f1599506be70bec265401eb37`

Configuration parsing script

Python script that parses SHINY SCORPION config binaries. Requires Python 3.6+ with the `constructor` package installed

`config_parser.py` - SHA256:
`f6ac9d15d1ec743baa40109b2055e778ba43fbc6986180d9792500690f989d4e`

RESOURCES

- Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- Resource to mitigate a ransomware attack: CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- No-cost cyber hygiene services: Cyber Hygiene Services and Ransomware Readiness Assessment.

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. CISA and the FBI do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA or the FBI.