Threat Actor Report: FunkeeK0ng

Analyst ID: rGxUihGQyj93

CAO: 12 February 2024

TLP AMBER

Executive Summary

FunkeeK0ng, a Southeast Asian hacktivist group that strongly associates with Furry culture, utilizes low-level cyberattacks like website defacements and data leaks to expose perceived injustices and garner media attention. Though lacking advanced technical skills, their unpredictable nature and focus on social justice causes make them a potential thorn in the side of targeted organizations.

Fig. 1. An example of an attack announcement made by the group

Key Points

- **Who**: Southeast Asian hacktivist group.
- **Motivation**: Social justice, anti-establishment, media attention.
- **Skills**: Low-level attacks; site defacements, DDoS, data leaks, social engineering, disinfo.
- **Impact**: Reputational damage, financial losses, public anxiety.

Assessment

ZedSec assesses that FunkeeK0ng presents a LOW military threat in the gray zone of conflict, operating outside traditional state structures. Their lack of conventional capabilities makes them a non-kinetic threat, but their cyber and information operations pose a potential nuisance to targeted organizations and governments. Their unpredictable nature and focus on sensitive topics complicate traditional

military responses. FunkeeK0ng is likely to remain active, continuing their low-level disruption tactics and seeking media attention. Their reliance on readily available tools and predictable TTPs makes them vulnerable to detection and mitigation efforts. However, their ability to exploit social media, manipulate public perception, and target sensitive topics requires ongoing vigilance and proactive countermeasures.

Threat Actor

Summary

Believed to originate from Southeast Asia, their exact location and structure remain unclear. FunkeeK0ng likely operates as a loosely connected network of individuals with shared ideologies, lacking a centralized leadership structure. It is assumed that their recruitment is done through online forums and social media communities that focus on hacktivism and social justice activism.

Driven by a strong belief in social justice, environmental protection, and anti-establishment ideals. Targets organizations perceived as unethical, oppressive, or environmentally destructive, regardless of affiliation (governments, corporations, media outlets). Actions motivated by a desire to expose wrongdoing, raise awareness, and challenge the status quo, often seeking media attention and public validation.

The group self-identifies itself as “degenerate furry cybersecurity artists” and is known for its comical slogans and vulgar language. Chats, images, scripts, and data leaks all involve anime or furry themes and imagery. They have connections with other hacker groups like PhantomSec and have members probably ranging in age from 19 to 29.

TTPs

Tactic: Social Engineering and Information Gathering
Technique: Pretexting
Procedure: FunkeeK0n created a fake LinkedIn profile impersonating a researcher from a fictional environmental NGO and targets employees of "Veridian Chemicals" (from your previous request), attempting to trick them into disclosing information about the company's waste disposal practices.

Tactic: Social Engineering and Information Gathering
Technique: Phishing

Procedure: FunkeeK0ng will create email lures by seeking to connect with other professionals at organizations through professional service sites or LinkedIn. These phishing emails will contain redirectors that deliver a fake landing page to capture credentials.

Tactic: Website Defacement with Disinformation
Technique: Content Modification
Procedure: FunkyCan defaced the website of "Apexium Pharmaceuticals", replacing product descriptions with fake news articles accusing the company of unethical drug testing practices.

Capabilities

- XSS
- SQLi
- Automated Tools

Infrastructure

- Tox Chat
- StartMail
- Nord VPN
- Public Telegram Group, with likely private Telegram Group
- Digital Ocean VPS

Victims

- Primary Targets: Governments, Manufacturing Corporations
- Secondary Targets: Media outlets

Intelligence Gaps

- Who are the core members?
- What is the leadership structure?
- How do they perform recruitment?
- Have they internally built any tools?

MITRE ATT&CK

Tactic	Technique	Description
TA0043	T1595	Active Scanning
TA0001	T1189	Drive-by Compromise
TA0001	T1190	Exploit Public-Facing Application
TA0001	T1566.002	Phishing: Spearphishing Link
TA0001	T1566.004	Phishing: Spearphishing Voice
TA0009	T1560.001	Archive Collected Data

Timeline of Activity