NCA-26.051126 – National CERT Advisory

Emerging AI-Enabled Cyber Threats Targeting Financial Institutions and OT/ Critical Infrastructure

Overview

1. Background

The increase in use of Artificial intelligence (AI), automated bots, botnets and agentic tools to automate reconnaissance, identify vulnerabilities, conduct credential-based attacks and launch coordinated cyber attacks is observed recently. These capabilities may help threat actors and sophisticated cyber criminal groups to broader the scale, speed and sophistication of their operations. This advisory is relevant to all sectors/organizations, however, two sectors require particular attention:

Financial Services: Banks and financial institutions may face attacks targeting core banking systems, digital banking platforms, APIs, payment systems and customer-facing applications. Potential scenarios include disruption of online services, automated credential attacks, and manipulation of displayed account balances which may trigger customer's panic even where underlying funds remain same.

OT and Critical Infrastructure: Third party service providers, Connected IoT devices, vulnerabilities in industrial control systems and insecure remote access may expose Oil and gas facilities, water utilities, power generation and distribution networks, manufacturing, transportation and other essential services. A compromise could disrupt physical processes and critical services.

Recent cyber incidents reported at European supermarkets involving refrigeration and freezer systems shows the potential physical and commercial consequences of attacks against connected operational systems. However, AI involvement in said incidents has not been confirmed yet.

2. Threat Indicators and Potential Risks

Organizations may observe for the following suspicious anomalies:

Financial Services

- Increase in automated login attempts, repeated authentication failures and credential stuffing.
- Unusual API requests, changes to application configurations, and abnormal transaction patterns.
- Difference between core banking records and customer facing account balances.
- Unauthorized access to payment systems.

OT and Critical Infrastructure

- Changes to refinery, pipeline, grid, power generation or distribution parameters.
- Access to ICS, SCADA and industrial control environments.
- Unexpected changes to pressure, temperature, cooling or heading control settings.
- Unexpected access sessions remotely or changes to IoT/OT device configurations.

3. Recommendations

Financial Services

- Check the core banking security, APIs, third party integrations, payment gateways and digital banking applications.
- Use multi-factor authentication, protection against automated login attempts, and privileged-access management.
- Enforce integrity checks between consumer facing applications and core banking records, and independent transaction reconciliation.
- Monitor bot-driven attempts, potential service disruption and abnormal API activity.

OT and Critical Infrastructure

- Find out internet facing IoT/OT assets and check the security of ICS, SCADA and industrial control systems.
- Limit direct internet exposure and remote access i.e. third party maintenance connections.
- Enforce OT/IT network segmentation and continuously monitor access to operational systems.
- Keep applying security updates and maintain backup operating procedures for essentials processes.

All Organizations

- Check organizational preparedness against bot-driven AI cyberattacks

- Enhance arrangements of incident response, business continuity and security monitoring
- Maintain security logs, and report suspected incidents through relevant national cyber security channel.

For other advisories, please visit the NCERT website: https://pkcert.gov.pk/advisories.asp

National Cyber Emergency Response Team (NCERT)
Government of Pakistan
Pak Secretariat, L Block, Islamabad
+92-51-9203422
info@pkcert.gov.pk
www.pkcert.gov.pk