



MINISTRY OF NATIONAL SECURITY

GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

April 29, 2022

For Immediate Release

PUBLIC ADVISORY

INCREASED CYBER ACTIVITY IN TRINIDAD AND TOBAGO AND THE REGION

Port of Spain: The Trinidad and Tobago Cyber Security Incident Response Team (TT-CSIRT) of the Ministry of National Security has observed a sharp increase in malicious cyber activity, targeting local and regional entities, over the past two (2) months. The TT-CSIRT is urging all entities (public and private) to adopt a heightened state of awareness and be guided by the following:

1

Top Threats to T&T

The most prominent threats that TT-CSIRT has observed include:

- Ransomware
- Social Engineering (Phishing)
- Malicious Insiders

Attack Vectors

Cyber-attacks can be initiated through multiple attack vectors. The most prominent vectors used against local entities are:

- Exploitation of system vulnerabilities (particularly outdated firewall appliances and email systems)
- Phishing emails with infected attachments or links
- Compromised user credentials

Incident Reporting

Should your organization fall victim to a cyber-attack, we encourage entities to contact:

The TT-CSIRT immediately, via our online form <https://ttcsirt.gov.tt/report-an-incident/> for incident management guidance and technical assistance.

The Cyber Crime and Social Media Unit of the Trinidad and Tobago Police Service, via the information at <https://ttcsirt.gov.tt/ttcs-cyber-crime-unit/>.

Measures for Securing Your Systems

The TT-CSIRT recommends that all organizations review the following resources; and take the necessary actions:

- TT-CSIRT Ransomware Guidance - <https://ttcsirt.gov.tt/ransomware-alert-2020/>
- TT-CSIRT Social Engineering Guidance - <https://ttcsirt.gov.tt/social-engineering/>
- Get Safe Online TT (Individuals) - <https://www.getsafeonline.tt/>
- Get Safe Online TT (Businesses) - <https://www.getsafeonline.tt/business/>

2

This alert can also be viewed on the TT-CSIRT website via <https://ttcsirt.gov.tt/threat-alert-2022/>

END