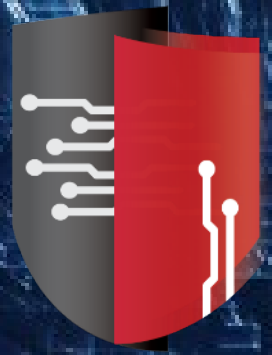


TT-CSIRT

Trinidad and Tobago Cyber Security Incident Response Team

Operationalizing Cyber Threat Intelligence

Rick Logan-Stanford
Cyber Security Specialist

TT-CSIRT

Trinidad and Tobago Cyber Security Incident Response Team

- ABOUT TTCSIRT
- CYBER THREAT INTELLIGENCE
- OPERATIONALIZING C.I.
- USE CASES
- Q & A

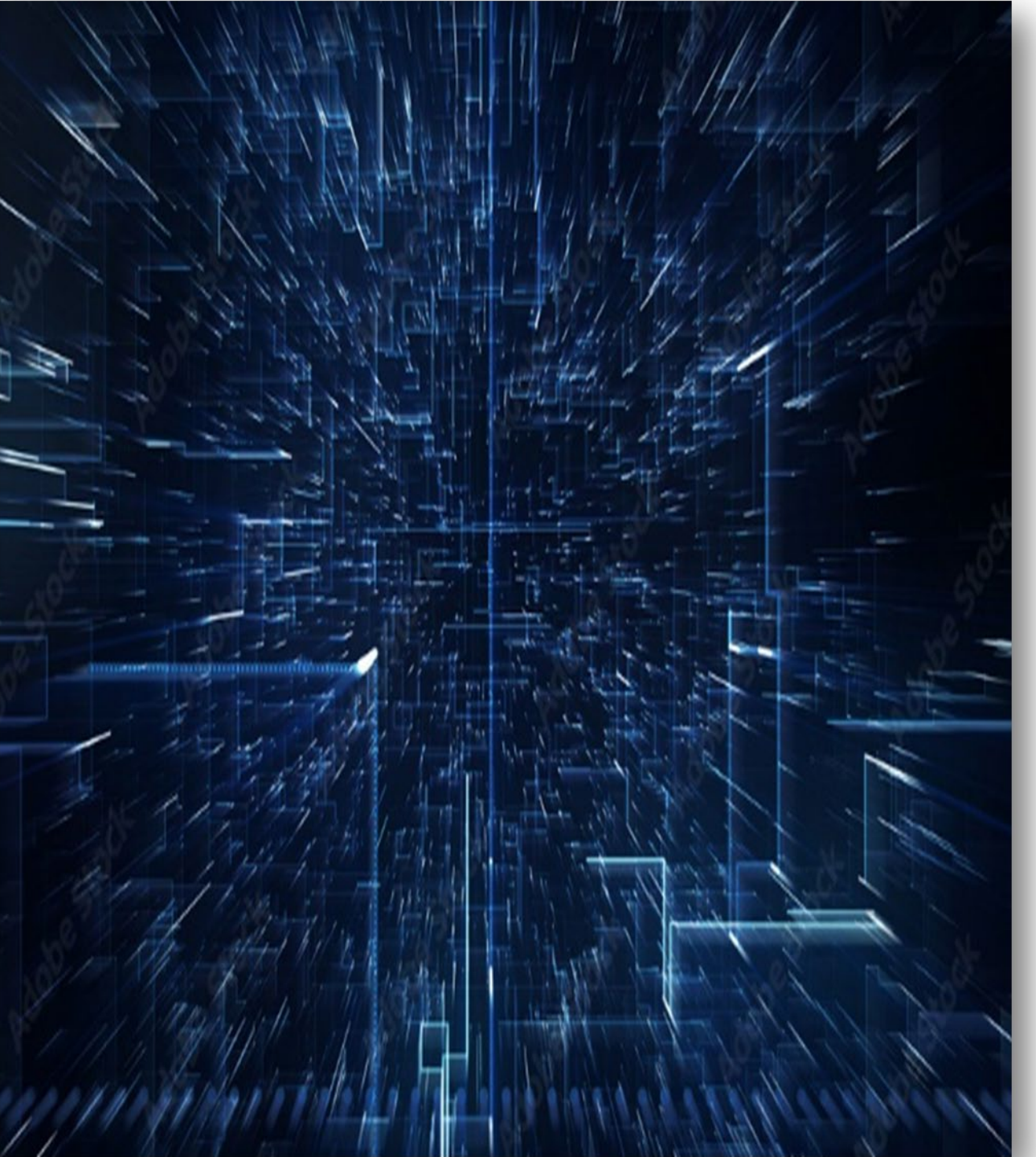
Trinidad and Tobago Cyber Security Incident Response Team

Administratively based in the Ministry of National Security

Developed out of the National Cyber Security Strategy 2012

Created in 2015 and Operationalized in 2017

https://ttcsirt.gov.tt/national-cyber-security-documents/



Core Services

- **Alerts and Advisories**
- **Incident Response**
- **Cyber Threat Intelligence**
- **Awareness Building**
- **Education/Training**
- **Security Audits or Assessments**
- **Secure Architecture**
- **Policy Development**
- **Vulnerability Handling**

https://ttcsirt.gov.tt/core-functions/

TT-CSIRT

Trinidad and Tobago Cyber Security Incident Response Team

Our Partners

- **TTPS CYBER AND SOCIAL MEDIA UNIT**
- **IGOVTT**
- **CARICOM IMPACS**
- **GETSAFEONLINETT**
- **UK FOREIGN, COMMONWEALTH & DEVELOPMENT OFFICE – CSIRT COMMONWEALTH**
- **ORGANIZATION OF AMERICAN STATES – CSIRTAMERICAS**

https://ttcsirt.gov.tt/core-functions/

CYBER THREAT INTELLIGENCE

What is Cyber Threat Intelligence?

Cyber Threat Intelligence is an evidence-based knowledge approach used to inform decisions for the mitigation of an attack which includes prevention.

Through operationalization of cyber threat intelligence, there are several aspects an organization or government entity will have to focus on in order to have maximum effectiveness for countermeasures and protection.

By operationalizing CTI, CSIRTs can help organizations and State entities facing challenges due to a lack of skills and funds, with CSIRTs being leveraged to minimize disinformation and misinformation with information that has been digested, analysed and made actionable.

Tools and Techniques

Some effective, efficient and economical tools CSIRTs can utilize to help in threat intelligence gathering:

- Shodan
- Dark Web Forums
- Threat Feeds and Alerts
- Dashboards (e.g. CSIRTAmericas Network Dashboard)
- Social Media

Operationalization

Aspects of Operationalizing C.I.:

- Intelligence requirements
- Threat Modelling
- Collection Management (with relation to the data being gathered, stored and assimilated)

Intelligence Requirements

By defining the threat requirements, time invested in information gathering and research can be efficiently used to prioritize the most relevant and critical information. This prevents the loss of crucial data in the noise or the processing of unnecessary noise. Understanding which type of information is not only of interest but relevant to the cyberspace in which the organization or entity operates.

For example, an organization in the financial sector would not have any need for information relevant to the energy sector or even SCADA systems. This prevents the wasting of time on irrelevant information gathering and processing.

Threat Modelling

Threat Modelling:

- Identify the Assets
- Outline Architecture
- Break Down the Application
- Identify Threats
- Classify & Structure Threats
- Rate Severity of Threats

Top Model Templates:

- **STRIDE** – designed to focus on IT-related threats
- **PASTA** – a risk-centric model which is adaptable and allows for threat simulation
- **LINDDUN** – focuses on Data and Privacy related threats
- **OCTAVE** – is focused on Risk Management and organizational impact
- **VAST** – scales across infrastructure focusing on the attacker

Best Practices of threat modelling from scratch:

- ✓ Define the scope and depth of analysis
- ✓ Gain a visual understanding of what is being threat-modelled
- ✓ Model attack possibilities
- ✓ Identify threats (stemming from potential attacks)
- ✓ Create a traceability matrix of missing or weak security controls

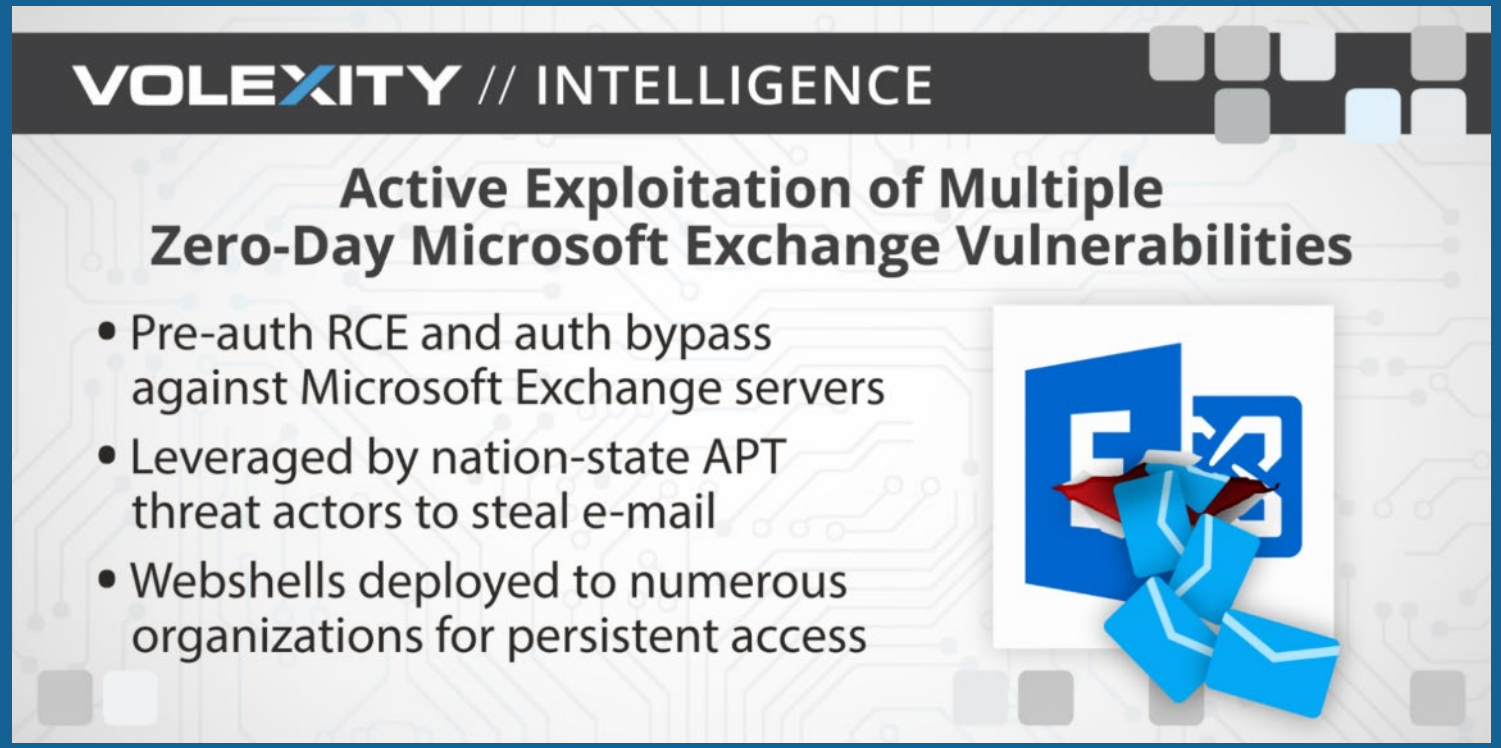
Collection Management

- Understand the data sources identified and available to fit the defined requirements.
- Data has to be accessible to analysts in the form of a simple, effective and convenient format.
- Consider internal and external blind spots with technical and automated techniques.

Employ a collection management framework to validate data collected. Validating the relevance, reliability, accuracy and completeness will produce effective and actionable results.

CASE STUDIES

CASE STUDY 1



Release Date:

- 2nd March, 2021

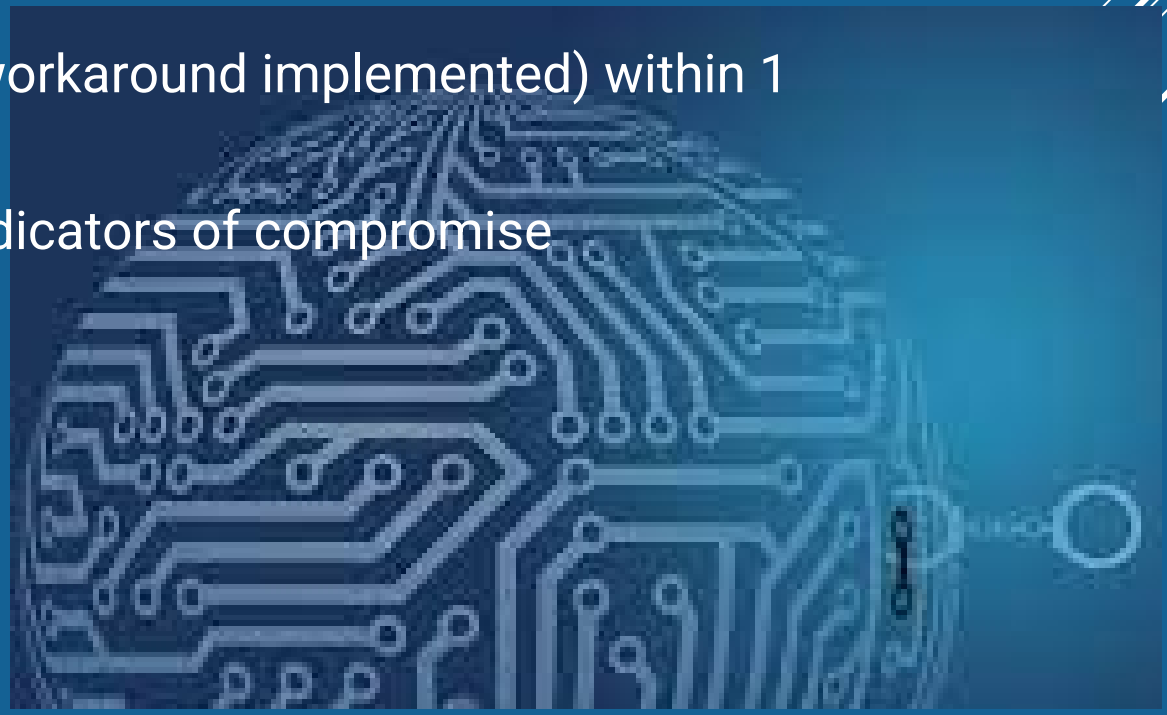
CVEs:

- CVE-2021-26857
- CVE-2021-26858
- CVE-2021-27065
- CVE-2021-26855

RESPONSE AND INVESTIGATION

The steps TT-CSIRT followed to limit impact to Trinidad and Tobago’s private and public constituencies:

- Developed a list of vulnerable servers using Shodan http.title:outlook exchange country:"TT"
- Ensured that each organization was patched (or workaround implemented) within 1 week of being alerted
- Developed a guide for organizations to look for indicators of compromise



CASE STUDY 2

Major VPN Vulnerability

- CVE-2018-13379
- Initial Advisory: 24th May, 2019

Exploit:

- Append the following to the public interface for the SSL-VPN

This particular vulnerability leaked the session file of vpn connections. The session file contains valuable information, such as username and plaintext password, which allows a threat actor to login easily.

RESPONSE AND INVESTIGATION

Response steps TT-CSIRT initiated to limit impact to the Trinidad and Tobago's constituency:

- Compared the dark web dump to Trinidad and Tobago's IP blocks
- Worked with ISPs to identify the affected organizations
- Worked with local product vendor office to alert those organizations
- Worked with identified entities to ensure each were patched (or workaround implemented) within 1 week of being alerted
- Developed a guide for organizations to look for indicators of compromise as well as actions to be taken.

Q & A

THANK YOU!

@TTCSIRT

https://ttcsirt.gov.tt

Stay SECURE!