RESEARCH FELLOW
DR BOOJOONG KANG

25 MAY 2018

Centre for Secure Information Technologies (CSIT)

CSIT is the UK's National Innovation and Knowledge Centre (IKC) for cyber security

Certified by GCHQ as "Academic Centre of Excellence in Cyber Security Research" (ACE-CSR)

Queen's Anniversary Prize, 2015 for "strengthening global cyber security"

5 of the top 25 US cyber security companies engaged with CSIT

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Main Research Focus

Networked Systems Security

Preventive and **Defensive Cybersecurity Technologies** against emerging **Cyberthreats** imposed by **Intrusion**, **Malware** and **Technological Vulnerabilities** of **Mobile Devices**, **Network Appliances** and **Protocols**, **Industrial Control Systems (ICS and SCADA)**, **IoT/IIoT** and **Cloud Technologies** and **Service**.

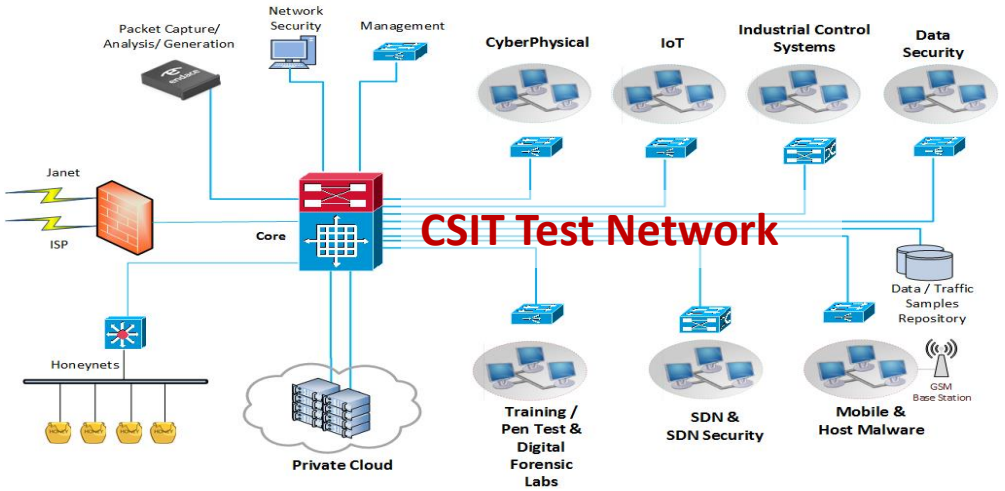
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Networked Systems Security

ICS CYBER SECURITY

ICS Security

Network Security



Cloud Security

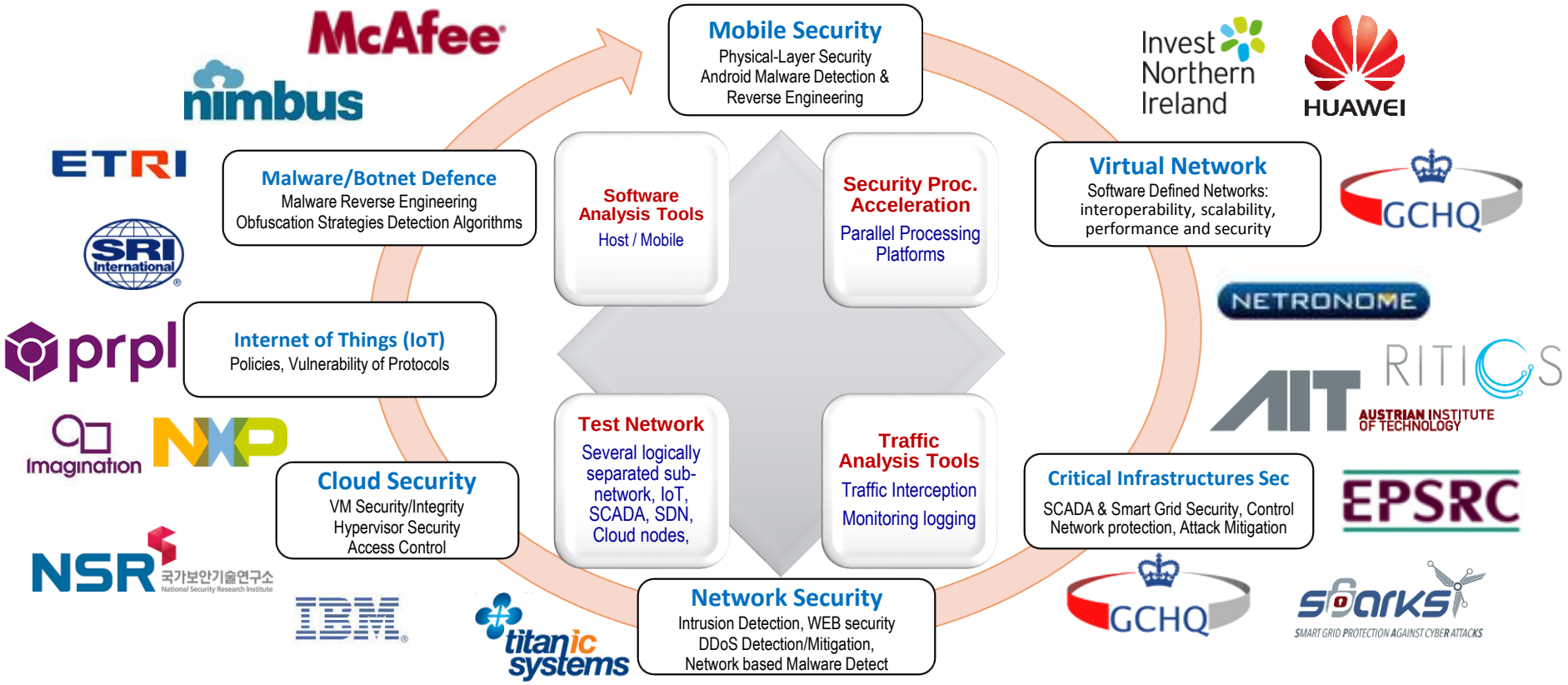
IoT Security

Mobile Security

Malware Analytics

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Networked Systems Security



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

ICS Security

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Industrial Control Systems

Oil & Gas

Power Grid

Transport System

Enhanced connectivity enables opportunities for unauthorized remote access and unforeseen attack surfaces

Ultimately Exposing ICS to Cyber Threats

Telecommunication Infrastructure

Water Supply System

Financial Systems

Timeline of well-investigated ICS specific Cyberattacks

Black Energy: Malware targeting internet-connected HMIs
2011 to 2014, HMI products: GE, Siemens, BroadWin

Havex: Targeting OPC communications (2014)
Widely used in process control systems

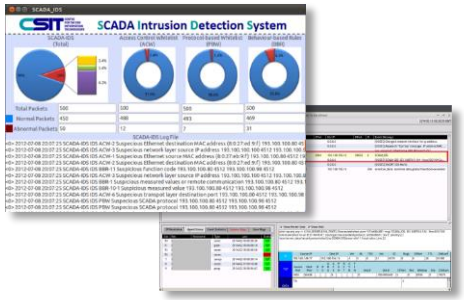
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

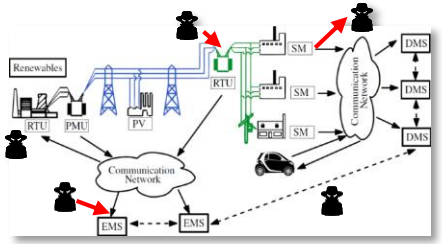
Ukraine PA: Employees spear-phished and Microsoft Office macros allowed RAT to be installed.

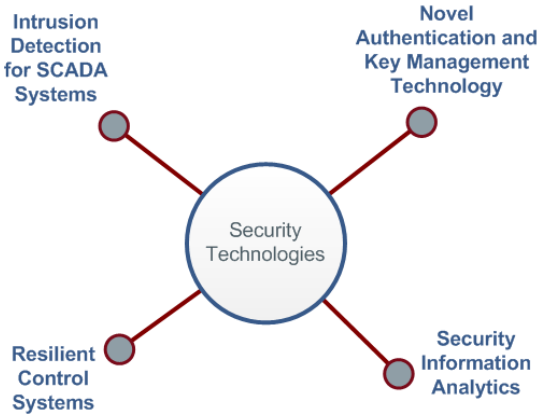
Ukraine PA2 + CrashOverride: Custom purpose malware designed to attack electric grid systems, taking advantage of the ICS protocols IEC101, IEC104, and IEC61850.

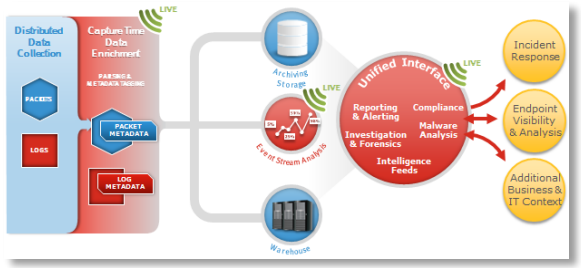
TRISIS: Malware designed to manipulate "safety controllers" made by Schneider Electric, widely in nuclear power plants, oil and gas production facilities, and paper mills.

Secure and Resilient ICS





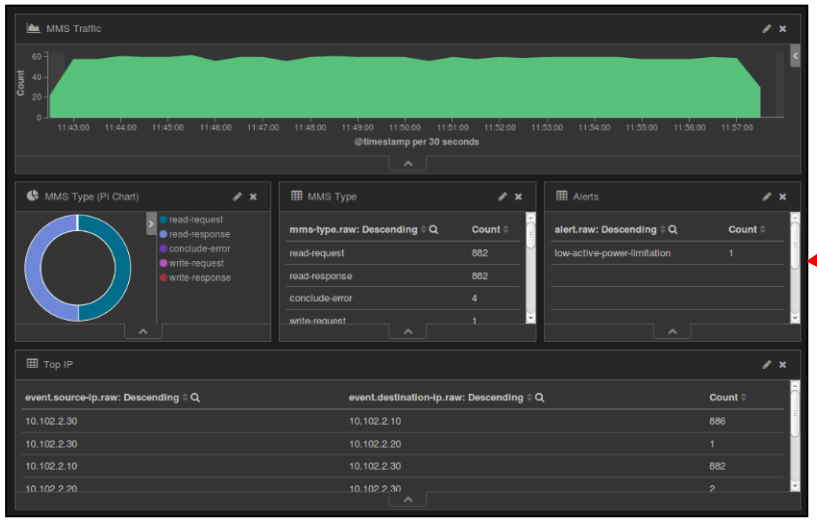




CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Intrusion Detection System

Network Traffic



Whitelist

Signature Detection

Stateful Analysis

Anomaly Detection

Unauthorized Access

Known Simple Attacks

Known Sophisticated Attacks

Protocol Violation

Unknown Attacks & Anomalies

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Malware & Mobile Security

Malware Research Objectives

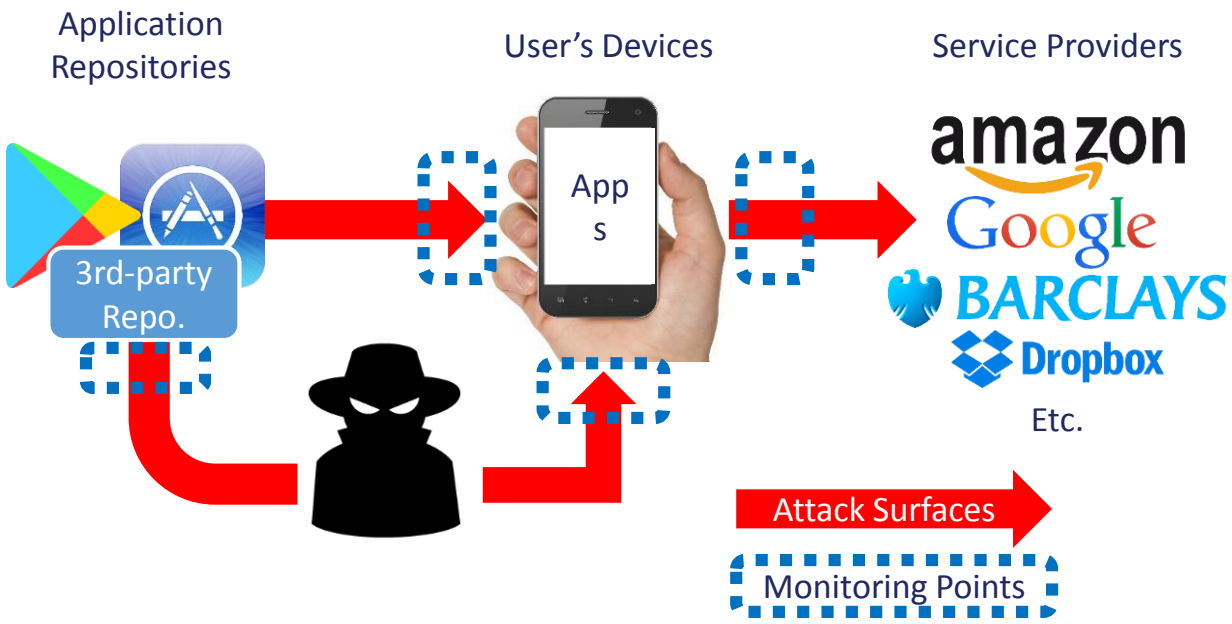
Develop strategies to detect, prevent and mitigate malware, which are:

- across all phases of the attack chain
- immune to obfuscation
- zero-day ready
- capable of detecting the currently undetectable
- potentially hardware-based

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Mobile Security

- Static & Dynamic Analysis
- Network Traffic Analysis
- User Behavior Analysis
- Artificial Intelligence

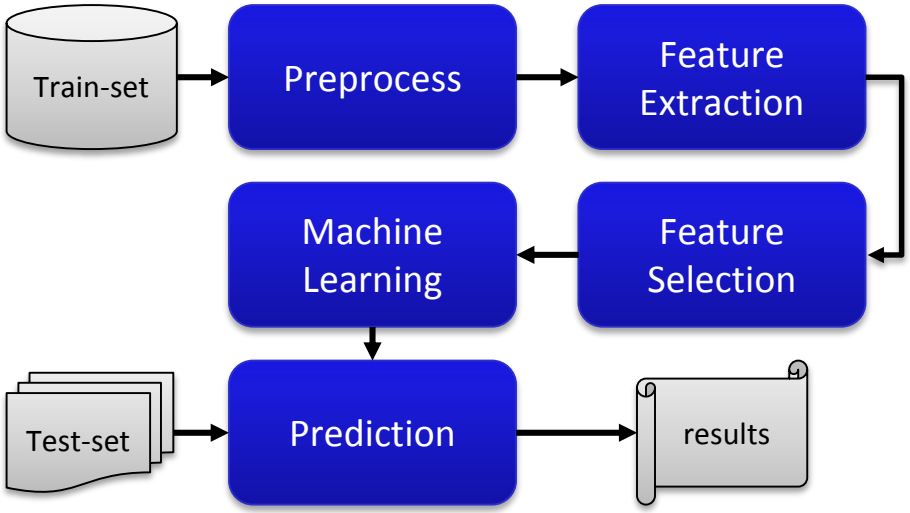


CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Malware Detection with Machine Learning

Features

- Permission, intents, components, configuration information from Manifest files
- Program code, API, strings from DEX files
- Other resources and shared libraries



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

N-gram Analysis on Opcodes

- 1 byte opcode = 256 opcodes (218 opcodes in used)
- *N*-gram is a contiguous sequence of *n* items
  - a contiguous sequence of *n* opcodes (218^n possibilities)

<Method>

```
.method public a(ILjava/lang/String;)V
   .register 5
    opcode          operands
   iget-object v0, p0, Lb;->K:Lcom/izp/views/IZPDelegate;
   if-eqz v0, :cond_b
   iget-object v0, p0, Lb->K:Lcom/izp/views/IZPDelegate;
   iget-object v1, p0, Lb;->J:Lcom/izp/views/IZPView;
   invoke-interface {v0, v1, p1, p2}, Lcom/izp/views/IZPDelegate;->errorReport(Lcom/izp/views/IZPView;ILjava/lang/String;)V
   :cond_b
   const/16 v0, 0x2710
   invoke-virtual {p0, v0}, Lb;->a(I)V
   return-void
.end method
```

n-grams of the opcodes (***n-opcodes***)


CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES
THANK YOU