Countering ransomware threats with ITU-T standards and CYBEX

Youki Kadobayashi

Co-rapporteur, ITU-T Q14/17
Co-convenor, CG-CYBEX

The role of ITU-T standards in the fight against ransomware

- Ransomware abuses anonymity
  - IdM standards can help
- Ransomware abuses cryptocurrency
  - DLT security standards can help
- Ransomware exploits vulnerabilities
  - CYBEX standards can help
- Ransomware campaigns are moving targets
  - Information exchange is key

IdM standards

- Q10/17 develops broad array of standards to assure identity and to provide strong authentication in an interoperable fashion:

- X.1250: Baseline capabilities for enhanced global identity management and interoperability
- X.1251: A framework for user control of digital identity
- X.1252: Baseline identity management terms and definitions
- X.1253: Security guidelines for identity management systems
- X.1254: Entity authentication assurance framework

IdM standards under development in collaboration with other SDOs

- Level of Assurance (LoA)
- Multi-factor authentication
- Step-up authentication

- With these standards,
  - Identity spoofing will be far more difficult
  - Theft of authentication credentials, which is one of the avenue of ransomware attacks, will also be much harder

DLT security

- At Q14/17, three draft Recommendations are under development in the area of *Security for DLT platforms*:
  - X.sradlt: Security architecture for distributed ledger technology
  - X.sct-dlt: Security capabilities of, and threats to distributed ledger technology
  - X.sadlt : Security assurance for distributed ledger technology
- Abuse of anonymous cryptocurrencies should be discussed within the group
- Technical characterization of cryptocurrencies should be considered

Standards for managing vulnerabilities

- CYBEX (ITU-T X.1500-series) provides key standards for vulnerability management
- For instance:
  - WannaCry, WannaCrypt can be prevented by patching the associated SMB vulnerabilities (CVE-2017-0143 to 0148)
  - Some of recent incidents could be prevented by vulnerability management practices

CYBEX standards

- X.1500, Overview of cybersecurity information exchange (CYBEX)
- X.1520, Common vulnerabilities and exposures (CVE)
- X.1521, Common vulnerability scoring system (CVSS)
- X.1524, Common weakness enumeration (CWE)
- X.1525: Common weakness scoring system (CWSS)
- X.1526, Language for the open definition of vulnerabilities and for the assessment of a system state
- X.1528, Common platform enumeration
- X.1541: Incident object description exchange format version 2
- X.1544, Common attack pattern enumeration and classification
- X.1546, Malware attribute enumeration and characterization

Ransomware over the cloud

- Data on the cloud storage has been under attack since 2017
  - MongoDB, ElasticSearch, Hadoop, etc.
  - Data stolen, encrypted, or wiped
- Installations are often insecure by default
  - Configuration vulnerability
  - Also: human mistakes. API key in Github code etc.

Information exchange: a crucial technique to fight against campaigns

- Campaigns are abusing dynamic elements:
  - Cloud,
  - DNS,
  - JavaScript
- Harder to detect, easier to evade

- Information exchange among variety of e-services providers are crucial to reveal the entire campaign:
  - Service providers for e-mail, advertisement, hosting, domain name registry, SOC, antivirus, + law enforcement

Summary: the role of ITU-T standards in the fight against ransomware

- Ransomware abuses anonymity
  - IdM standards can help
- Ransomware abuses cryptocurrency
  - DLT security standards can help
- Ransomware exploits vulnerabilities
  - CYBEX standards can help
- Ransomware campaigns are moving targets
  - Information exchange is key