TLP

Week 8B

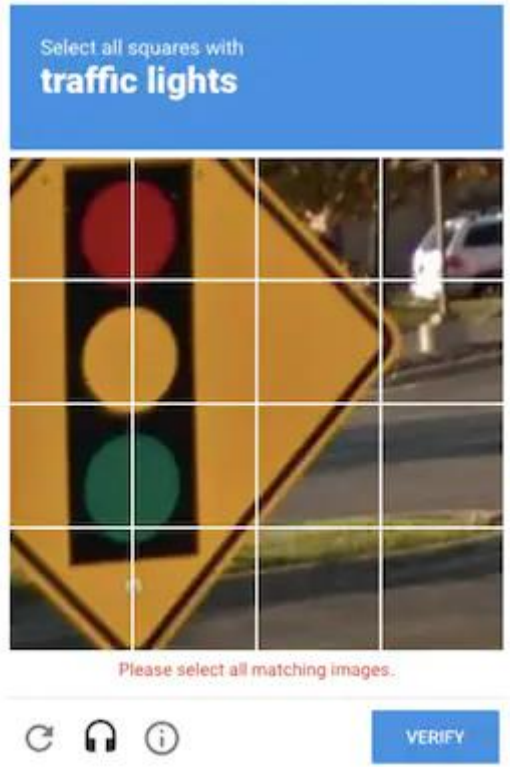
Presented by Dr Rory Coulter

Traffic Light Protocol

The Traffic Light Protocol (TLP) is a system for sharing sensitive information securely

Uses different colour-coded levels to indicate the degree of restriction on access and use

- Introduced to aid and support information sharing (with appropriate audience)
- TLP isn't a classification scheme (e.g., Secret, Top Secret)
- Designations:
  - TLP:RED
  - TLP:AMBER+STRICT
  - TLP:AMBER
  - TLP:GREEN
  - TLP:CLEAR



https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

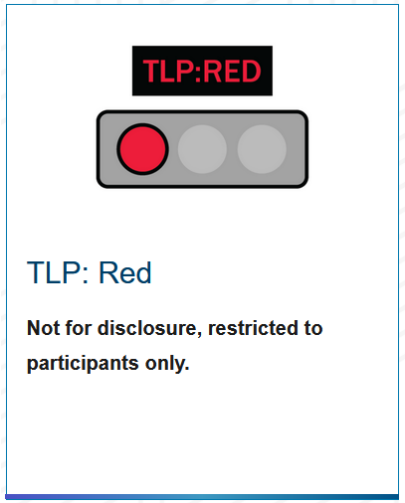
https://akm-img-a-in.tosshub.com/indiatoday/images/story/202105/captcha.jpg?size=690:388

Traffic Light Protocol (cont.)

TLP:RED is the highest level of restriction

Information marked as TLP: RED should not be disclosed and is restricted to participants only

- It is used when sharing the information could pose significant risks to privacy, reputation, or operations of the organisations involved
- Recipients may not share TLP: RED information with parties outside of the specific exchange, meeting, or conversation where it was originally disclosed
- TLP: RED information is usually exchanged verbally or in person



https://www.cyber.gov.au/sites/default/files/2023-02/2023-01%20-%20ACSC%20Ransomware%20Profile%20-%20Royal.pdf

https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

SWINBURNE UNIVERSITY OF TECHNOLOGY

Traffic Light Protocol (cont.)

TLP:AMBER+STRICT

TLP:AMBER+STRICT indicates a high level of restriction

- It is used when information requires support but still carries risks to privacy, reputation, or operations if shared outside the organisation
- Recipients may only share TLP: AMBER+STRICT information with members of their own organisation on a need-to-know basis to protect their organisation and prevent further harm

https://www.cyber.gov.au/sites/default/files/2023-02/2023-01%20-%20ACSC%20Ransomware%20Profile%20-%20Royal.pdf

https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

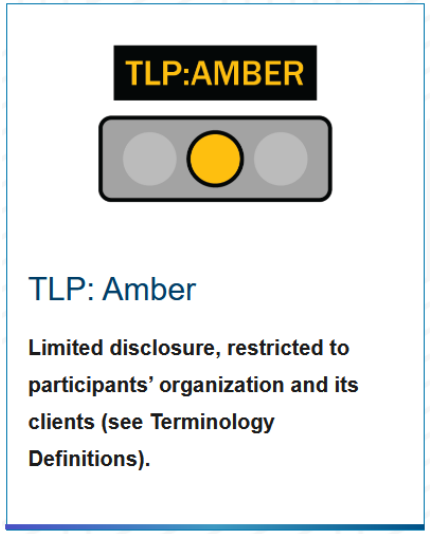
SWINBURNE UNIVERSITY OF TECHNOLOGY

Traffic Light Protocol (cont.)

TLP:AMBER

TLP:AMBER signifies limited disclosure

- It is used when information requires support but still carries risks if shared outside the organisations involved
- TLP: AMBER+STRICT should be used to restrict sharing to the recipient organisation only
- Recipients may share TLP: AMBER information with members of their own organisation and its clients on a need-to-know basis to protect their interests



https://www.cyber.gov.au/sites/default/files/2023-02/2023-01%20-%20ACSC%20Ransomware%20Profile%20-%20Royal.pdf

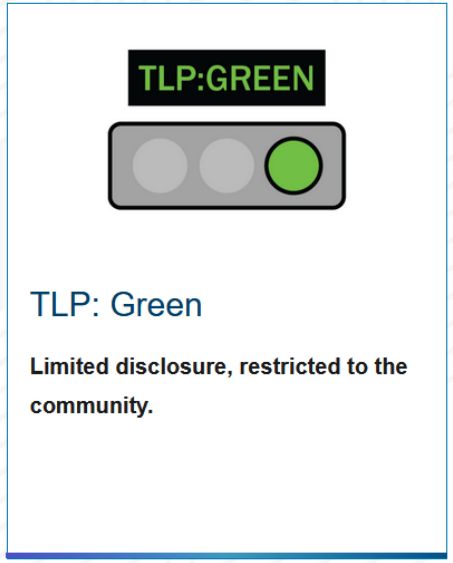
https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

Traffic Light Protocol (cont.)

TLP:GREEN indicates limited disclosure

It is used when information can increase awareness within a specific community

- Recipients may share TLP: GREEN information with peers and partner organisations within their community but not through publicly accessible channels
- TLP: GREEN information is typically shared within the cyber security or cyber defence community



https://www.cyber.gov.au/sites/default/files/2023-02/2023-01%20-%20ACSC%20Ransomware%20Profile%20-%20Royal.pdf

https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

Traffic Light Protocol (cont.)

TLP:CLEAR signifies no significant restrictions on disclosure

It is used when information carries minimal or no foreseeable risk of misuse

- Recipients can share TLP:CLEAR information without restriction, following standard copyright rules and procedures for public release

A Threat Advisory

Let’s look at a way intelligence is shared

TLP:CLEAR The what

- A Cyber Threat Advisory is a formal communication that provides organisations and individuals with critical information about potential or active cyber security threats
- Released by government and vendors
- Cyber Threat Advisories are typically issued by trusted cybersecurity authorities, government agencies, or industry-specific information sharing and analysis centres (ISACs)
- Primary purpose of a Cyber Threat Advisory is to raise awareness about specific cyber threats, vulnerabilities, or incidents that could impact an organisation's security

https://www.cyber.gov.au/sites/default/files/2023-08/aa23-215a_joint_csa_2022_top_routinely_exploited_vulnerabilities.pdf

SWINBURNE UNIVERSITY OF TECHNOLOGY

A Threat Advisory (cont.)

Let’s look at a way intelligence is shared

TLP:CLEAR What may be covered

- Threat Description: Detailed information about the nature and characteristics of the cyber threat
- Indicators of Compromise (IoCs): Specific data or artifacts associated with the threat
- Vulnerabilities: Information about any software or hardware vulnerabilities being exploited
- Mitigation and Remediation: Guidance on how to detect, prevent, and respond to the threat
- Impact Assessment: An analysis of the potential impact on affected systems or networks
- Recommendations: Actions that organisations should take to protect themselves

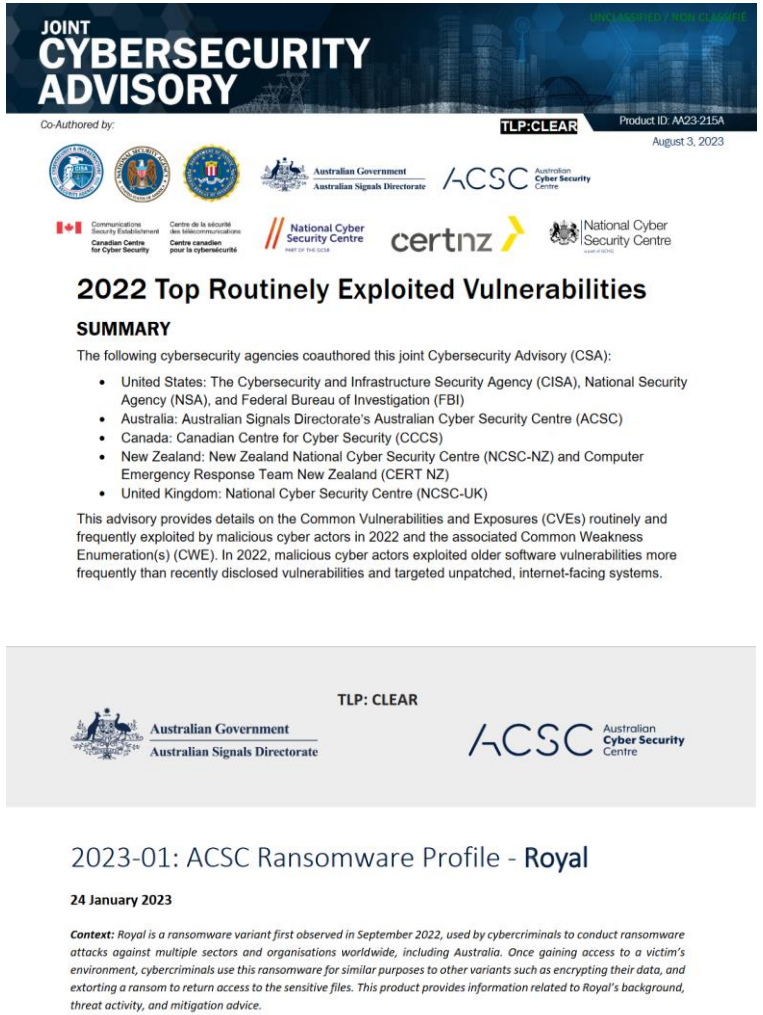
https://www.cyber.gov.au/sites/default/files/2023-08/aa23-215a_joint_csa_2022_top_routinely_exploited_vulnerabilities.pdf

A Threat Advisory (cont.)

Let's look at a way intelligence is shared

Two Examples

- Top Vulnerabilities
  - See below for the link
- Actor Profile
  - See below for the link



JOINT
CYBERSECURITY
ADVISORY

UNCLASSIFIED / NON CLASSIFIÉ

Co-Authored by:

TLP:CLEAR

Product ID: AA23-215A

August 3, 2023

Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
certnz
National Cyber Security Centre

2022 Top Routinely Exploited Vulnerabilities

SUMMARY

The following cybersecurity agencies coauthored this joint Cybersecurity Advisory (CSA):

- United States: The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI)
- Australia: Australian Signals Directorate's Australian Cyber Security Centre (ACSC)
- Canada: Canadian Centre for Cyber Security (CCCS)
- New Zealand: New Zealand National Cyber Security Centre (NCSC-NZ) and Computer Emergency Response Team New Zealand (CERT NZ)
- United Kingdom: National Cyber Security Centre (NCSC-UK)

This advisory provides details on the Common Vulnerabilities and Exposures (CVEs) routinely and frequently exploited by malicious cyber actors in 2022 and the associated Common Weakness Enumeration(s) (CWE). In 2022, malicious cyber actors exploited older software vulnerabilities more frequently than recently disclosed vulnerabilities and targeted unpatched, internet-facing systems.

TLP: CLEAR

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

2023-01: ACSC Ransomware Profile - **Royal**

24 January 2023

Context: *Royal is a ransomware variant first observed in September 2022, used by cybercriminals to conduct ransomware attacks against multiple sectors and organisations worldwide, including Australia. Once gaining access to a victim's environment, cybercriminals use this ransomware for similar purposes to other variants such as encrypting their data, and extorting a ransom to return access to the sensitive files. This product provides information related to Royal's background, threat activity, and mitigation advice.*

https://www.cyber.gov.au/sites/default/files/2023-08/aa23-215a_joint_csa_2022_top_routinely_exploited_vulnerabilities.pdf

https://www.cyber.gov.au/sites/default/files/2023-02/2023-01%20-%20ACSC%20Ransomware%20Profile%20-%20Royal.pdf

SWINBURNE UNIVERSITY OF TECHNOLOGY