

|  |
| --- |
| Cyber Alert |
| Victorian Government  Cyber Incident Response Service |

# Weekly AusCERT Threat Report

## **Wednesday, 16 November to Tuesday, 22 November**

## Purpose

This report provides insight into malware campaigns and other security vulnerabilities that may be relevant to Victorian government organisations.

## Threat reporting

* 7 malware variants and associated indicators of compromise (IOCs) were identified during the reporting period (16 November - 22 November).
* During the reporting period, emails from various phishing and malware campaigns observed across government and industry contained the following terms and keywords:

|  |
| --- |
|  |

* Malware by name:
* These phishing and malware campaigns often direct recipients to compromised/malicious websites or attachments.

## What can I do?

Victorian government organisations are encouraged to:

* **review the attached list of IOCs**
* **apply the relevant filtering/monitoring** at mail servers, web proxy servers, DNS servers and systems.

## Report all cyber security incidents

Victorian government organisations should report all cyber security incidents to the Cyber Incident Response Service on 1300 CSU VIC (1300 278 842) or email [**cybersecurity@dpc.vic.gov.au**](mailto:cybersecurity@dpc.vic.gov.au)**.**