techwell

Check Point®
SOFTWARE TECHNOLOGIES

Threat Intelligence Report

Australia

Threat Intelligence Summary

- An organization in Australia is being attacked on average 405 times per week in the last 6 months.
- The top malware in Australia is Trickbot, impacting 8% of organizations.
- The top malware list in Australia includes 2 Banking Trojans, 1 Trojan (Formbook), 1 Downloader (Zloader), 1 RAT (AgentTesla) and 1 Infostealer (AgentTesla).
- 79% of the malicious files in Australia were delivered via Email.
- The most common vulnerability exploit type in Australia is Remote Code Execution, impacting 58% of the organizations.
- Weekly impacted organizations by malware types:

	Cryptominer	Ransomware	Mobile	InfoStealer	Banking	Botnet
Australia Avg.	0.9%	0.9%	0.7%	0.8%	2.5%	4.9%
Global Avg.	3.8%	2.1%	1.2%	1.8%	5.1%	10.0%

Threat Landscape

- **Cloud adoption races ahead of security -** 2020 saw organizations' digital transformation programs advance by over five years in response to the pandemic, but public cloud security is still a major concern for 75% of enterprises. Also, over 80% of enterprises found their existing security tools don't work at all or have only limited functions in the cloud, showing that cloud security problems will continue into 2021.

- **Remote working is targeted -** Hackers ramped up 'thread hijacking' attacks on remote workers to steal data or infiltrate networks using the Emotet and Qbot trojans, which impacted 24% of organizations globally. Attacks against remote access systems such as RDP and VPN also increased sharply.

- **Double-extortion ransomware attacks rise -** In Q3 2020, nearly half of all ransomware incidents involved the threat of releasing data stolen from the target organization. On average, a new organization becomes a victim of ransomware every 10 seconds worldwide.

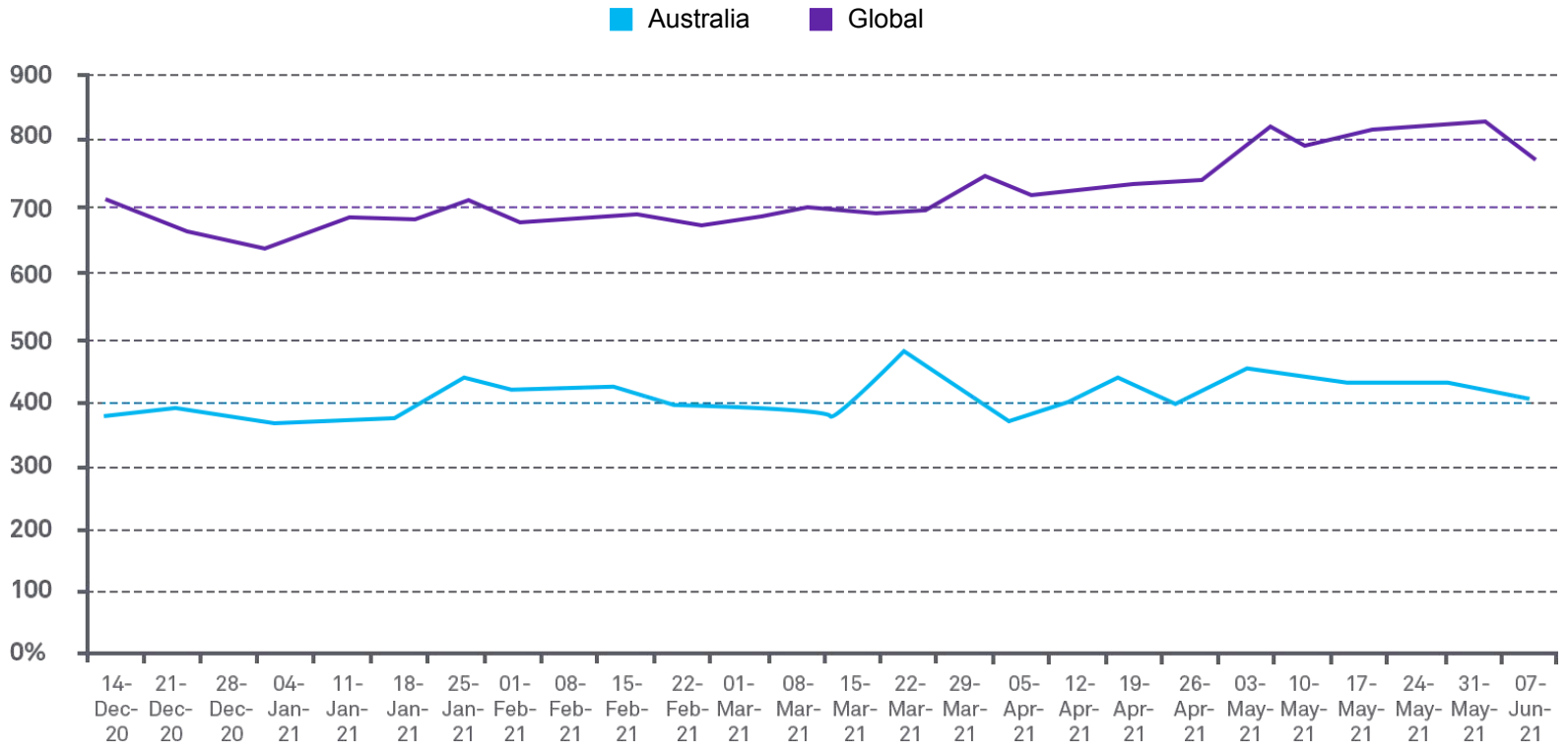
- **Attacks on healthcare sector become an epidemic -** In Q4 2020, CPR reported that cyber-attacks (especially ransomware attacks) on hospitals had increased by 45% worldwide, because criminals believe they are more likely to meet ransom demands due to the pressures from COVID-19 cases.

- **Mobiles are moving targets -** 46% of organizations had at least one employee download a malicious mobile application, which threatens their networks and data in 2020. The increased use of mobiles during global lockdowns has also driven growth in banking and information-stealing mobile Trojans.

Major attacks and data breaches – Australia

- Apr-21 - Click Studio, Australian software company developing the Passwordstate password manager, has suffered a data breach potentially exposing their 29,000 enterprise customers. Any customer who did In-Place Upgrades within the 26-hour attack timeframe would have had their credentials compromised and needs to replace them.
- Mar-21 - Eastern Health, one of Melbournes largest metropolitan public health services, has fallen victim to a cyber- attack, leaving many of its systems offline and forcing the facilities to postpone less urgent medical procedures.
- Feb-21 - Singaporean Telecom giant Singtel has fallen victim to an attack originating from a security flaw in a third-party file-transfer appliance. An Australian medical research institution has also suffered a similar attack. The software leveraged for the attack is Accellion, a legacy file-transfer platform.
- Nov-20 - North Korean surveillance campaign targeting the aerospace and defense sectors in Australia, Israel, Russia and India is spreading a new spyware called Torisma via fake job offers sent through social media.
- Jul-20 - Advisories from the UK, US, Canada and Australia warn that Russias Foreign Intelligence Service (SVR) has been conducting espionage operations to target COVID-19 research organizations. APT29 (aka Cozy Bear) is believed to be behind the operation, using the WellMess malware.
    - Check Point SandBlast provides protection against this threat (Trojan.Win32.WellMess)
- Jul-20 - Researchers have discovered almost 250,000 sets of personally identifiable information of users from the UK, Australia, South Africa, the US, Singapore and other countries exposed in a multi-stage bitcoin scam.

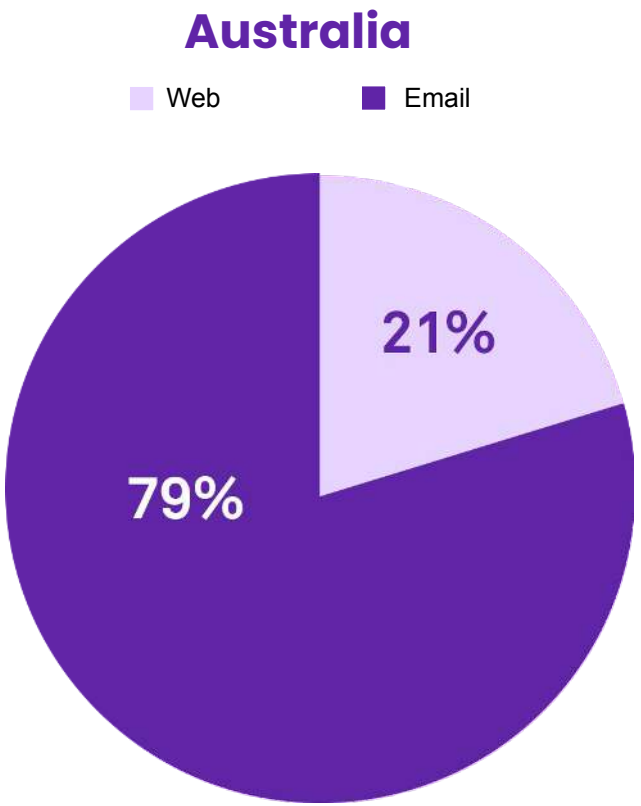
Attacks per Organization



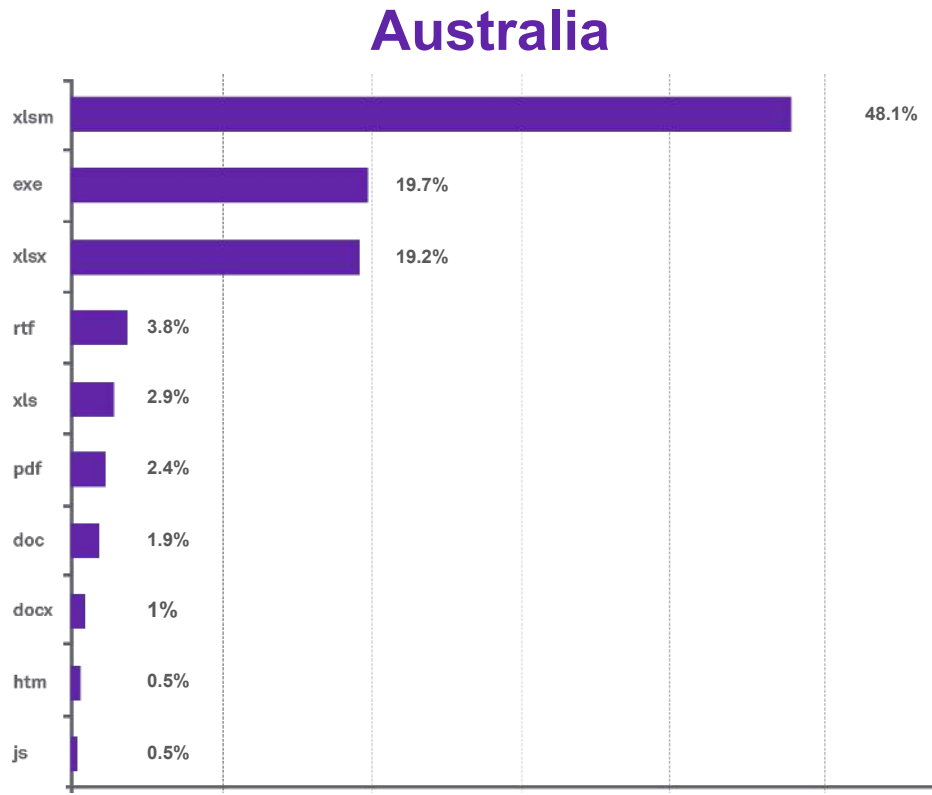
Top Malware – Australia

MALWARE FAMILY	AUSTRALIA IMPACT	GLOBAL IMPACT	DESCRIPTION
Trickbot	8%	8%	Trickbot is a modular Botnet and Banking Trojan that targets the Windows platform, mostly delivered via spam campaigns or other malware families such as Emotet. Trickbot sends information about the infected system and can also download and execute arbitrary modules from a large array of available modules: from a VNC module for remote control, to an SMB module for spreading within a compromised network. Once a machine is infected, the Trickbot gang, the threat actors behind this malware, utilize this wide array of modules not only to steal banking credentials from the target PC, but also for lateral movement and reconnaissance on the targeted organization itself, prior to delivering a company-wide targeted ransomware attack.
Formbook	2%	3%	First detected in 2016, FormBook is an InfoStealer that targets the Windows OS. It is marketed as MaaS in underground hacking forums for its strong evasion techniques and relatively low price. FormBook harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to orders from its C&C.
AgentTesla	2%	1%	First detected in 2016, FormBook is an InfoStealer that targets the Windows OS. It is marketed as MaaS in underground hacking forums for its strong evasion techniques and relatively low price. FormBook harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to orders from its C&C.
Icedid	2%	1%	IcedID is a banking Trojan which first emerged in September 2017. It spreads by mail spam campaigns and often uses other malwares like Emotet to help it proliferate. IcedID uses evasive techniques like process injection and steganography, and steals user financial data via both redirection attacks (installs a local proxy to redirect users to fake-cloned sites) and web injection attacks.
Zloader	1%	1%	Zloader is a banking malware which uses webinjects to steal credentials and private information, and can extract passwords and cookies from the victims web browser. It downloads VNC that allows the threat actors to connect to the victims system and perform financial transactions from the users device. First seen in 2016, the Trojan is based on leaked code of the Zeus malware from 2011. In 2020, the malware is very popular among threat actors and includes many new variants.

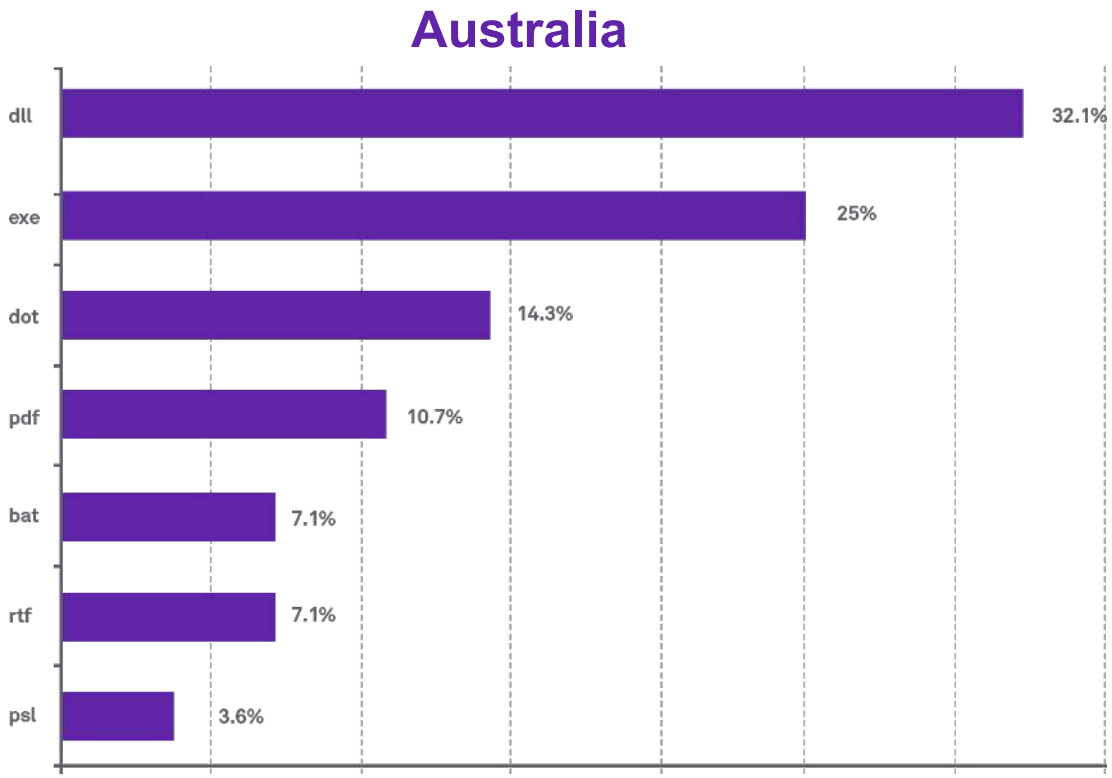
Attack Vectors for Malicious Files



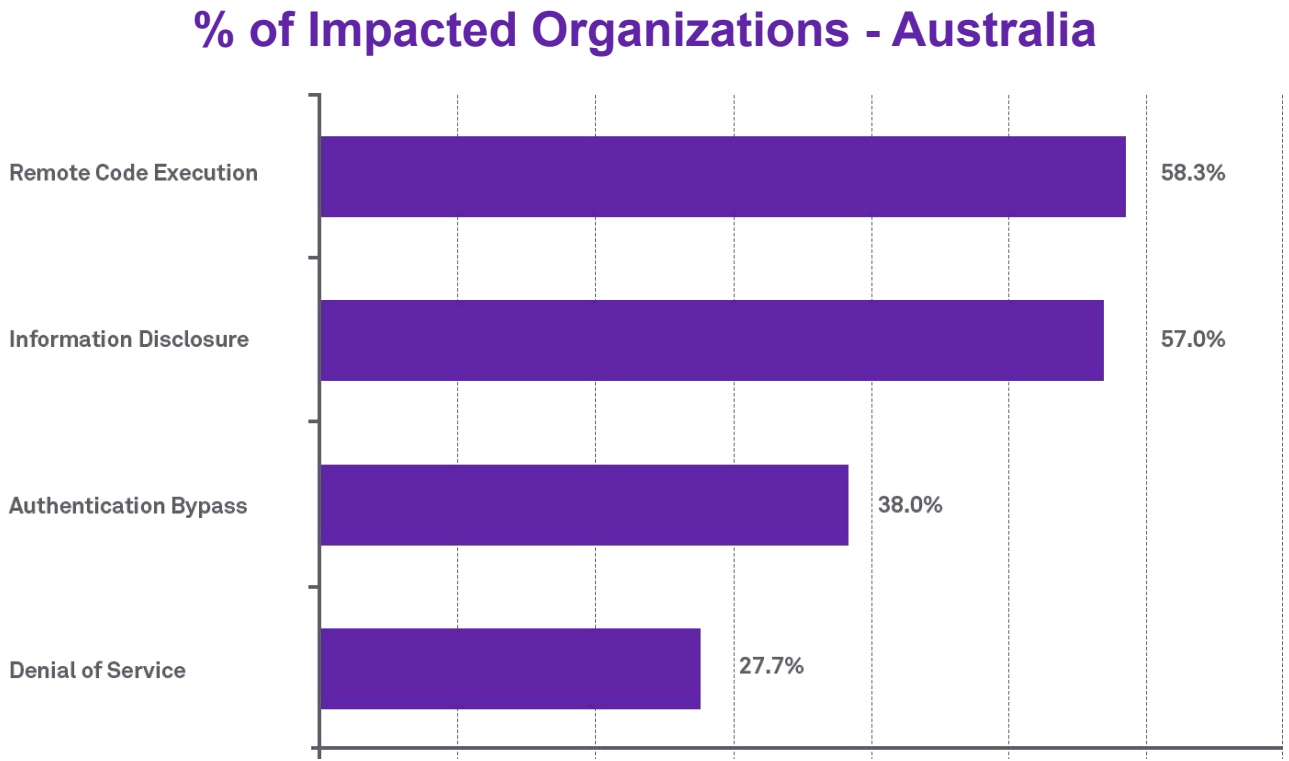
Top Malicious File Types, Email



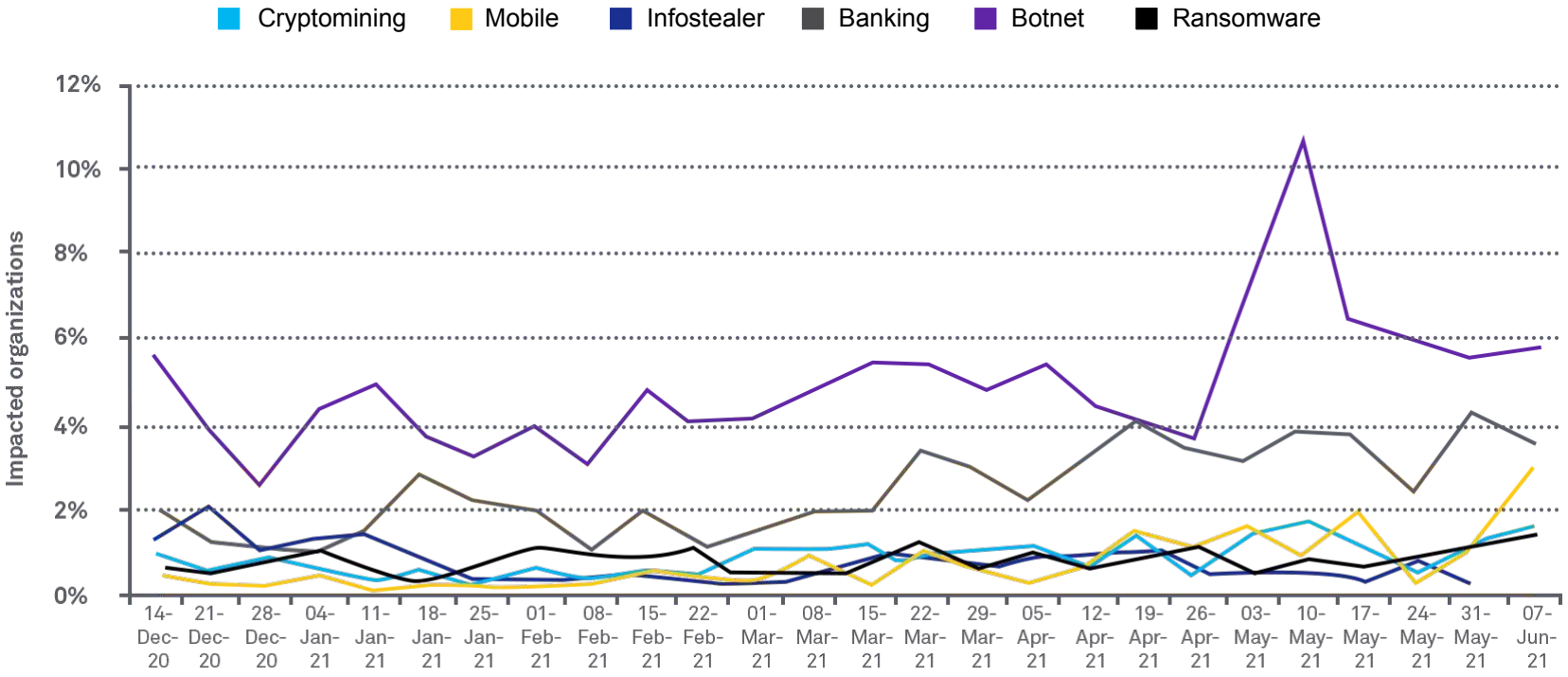
Top Malicious File Types, Web



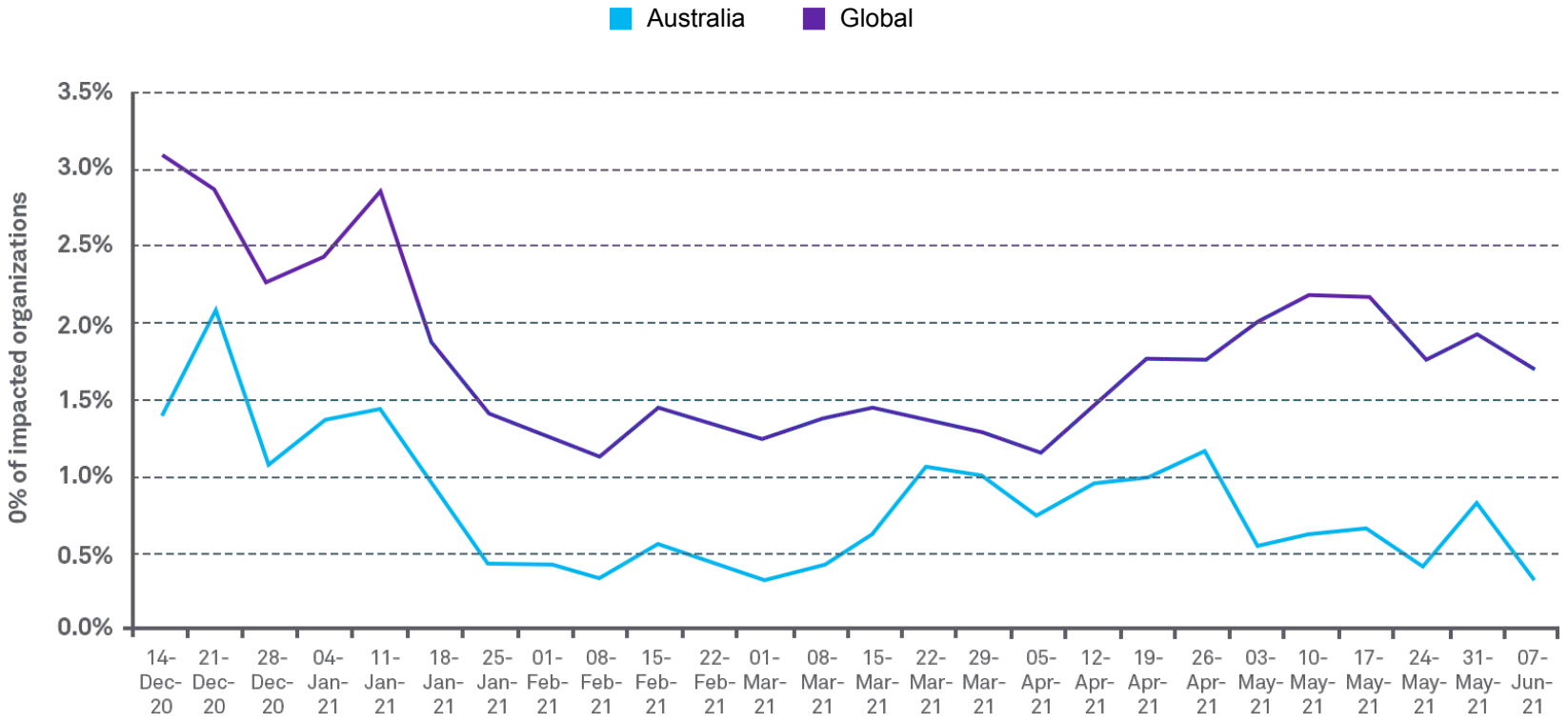
Top Vulnerability Exploit Types



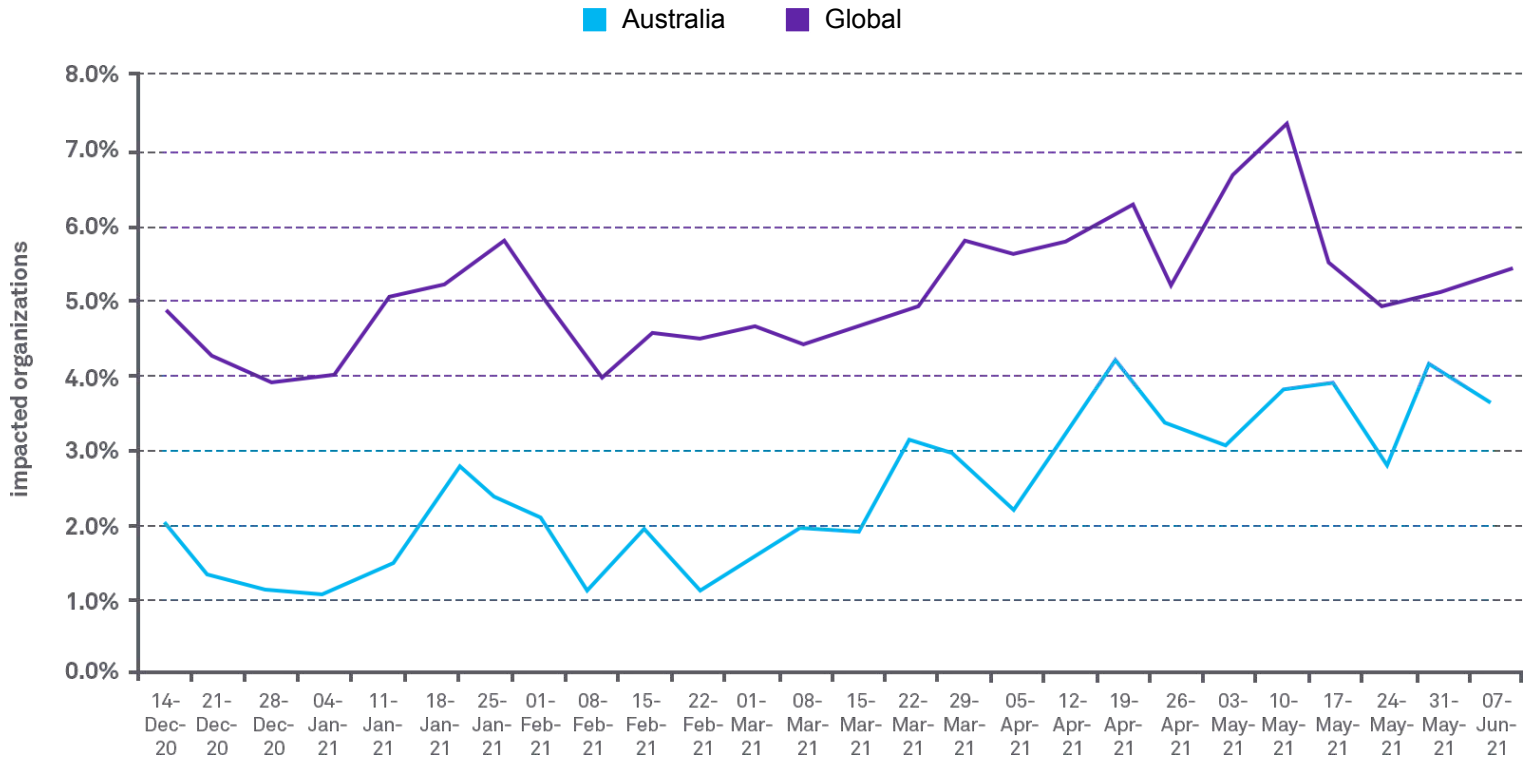
Major Malware Types trend - Australia



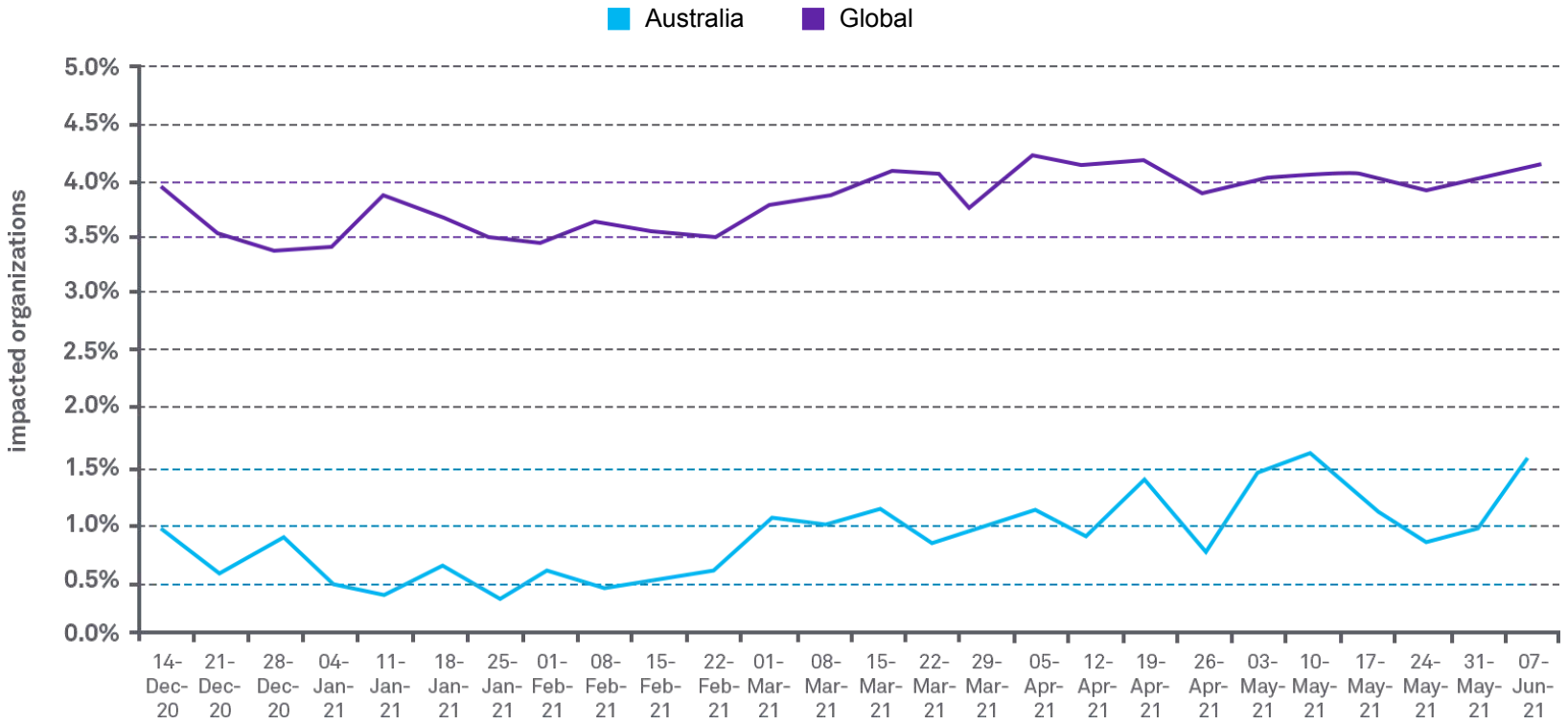
InfoStealer Attacks



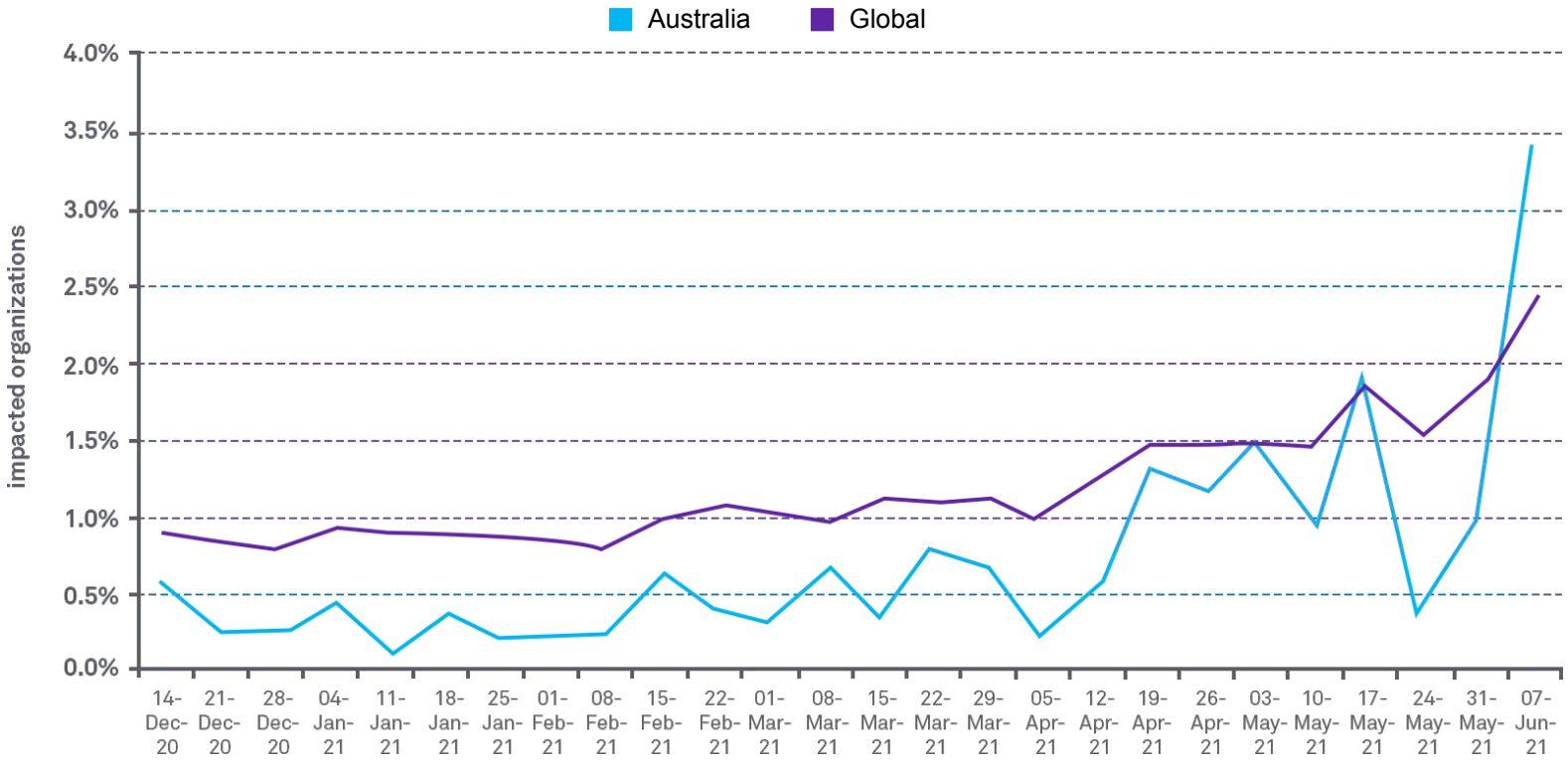
Banking Attacks



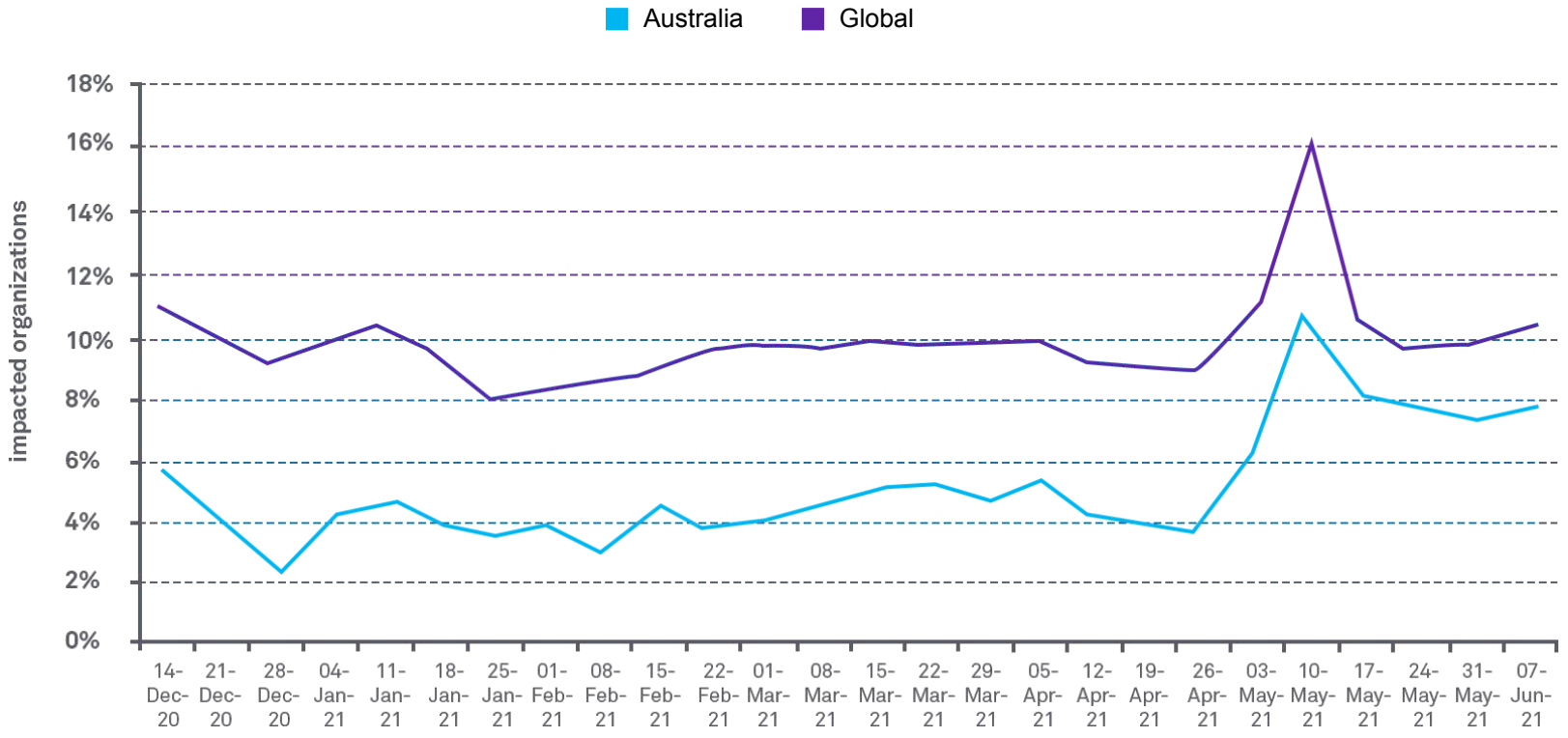
Cryptominer Attacks



Mobile Attacks



Botnet Attacks



Ransomware Attacks