ANOMALI

Cyber Threat Landscape Australasia Region

Source Summary Statement: *This product is based on research utilizing various open and private sources, proprietary sources, and intelligence vendors. This Cyber Threat Landscape report is based on collections and analysis that ended 03 SEP 2020.*

Overview

Anomali Threat Research has conducted analysis on numerous types of malicious cyber activity that affect the Australasia region. Due to the complex nature of sophisticated threat actors and groups, in addition to economic and geopolitical factors that can motivate cyberattacks, this report will be broken down into sections to highlight specific threats and risk. The most prolific threat groups and most-observed tactics, techniques, and procedures (TTPs) that are being used by threat actors will be discussed, as well as current geopolitical topics that contribute to and affect malicious cyber activity.

Australasia

For the purposes of this report, Australasia is defined as: American Samoa, Australia, Bougainville Island, Choiseul, Fiji, Malaita, New Britain, New Caledonia, New Ireland, New Georgia Islands, New Zealand, Niue, Papua New Guinea (including Papua and West Papua), Samoa, Santa Isabel Island, Solomon Islands, Tonga, Vanuatu, and Wallis and Futuna.

Geopolitics

As former British colonies sharing a common history, cultural outlook and language, Australia and New Zealand retain close ties with Western nations. These ties are particularly strong between Australia, New Zealand, the UK, and the US. The ANZUS is a formal military alliance between Australia, New Zealand and the US, this currently does not include a cyber dimension but could in the future.

These nations also operate within the Five Eyes (FVEY), an intelligence alliance encompassing Australia, Canada, New Zealand, the UK, and the US. This intelligence alliance was sparked by the joint declaration made in 1941 called The Atlantic Charter, later instituted in the United Kingdom - United States of America Agreement (UKUSA) signed by President Franklin Roosevelt and Prime Minister

Winston Churchill for objectives after the end of World War II.[1] This arrangement provides Australia and New Zealand with effective cyber intelligence sharing from each of the partners Signals Intelligence (SIGINT) but increases the potential for state-sponsored groups to target either country for strategic objectives. These are inherent risks of partnership, as adversaries know that specific entities hold valuable intelligence and will thus attempt to exploit weaknesses in one partner to compromise another (similar to a supply-chain attack). State-sponsored advanced persistent threat (APT) groups are often motivated by theft of this type of information.

In contrast to Western focused security policies, Australia and New Zealand's economic policies are heavily dependent on China. The People's Republic of China forms the largest trading partner for both countries, leading successive governments to adopt policies ranging from appeasement to full support of China's economic agenda. Australia is rich in natural resources that China needs for continued industrial development and New Zealand can provide access to Antarctica. Additionally, New Zealand is responsible for the foreign affairs of three territories in the South Pacific, potentially giving China four votes at international organisations when and if China can convince New Zealand to support Beijing's position.[2] Recently, tensions have risen as the scale of China's political meddling and corporate espionage has become more apparent. This has the potential to escalate into a full diplomatic incident.

Australasia's geographical location to strategic areas, such as important trade routes in Indonesia, and relatively close proximity to nuclear powers (China, India, and Pakistan) contributes to tension in the region. Australia, which conducts most of its trade with China, is likely of increased interest to China-sponsored APTs target countries China trades with.

The South China Sea is an example of these years-long growing tensions China building up its military presence with artificial-island outposts.[3] These military movements often trigger the US and its allies to increase their presence in the area in response, further escalating tensions.[4] There are also conflicts with China's territorial claim (known as the nine-dash line) because parts of the valuable area are also claimed by Brunei, Malaysia, the Philippines, Taiwan, and Vietnam.[5] The South China Sea may hold the most attention because of the number of countries involved, some of which have attributed APT groups (China, Vietnam) that likely conduct cyber reconnaissance on countries located in or near the region, as well as those with vested interest in the area.[6] China has targeted entities involved in its Belt and Road initiative in previous campaigns and will almost certainly continue to do so.

Cyber Landscape

The cyber threat landscape in Australasia is dominated by the Australian continent, and this trend is continuing, as of this writing. In addition, there are five Computer Emergency Response Teams (CERTs) in the region located in the following countries: Australia, New Zealand, Papua New Guinea, Tonga, Vanuatu.[7] In late June 2020, the Australian government announced that it would be investing 1.35 billion Australian dollars (approximately $930 million USD) into its cyber abilities in what appears to be a direct response to rising cyberattacks attributed to the Chinese government.[8] The funds will be used to increase cyber warfare and SIGINT capabilities by hiring cybersecurity professionals.[9] Australia's government stated in August 2020 that it plans to invest $1.67 billion (USD) over the next 10 years "to achieve our vision of creating a more secure online world for Australians."[10] Businesses and individuals are conducting more

activity online as the COVID-19 pandemic affects the world. However, even prior to the Coronavirus, Australia began to notice how small to medium-sized businesses were beginning to open their own websites for online sales.[11] This creates more potential avenues for threat actors to make an illicit profit. Australia saw approximately six cyber incidents per day from July 1, 2019 through June 30, 2020, and the Australian Cyber Security Centre (ACSC) responded to 2,266 cyber incidents during that timeframe.[12] These incidents do not include the ones deferred to the police or other organizations, therefore, the actual amount of incidents is very likely much higher.[13]

Other governments in the region have also begun implementing cyber strategy initiatives, or have acknowledged the risk of cybercrime in their country. New Zealand pledged $20 million in 2019 to increase CERT funding as well as to help develop other pacific nations cyber response capabilities.[14] Sharing of Cyber Threat Intelligence (CTI) and resources is crucial because regions of the world can often face similar threats and challenges from actors located in the area. For example, the Director of Public Prosecution of the Solomon Islands began discussing the lack of ability to prosecute cybercrimes in 2017, and beginning with Information and Communications Technology (ICT) policies would be crucial to assist in legal action.[15]

While the COVID-19 pandemic has brought unprecedented changes to society, the effects on the cyber threat landscape have remained relatively minor.[16] Some of the changes in the cyber threat landscape post-COVID-19 include:[17]

- A shift from working in the office to remote locations exposes enterprise networks to a new type of threat.
- The use of COVID-19 topics and increase in health-themes for social engineering.
- Increase in targeting of entities working in healthcare and healthcare-related manufacturing with cyberespionage objectives. In addition, these critical organizations are also increasingly vulnerable to ransomware attacks.
- Heightened tensions with China.

Threat Actors and Groups

There are multiple active and historic APT groups and threat actors that target entities and individuals with various motivations and objectives. While this section seeks to highlight some of the most concerning actors and groups associated with Australasia, a larger list of threat groups that target, or are located in, Australasia can be found in Appendix A. Awareness of these actors and their TTPs can assist in a proactive, rather than reactive, cyber strategy.

APT32

Aliases: *OceanLotus, SeaLotus*

APT32 has been conducting cyberespionage campaigns since at least 2013, with a particular focus on individuals and businesses with ties to Vietnam.[18] FireEye researchers contend that the group's malicious activity is aligned with Vietnamese government interests. The group uses their own unique malware in addition to open source tools to attack their targets. The combination of malware and tools allows the group to maintain presence on an infected machine or system, as well as moving laterally through a network.[19]

APT32's primary attack methods are phishing and spearphishing emails with social engineering content. The group uses ActiveMimes files that contain OLE files attachments with malicious macros. If they are enabled, malicious payloads will begin downloading from command and control (C2) servers. The group has been identified

to use various malicious payloads that can be dynamically updated in memory. Furthermore, researchers observed that the group performs sophisticated reconnaissance on their targets in order to identify which machines and systems they want to compromise.[20]

APT41

APT41 is a China-based group that have carried out financially-motivated attacks from as early as 2012, however, they have become more known for their state-sponsored campaigns with activity as early as 2013.[21] The group's earliest activity focused on financial gain and targeted organizations in the video game industry by gaining access to game development environments. The group's financially-motivated activities focused on stealing source code and digital certificates, virtual currency mining, and attempting to deploy ransomware within these game environments. The TTPs used and campaigns carried out by APT41 for financial motivations were leveraged for state-sponsored attacks.[22] From 2013 onwards, APT41 was observed concurrently conducting cyberespionage operations against high-value industry sectors along with their previous financially-motivated attacks towards the games industry.[23]

APT41 is unique in their operation compared to other APT groups because they are conducting financially-motivated cybercrime and espionage campaigns simultaneously.[24] This is rare, as most espionage focused groups will only conduct nation-state level campaigns assigned to them.

Carbanak

Aliases: *Anunak*, *Carbon Spider*, *TelePort Crew*

The Carbanak group, which has been active since at least 2014, is primarily focused on attacking banks and companies in, and related to, the retail industry.[25] Initially, the group focused only on attacking Russian banks, but in August 2015 they reportedly expanded their target scope to banks, hospitality, manufacturers of Point of Sale (PoS) systems, retailers, and restaurant industries worldwide.[26] They are a sophisticated group that will compromise vendors employed by the primary target to use the vendor's legitimate emails in spearphishing campaigns.

The Carbanak group typically attempts to obtain a foothold in an organization via spearphishing emails that are distributed using stolen email credentials. The credentials used to make the phishing emails appear authentic usually belong to coworkers or third parties trusted by the targeted organizations. The observed infection vectors in emails have been Microsoft Word documents with known vulnerabilities, Rich Text Format (RTF) documents with embedded Object Linking and Enabling (OLE) objects containing VBScripts, and Control Panel items (CPL files).[27] To increase the chances of success, they register similar looking domains, known as typosquatting, and clone the legitimate websites of the spoofed vendor to serve the malware. In some cases, the initial infection has been from Null, RedKit, or Neutrino Exploit Kits via a drive-by-download attack.[28]

Elderwood

Aliases: *Elderwood Gang*, *Sneaky Panda*, *Beijing Group*

The threat group, Elderwood, is reportedly a China-based group whose malicious activities were first identified in 2012.[29] The group is motivated by the theft of proprietary information. Elderwood uses a platform, the group's namesake dubbed by researchers in 2014, that contains various exploits utilized in spearphishing and watering-hole campaigns.[30] According to Symantec researchers, Elderwood activity consists of different sub-groups, each with their own specific targeting. These groups all share a common zero-day exploit

supplier, primarily affecting Adobe Flash and Internet Explorer through the use of the Elderwood platform. The Elderwood Gang was believed to be behind the attack disclosed publicly in January 2010 that affected Adobe Systems, Google, and Juniper Networks and approximately 30 other companies, called Operation Aurora.[31] Elderwood actors were found to have utilized eight zero-day vulnerabilities that affected Adobe Flash and Internet Explorer during this campaign.[32]

Elderwood actors conduct specific targeting through spearphishing and watering hole attacks with the objective of installing information-stealing malware. The Elderwood platform was found to be easily configured to launch automated attacks so that individuals of non-technical backgrounds could still conduct malicious activity.[33] The Elderwood Gang displayed patience in Operation Aurora while conducting watering-hole attacks, often compromising the website and waiting for months before the infection took place. Once a target visited the website, a zero-day exploit launched and infected the machine with a trojan.[34]

Other threat groups and malware families were identified by researchers through reverse-engineering the Elderwood platform. These groups and their associated malware include the following:[35]

- Hidden Lynx – Zxshell
- Linfo/Icefog – Linfo, Hormesu
- Sakurel – Sakurel
- Vidgrab – Vidgrab, Jolob

Lazarus Group

Aliases: *Hidden Cobra, Labyrinth Chollima, Group 77*

The Lazarus Group APT is believed to be based in the Democratic People's Republic of Korea (DPRK) and has been active since at least 2009. Lazarus Group is assessed to be composed of operatives from "Bureau 121" (121국), the cyber warfare division of North Korea's Reconnaissance General Bureau.[36] The Reconnaissance General Bureau was formed due to a reorganization in 2009 but we do not have insight into its exact structure due to North Korea's denial and deception tactics. Bureau 121 is North Korea's most important cyber unit that is used for both offensive and defensive operations.

The most common initial vector for Lazarus Group is spearphishing emails. Lazarus Group will use decoy documents that are likely of interest to the intended document. Commonly these decoy documents have political themes such as media reports discussing South Korean parliamentary elections, or information about government conferences.[37] These documents have either exploited macros or have malicious attachments. In other cases Lazarus Group has been noted to exploit vulnerabilities in the indigenous Korean Hangul Word Processor (한/글), using ".hwp" decoy documents, which is a popular attack vector as 80% of the documents attached to South Korean and public agencies websites are HWP files.[38]

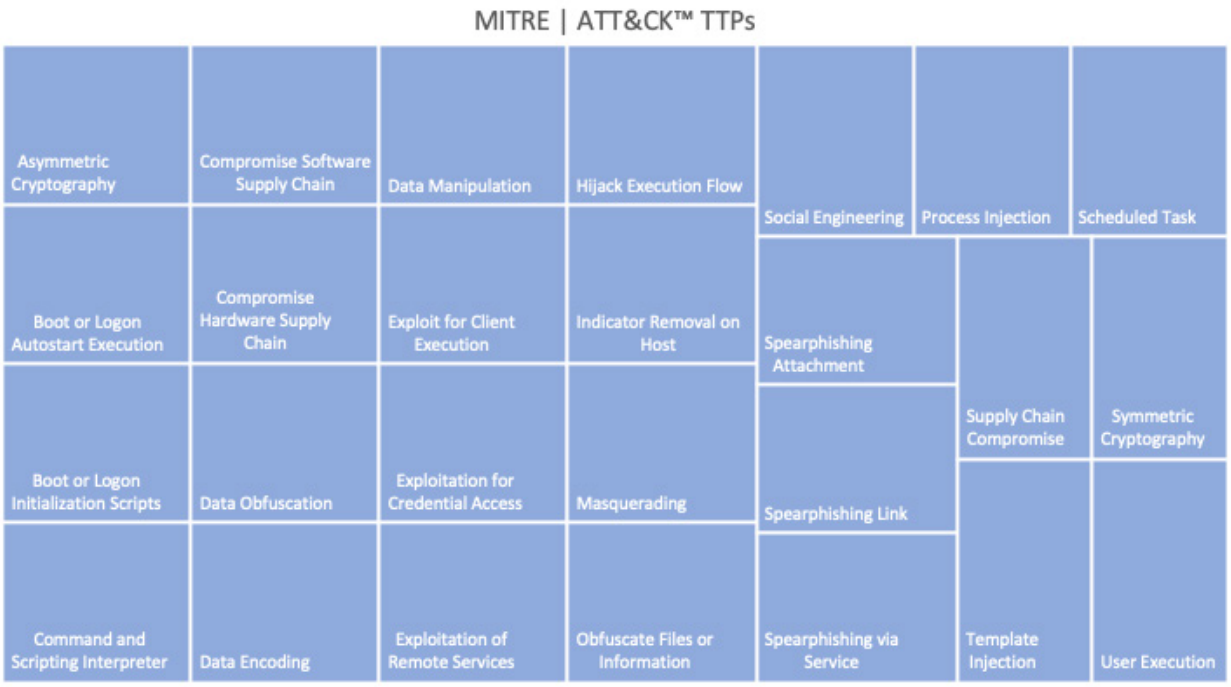

Figure 1. Commonly used APT TTPs

Common TTPs

Malicious activity conducted by threat actors can vary amongst different types of groups. The different types of groups, for the purposes of this section, can be broken down into three categories: APT, Cybercriminal, and Hacktivist. The different motivations by threat actors in these categories result in different common attack vectors and TTPs utilized by threat actors. The TTPs listed in subsequent sections are not intended to be seen as a comprehensive list, as threat actors utilize too many TTPs and some overlap amongst them is expected.

APT

APTs typically attempt to engage in long-term cyberespionage campaigns intent on information theft. That information can be owned by a variety of entities, including but not limited to financial services, banking, education, government organizations, military, and technology, among others.

- Asymmetric Cryptography
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Command and Scripting Interpreter
- Compromise Software Supply Chain
- Compromise Hardware Supply Chain
- Data Obfuscation
- Data Encoding
- Data Manipulation
- Exploit for Client Execution
- Exploitation for Credential Access
- Exploitation of Remote Services
- Hijack Execution Flow
- Indicator Removal on Host
- Masquerading
- Obfuscate Files or Information
- Social Engineering
- Process Injection
- Scheduled Task
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Symmetric Cryptography
- Template Injection
- User Execution

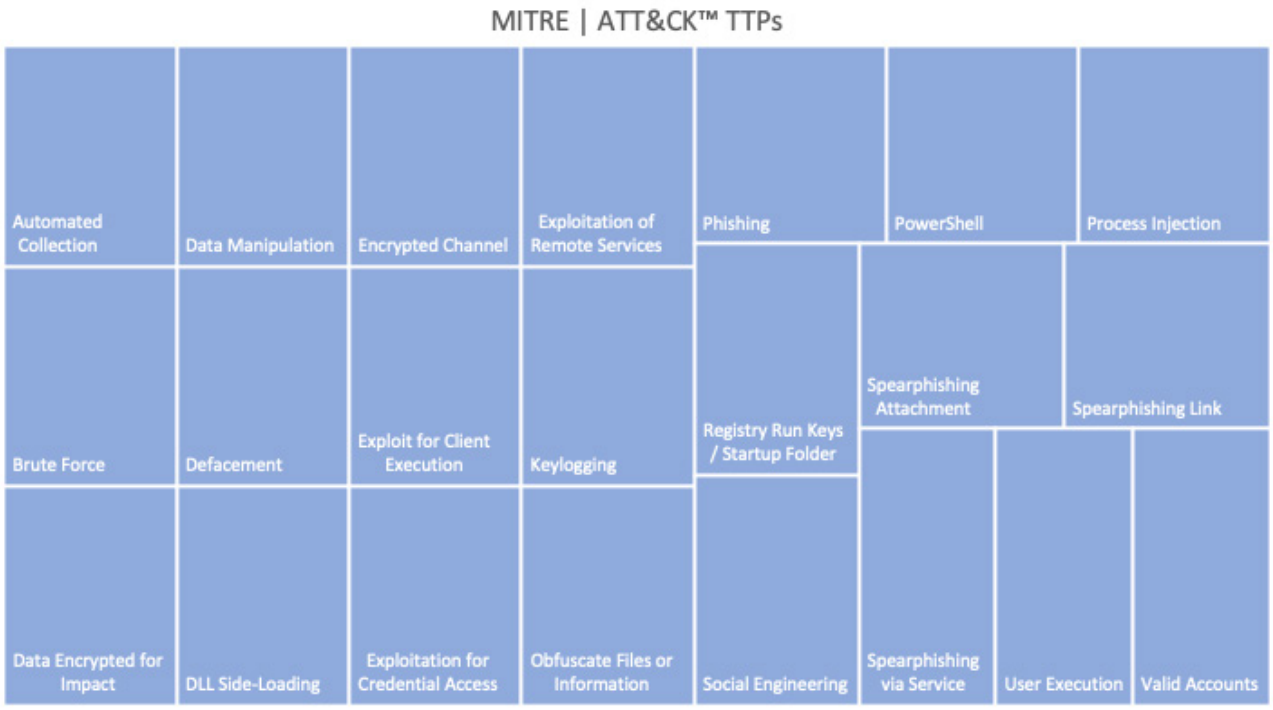

Figure 2. Common Cybercriminal TTPs

Cybercriminal

Cybercriminals are usually financially-motivated and will go to great lengths to accomplish their objectives. Their sophistication can rival state-sponsored APTs in some instances.

- Automated Collection
- Brute Force
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- DLL Side-Loading
- Encrypted Channel
- Exploit for Client Execution
- Exploitation for Credential Access
- Exploitation of Remote Services
- Keylogging
- Obfuscate Files or Information
- Phishing
- PowerShell
- Process Injection
- Registry Run Keys / Startup Folder
- Social Engineering
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- User Execution
- Valid Accounts

Hacktivist

Hacktivist groups are typically unsophisticated and conduct cyberattacks intended to bring attention to a specific cause or event. These attacks usually consist of Distributed Denial of Service (DDoS), phishing, ransomware, and website defacement attacks.

- Brute Force
- Data Encrypted for Impact
- Defacement
- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Phishing
- Social Engineering

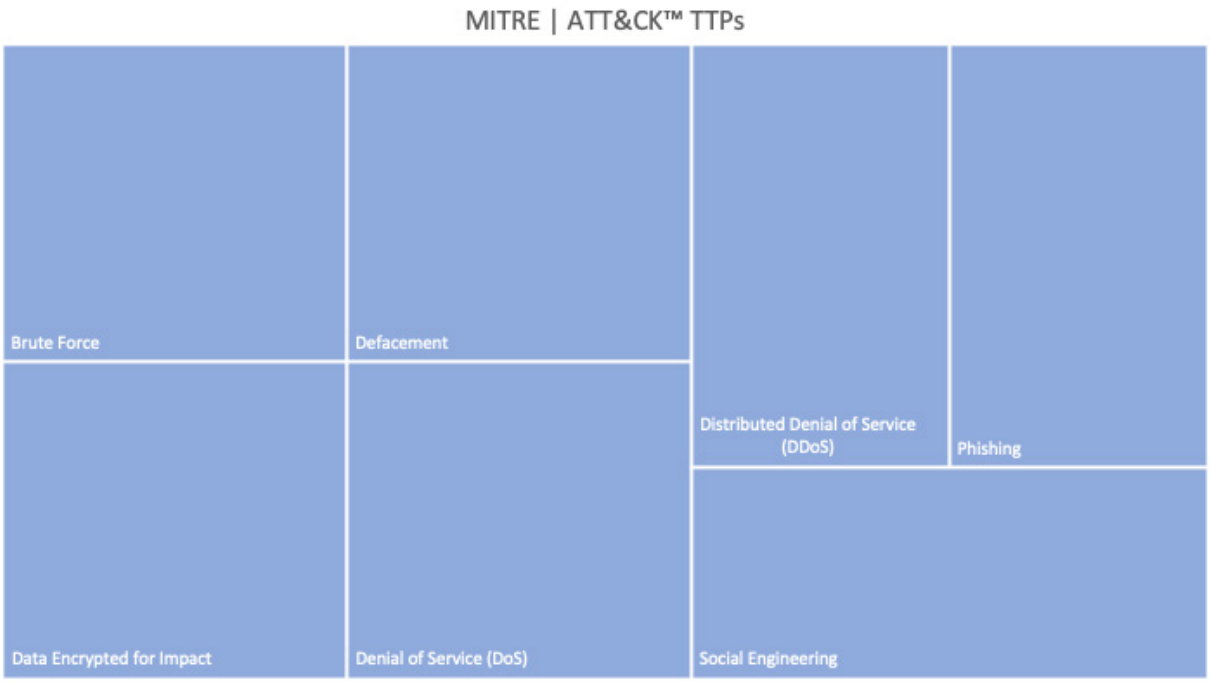

Figure 3. Common Hacktivist TTPs

Industry Targeting

As mentioned in previous sections, targeting depends on the motivations and objectives of the threat actor or group. There have been numerous cyber incidents that affected the Australasia region, however, most that are reported in open sources only affect Australia and New Zealand. However, in many cases of cyberattacks, the motivation is often monetary. Therefore, industries with high volumes of online traffic and transactions are often targeted because of the direct financial involvement. In addition, strategic interests of state-sponsored actors will target governments and related entities, military, and technology companies to steal sensitive information. Furthermore, some groups will also target organizations to steal data that can be sold on underground markets.

According to the Australia Cyber Security Centre (ACSC), cyberattacks targeting Australia were found to primarily be financially-motivated throughout 2019 and affect one-in-three adults.[39] However, from July 1, 2019 to June 30, 2020, the ACSC found that the Australian government was the most heavily-targeted sector, followed by state governments.[40] The list created by the ACSC from most to least targeted is shown below:[41]

1. Australian Government
2. Government (state/territory)
3. All other affected sectors
4. Other
5. Individuals
6. Health
7. Education and research
8. Banking and financial services
9. Information technology
10. Retail
11. Legal and professional services
12. Water
13. Communications
14. Transport
15. Mining and resources

New Zealand faces similar threats to other countries in the Australasia region, primarily the China-based APT nexus and cybercrime. From April 2019 through April 2020, the New Zealand CERT found that scams and fraud constituted most of the malicious cyber activity.[42] In addition, the New Zealand Stock Exchange (NZX) was struck with DDoS attacks four days in a row, which caused disruption and monetary losses in an "offshore" cyberattack.[43] The overall financial losses were approximately $44 million (USD) from 2017-2020, with approximately $7.8 million (USD) lost as late June 2020.[44] The top five sectors per reported incident to the CERT NZ from approximate most to least consist of the following:[45]

- Financial and Insurance services
- Technology
- Education and Training
- Retail Trade and Accommodation
- Professional, Scientific and Technical

Conclusion

The Australasia region is targeted by threat actors and groups for numerous reasons. These include: intelligence relations with Western governments, and geographical location to areas with high volumes of trade and strategic importance. Threat actors of varying levels of sophistication specifically target the region, in addition to opportunistic cyberattacks. Furthermore, awareness of these actors, their motivations, and their TTPs can assist individuals and organizations in taking proactive mitigation steps to protect themselves from potential cyberattacks.

Endnotes

1 "1941: The Atlantic Charter," United Nations, accessed August 31, 2020, https://www.un.org/en/sections/history-united-nations-charter/1941-atlantic-charter/index.html.

2 Professor Anne-Marie Brady, "Magic Weapons: China's political influence activities under Xi Jinping," Wilson Center, accessed August 31, 2020, June 7, 2017, https://www.wilsoncenter.org/sites/default/files/media/documents/article/magic_weapons.pdf, 12

3 "Explainer | South China Sea, the dispute that could start a military conflict," South China Morning Post, accessed August 31, 2020, published August 11, 2020, https://www.scmp.com/news/china/diplomacy/article/3096897/south-china-sea-dispute-could-start-military-conflict.

4 "Global Conflict Tracker," Council on Foreign Relations, accessed August 31, 2020, https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea.

5 Kevin Varley, et al., "Fight Over Fish Fans a New Stage of Conflict in South China Sea," Bloomberg, accessed September 1, 2020, published September 1, 2020, https://www.bloomberg.com/graphics/2020-dangerous-conditions-in-depleted-south-china-sea/; "Explainer | South China Sea, the dispute that could start a military conflict," South China Morning Post.

6 Fred Plan, et al., "APT40, Examining a China Nexus Espionage Actor," FireEye Blog, accessed September 1, 2020, published March 4, 2019, https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html; FireEye Threat Intelligence, "SOUTHEAST ASIA: AN EVOLVING CYBER THREAT LANDSCAPE," FireEye Singtel, accessed September 1, 2020, published March 2015, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf, 3.

7 "The Papua New Guinea Computer Emergency Response Team (CERT)," PNGCERT, accessed September 1, 2020, https://www.pngcert.org.pg/; "CERT Australia," Australian Cyber Security Centre, accessed September 1, 2020, https://www.cyber.gov.au/acsc/view-all-content/glossary/cert-australia; "Responding to cyber security threats in Vanuatu," CERT VU, accessed September 1, 2020, https://cert.gov.vu/; "Mission Statement," CERT Tonga, accessed September 1, 2020, published April 19, 2018, https://www.cert.gov.to/.

8 Damien Cave, "Australia Spending Nearly $1 Billion on Cyberdefense as China Tensions Rise," The New York Times, accessed September 1, 2020, published June 30, 2020, https://www.nytimes.com/2020/06/30/world/australia/cyber-defense-china-hacking.html.

9 Renju Jose, "Australia to invest more in cyber security, hire specialists," Reuters, accessed September 1, 2020, published June 29, 2020, https://www.reuters.com/article/australia-cyber/australia-to-invest-more-in-cyber-security-hire-specialists-idUSL4N2E64FV#:~:text=SYDNEY%2C%20June%2030%20(Reuters),hacking%20attempts%20against%20the%20country; Australian Government, "AUSTRALIA'S CYBER SECURITY STRATEGY, 2020," Australia's Cyber Security Strategy 2020, accessed September 1, 2020, published August 6, 2020, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf, 18.

10 Australian Government, "AUSTRALIA'S CYBER SECURITY STRATEGY, 2020," Australia's Cyber Security Strategy 2020, 6.

11 Australian Government, "AUSTRALIA'S CYBER SECURITY STRATEGY, 2020," Australia's Cyber Security Strategy 2020, 10; Australian Government, "The Australian Cyber Security Centre Threat Report 2015," Australian Cyber Security Centre, accessed September 1, 2020, published 2015, https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2015.pdf, 5.

12 Australian Government, "AUSTRALIA'S CYBER SECURITY STRATEGY, 2020," Australia's Cyber Security Strategy 2020, 10.

13 Ibid.

14 National Security Group, "New Zealand's Cyber Security Strategy 2019," Department of the Prime Minister and Cabinet, accessed September 1, 2020, published July 2, 2019, https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019.

15 Milton Ragaruma, "Solomon Islands vulnerable to cyber crime," Island Sun, accessed September 1, 2020, published September 20, 2017, https://theislandsun.com.sb/solomon-islands-vulnerable-cyber-crime/.

16 Gage Mele, Parthiban R., and Tara Gould, "COVID-19 Themes Are Being Utilized by Threat Actors of Varying Sophistication," Anomali Threat Research Blog, accessed September 1, 2020, published March 23, 2020, https://www.anomali.com/blog/covid-19-themes-are-being-utilized-by-threat-actors-of-varying-sophistication; Tara Gould, Gage Mele, Parthiban Rajendran, and Rory Gould, "Anomali Threat Research Identifies Fake COVID-19 Contact Tracing Apps Used to Download Malware that Monitors Devices, Steals Personal Data," Anomali Threat Research Blog, accessed September 1, 2020, published June 10, 2020, https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data; Sandra Joyce, "Limited Shifts in the Cyber Threat Landscape Driven by COVID-19," FireEye Blog, accessed September 1, 2020, published April 8, 2020, https://www.fireeye.com/blog/threat-research/2020/04/limited-shifts-in-cyber-threat-landscape-driven-by-covid-19.html.

17 Gage Mele, Parthiban R., and Tara Gould, "COVID-19 Themes Are Being Utilized by Threat Actors of Varying Sophistication," Anomali Threat Research Blog; Tara Gould, Gage Mele, Parthiban Rajendran, and Rory Gould, "Anomali Threat Research Identifies Fake COVID-19 Contact Tracing Apps Used to Download Malware that Monitors Devices, Steals Personal Data," Anomali Threat Research Blog; Sandra Joyce, "Limited Shifts in the Cyber Threat Landscape Driven by COVID-19," Fireeye Blog.

18 Scott Henderson, et al., "Vietnamese threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage," FireEye Blog, accessed August 31, 2020, published April 22, 2020, https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html.

19 https://www.wired.com/2017/05/close-look-notorious-apt32-hacking-group-action/

20 Nick Carr, "Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations," FireEye Blog, accessed August 31 2020, published May 14, 2017, https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html.

21 FireEye, "Double Dragon, APT41, a dual espionage and cyber crime operation", accessed November 11, 2019, published August 07, 2019, https://content.fireeye.com/apt-41/rpt-apt4.

22 Ibid.

23 Ibid.

24 Ibid.

25 "ANUNAK: APT AGAINST FINANCIAL INSTITUTIONS," Group-IB and Fox-IT, accessed March 5, 2019, published December 2014, https://www.group-ib.com/resources/threat-research/Anunak_APT_against_financial_institutions.pdf, 2-3.

26 Tom Spring, "Carbanak Attacks Shift to Hospitality Sector," Threatpost, accessed March 5, 2019, published November 15, 2016, https://threatpost.com/carbanak-attacks-shift-to-hospitality-sector/121966/.

27 Nicholas Griffin, "Carbanak Group uses Google for malware command-and-control," Forcepoint Blog, accessed March 5, 2019, published January 17, 2017, https://www.forcepoint.com/blog/x-labs/carbanak-group-uses-google-malware-command-and-control.

28 GReAT, "The Great Bank Robbery, the Carbanak APT," Securelist, accessed March 5, 2019, published February 16, 2015, https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/.

29 "How the Elderwood Platform is Fueling 2014's Zero-Day Attacks," Broadcom, accessed April 13, 2020, published May 5, 2014, https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=26ca56e9-b2ca-4939-8b7a-dc6c1905a753&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

30 Ibid.

31 Pierluigi Paganini, "Elderwood project, who is behind Op. Aurora and ongoing attacks?" Security Affairs, accessed April 13, 2020, published September 9, 2012, http://securityaffairs.co/wordpress/8528/hacking/elderwood-project-who-is-behind-op-aurora-and-ongoing-attacks.html.

32 "How the Elderwood Platform is Fueling 2014's Zero-Day Attacks," Broadcom.

33 Ibid.; Mark Clayton, "Stealing US business secrets: Experts ID two huge cyber 'gangs' in China," The Christian Science Monitor, accessed April 13, 2020, published September 14, 2012, https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China.

34 Ibid.

35 Ibid.

36 "LAZARUS ARISEN," Group-IB Blog, accessed November 13, 2019, published May 30, 2017, https://www.group-ib.com/blog/lazarus.

37 CH Lei, et al., "Lazarus Campaign Uses Remote Tools, RATANKBA, and More, Trend Micro, accessed November 13, 2019, published January 24, 2018, https://www.trendmicro.com/en_us/research/18/a/lazarus-campaign-targeting-cryptocurrencies-reveals-remote-controller-tool-evolved-ratankba.html.

38 "Alert (TA17-164A)," US-CERT, accessed November 13, 2019, published June 13, 2017, https://us-cert.cisa.gov/ncas/alerts/TA17-164A.

39 Xue Yin Peh, "Australia Cyber Threat Landscape Report (H1 2019)," Digital Shadows Blog, accessed August 31, 2020, published October 29, 2019, https://www.digitalshadows.com/blog-and-research/australia-cyber-threat-landscape-report-h1-2019/; Australian Government, "AUSTRALIA'S CYBER SECURITY STRATEGY, 2020," Australia's Cyber Security Strategy 2020, 13.

40 Australian Government, "AUSTRALIA'S CYBER SECURITY STRATEGY, 2020," Australia's Cyber Security Strategy 2020, 12.

41 Ibid., 14.

42 CERT NZ, "2020 half year summary," New Zealand Government, accessed September 2, 2020, published 2020, https://www.cert.govt.nz/about/quarterly-report/2020-half-year-summary/.

43 Alicia Hope, New Zealand Stock Exchange Shut Down by DDoS Attack," CPO Magazine, accessed September 3, 2020, published September 3, 2020, https://www.cpomagazine.com/cyber-security/new-zealand-stock-exchange-shut-down-by-ddos-cyber-attack/.

44 CERT NZ, "2020 half year summary," New Zealand Government.

45 Ibid.

46 Adam Meyers, "Who is Anchor Panda," Crowdstrike Blog, accessed September 3, 2020, published March 22, 2013, https://www.crowdstrike.com/blog/whois-anchor-panda/.

47 "THREAT GROUP CARDS: A THREAT ACTOR ENCYCLOPEDIA," ThaiCERT, accessed August 30, 2020, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf, 22; Henry Belot, "Chinese hackers targeting Australian law firms, and industry specialist warns," ABC News, accessed August 30, 2020, published November 30, 2017, https://www.abc.net.au/news/2017-12-01/chinese-hackers-targeting-australian-law-firms/9213520.

48 Ian Ahl, "Privileges and Credentials: Phished at the Request of Counsel," FireEye Blog, accessed August 30, 2020, published June 6, 2017, https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html.

49 "APT29," ThreatStream, https://ui.threatstream.com/actor/12600.

50 "APT32," ThreatStream, https://ui.threatstream.com/actor/1465.

51 "APT41," ThreatStream, https://ui.threatstream.com/actor/28033.

52 "Carbanak," ThreatStream, https://ui.threatstream.com/actor/1688.

53 "Deep Panda," ThreatStream, https://ui.threatstream.com/actor/1724.

54 GReAT, "THE DESERT FALCONS TARGETED ATTACKS, Kaspersky Lab, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064309/The-Desert-Falcons-targeted-attacks.pdf, 4.

55 "Elderwood," ThreatStream, https://ui.threatstream.com/actor/14721.

56 "Threat Group-3390," MITRE ATT&CK, https://attack.mitre.org/groups/G0027/.

57 Catalin Cimpanu, "Australian tech unicorn Canva suffers security breach," ZDNet, accessed August 30, 2020, published May 24, 2019, https://www.zdnet.com/article/australian-tech-unicorn-canva-suffers-security-breach/.

58 A. L. Johnson, "Hidden Lynx - Professional Hacker for Hire," Broadcom, accessed August 31, 2020, published September 17, 2013, https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8962de07-8e6a-41cc-a6d6-d22ea52dcbfa&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

59 GReAT, "THE 'ICEFOG' APT: A TALE OF CLOAK AND THREE DAGGERS," Kaspersky Lab, accessed September 2, 2020, https://media.kaspersky.com/en/icefog-apt-threat.pdf; Pierluigi Paganini, "Hunting the ICEFOG APT group after years of silence," Security Affairs, accessed September 2, 2020, published June 8, 2019, https://securityaffairs.co/wordpress/86826/apt/icefog-apt-group-return.html.

60 Tara Seals, "Researcher Claims Iranian APT Behind 6TB Data Heist at Citrix," Threatpost, accessed September 2, 2020, published March 11, 2019, https://threatpost.com/ranian-apt-6tb-data-citrix/142688/; Doug Olenick, "Iridium cyberespionage gang behind the Aussie parliament attacks," SecurityWeek, accessed September 2, 2020, published March 1, 2019, https://www.scmagazine.com/home/security-news/apts-cyberespionage/iridium-cyberespionage-gang-behind-aussie-parliament-attacks/.

61 "Lazarus Group," ThreatStream, https://ui.threatstream.com/actor/281.

62 "MageCart," ThreatStream, https://ui.threatstream.com/actor/21764

63 THREAT GROUP CARDS: A THREAT ACTOR ENCYCLOPEDIA," ThaiCERT, accessed September 2, 2020, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf, 165.

64 Xue Yin Peh, "Australia Cyber Threat Landscape Report (H1 2019)," Digital Shadows Blog.

65 "Silence," ThreatStream, https://ui.threatstream.com/actor/26796.

66 "Silent Librarian," ThreatStream, https://ui.threatstream.com/actor/11439.

67 "APT10," ThreatStream, https://ui.threatstream.com/actor/1174.

68 "Turla," ThreatStream, https://ui.threatstream.com/actor/1145.

69 "Iranian Nation-State APT Groups 'Black Box' Leak," ClearSky Cyber Security, accessed September 2, 2020, published May 2019, https://www.clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf, 12; Catalin Cimpanu, "New Leaks of Iranian cyber-espionage operations hit Telegram and the Dark Web," ZDNet, accessed September 2, 2020, puiblished May 9, 2019, https://www.zdnet.com/article/new-leaks-of-iranian-cyber-espionage-operations-hit-telegram-and-the-dark-web/.

70 Catalin Cimpanu, "New Leaks of Iranian cyber-espionage operations hit Telegram and the Dark Web," ZDNet.

Appendix A

Table 1. Threat Groups that Target, or are Located In, Australia.

Threat Actor/Group	Description	Country of Origin
Anchor Panda (APT14, Aluminum)	Targets countries with interest in the South China Sea in addition to western companies in multiple industries.[46] Possibly associated with the Iridium group.	China
APT19 (Codoso, Sunshop Group)	Information-motivated group likely compromised of freelancers that target numerous industries, primarily with commodity tools.[47] There is likely some form of agreement between the group and the Chinese government.[48]	China
APT29 (Cozy Bear, Cozy Duke, Mini Duke, The Dukes)	The group boasts an arsenal of custom and complex malwares at its disposal and is believed to be sponsored by the Russian Federation government. APT29 is known for compromising US's Democratic National Committee in 2016, and has been active since at least 2008.[49]	Russia
APT32 (OceanLotus, SeaLotus, APT-C-00, Ocean Buffalo)	Cyberespionage group that targets numerous industries with commodity and custom malware since at least 2013.[50]	Vietnam
APT41	Sophisticated group that engages in cyberespionage and financially-motivated campaigns.[51]	China
Carbanak (Anunak, Carbon Spider)	Financially-motivated group that has been active since at least 2013. They are a sophisticated group that will compromise vendors employed by the primary target to use the vendor's legitimate emails in spearphishing campaigns.[52]	Ukraine
Deep Panda (APT26, Shell Crew, WebMasters, KungFu Kittens, Group 13, PinkPanther, Black Vine)	Cyberespionage group that conducts campaigns that primarily target the US, however multiple other countries are also targeted. This includes an interest in countries and entities associated to, and located in, the Asia Pacific region.[53]	China
Desert Falcons (APT-C-23, Two-tailed Scorpion)	Information-motivated group that consists of approximately 30 members around the world that spend the time necessary to create convincing fake material for their campaigns.[54]	Gaza
Elderwood (Elderwood Gang, Sneaky Panda, SIG22, Beijing Group)	Motivated by the theft of proprietary information and was first identified in 2012. Believed to consist of different sub-groups each with their own specific targeting. Elderwood uses a platform that contains various exploits utilized in spearphishing and watering-hole campaigns.[55]	China

Threat Actor/Group	Description	Country of Origin
Emissary Panda (APT27, LuckyMouse, Bronze Union, TG-3390, TEMP.Hippo, Group 35)	Utilizes strategic web compromise to target organizations with the objective of information theft.[56]	China
Gnosticplayers	Cybercriminal who has claimed responsibility for numerous data breaches and dumping them on underground markets.[57]	Pakistan
Hidden Lynx (Aurora Panda, Group 8)	Cyberespionage group that offers "professional hackers for hire."[58]	China
Icefog (Dagger Panda)	APT group that targets numerous industries, often in supply chain attacks, and uses multiple tools to steal sensitive data.[59]	China, Japan, South Korea
Iridium	Cyberespionage group "that uses proprietary techniques to bypass two-factor authentication for critical applications."[60] Possibly associated with the Achilles group.	Iran
Lazarus Group (Hidden Cobra, Guardians of Peace, Dark Seoul, New Romanic Cyber Army, Whois Hacking team)	APT group that is well known for their tendency to engage in data destruction/disk wiping attacks, and DDoS attacks against targets around the world. Operatives are believed to be distributed throughout strategical geographic locations.[61]	North Korea
Magecart	The umbrella term, MageCart, refers to groups that target online commercial websites and injects payment skimming scripts to illicitly obtain credit card credentials.[62]	Unknown
NetTraveler (APT21)	Cyberespionage group that targets high profile individuals to install surveillance malware on their machines.[63]	China
Scarlet Widow	Financially-motivated group known for conducting BEC campaigns.[64]	Nigeria
Silence (Silence Group, Silence Gang)	Financially-motivated group-for-hire that is suspected to be made up of cybersecurity professionals who have migrated towards conducting black hat activities.[65]	Unknown
Silent Librarian (Mabna Institute)	Cyberespionage group on stealing academic and research materials to energy, medical, technical fields.[66]	Iran
Stone Panda (APT10, menuPass, menuPass Team, Red Apollo, CVNX, Potassium, Hogfish, Happyyongzi)	Gained notoriety by targeting defense contractors around the world, but primarily those located in the US.[67]	China

Threat Actor/Group	Description	Country of Origin
Turla (Waterbug, Venomous Bear, Group 88, SIG23, Iron Hunter, Pacifier APT)	Connected to the "Epic" cyber espionage campaign that targets government agencies around the globe, and is also connected to the Agent.btz worm that infected the network of the US Department of Justice in 2008.[68]	Russia
Rana (Rana Institute)	Cyberespionage group that was discovered on Telegram and underground forum leaks.[69] A freelancing group that appears to have some agreement with the Iranian government.[70]	Iran

Actors:

APT, APT32, OceanLotus, SeaLotus, APT-C-00, Ocean Buffalo, Carbanak, Anunak, Carbon Spider, Deep Panda, APT26, Shell Crew, WebMasters, KungFu Kittens, Group 13, PinkPanther, Black Vine, Desert Falcons, APT-C-23, Two-tailed Scorpion, Elderwood, Elderwood Gang, Sneaky Panda, SIG22, Beijing Group, Emissary Panda, APT27, LuckyMouse, Bronze Union, TG-3390, TEMP.Hippo, Group 35, Gnosticplayers, Hidden Lynx, Aurora Panda, Group 8, Icefog, Dagger Panda, Iridium, Lazarus Group, Hidden Cobra, Guardians of Peace, Dark Seoul, New Romanic Cyber Army, Whois Hacking team, Magecart, NetTraveler, APT21, Scarlet Widow, Silence, Silence Group, Silence Gang, Silent Librarian, Mabna Institute, Stone Panda, APT10, menuPass, menuPass Team, Red Apollo, CVNX, Potassium, Hogfish, Happyyongzi, Turla, Waterbug, Venomous Bear, Group 88, SIG23, Iron Hunter, Pacifier APT, Rana, Rana Institute

Countries:

American Samoa, Australia, Bougainville Island, Choiseul, Fiji, Malaita, New Britain, New Caledonia, New Ireland, New Georgia Islands, New Zealand, Niue, Papua New Guinea, Papua, West Papua, Samoa, Santa Isabel Island, Solomon Islands, Tonga, Vanuatu, Wallis and Futuna.

Industries:

Agriculture, Forestry, Fishing and Hunting, Mining, Utilities, Construction, Manufacturing, Wholesale Trade, Retail Trade, Transportation and Warehousing, Information, Finance and Insurance, Real Estate Rental and Leasing, Professional, Scientific, and Technical Services, Management of Companies and Enterprises, Administrative and Support and Waste Management and Remediation Services, Educational Services, Health Care and Social Assistance, Arts, Entertainment, and Recreation, Accommodation and Food Services, Other Services, Public Administration