Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

No. 719 September 2025

Abstract | Ransomware is one of the most prolific and economically damaging cybercrime threats of the contemporary era. This exploratory study aims to enhance knowledge about ransomware criminal groups. Our focus is on ransomware criminal groups that targeted organisations in Australia, Canada, New Zealand and the United Kingdom between 2020 and 2022. The paper examines the evolution and activities of ransomware criminal groups. Results reveal the most active ransomware criminal groups, the median range of their careers and the most targeted victim organisations by country and sector type.

Examining the activities and careers of ransomware criminal groups

Chad Whelan, David Bright, James Martin, Callum Jones and Benoît Dupont

Introduction

Ransomware has emerged as one of the most significant cybercrime threats in the contemporary era. This malicious software employs cryptoviral techniques to encrypt victims' data or system, extorting payment in cryptocurrencies for the release of decryption keys (Brill & Thompson 2019; Lee & Choi 2021). Recently, ransom demands have evolved into 'double extortion' and 'triple extortion', involving threats to sell or expose stolen data and pressuring victims through contacts with stakeholders (Datta & Acton 2022; Kara & Aydos 2022). Ransomware groups compromise systems through various means such as botnets, freeware and phishing emails that exploit cognitive biases (Bhardwaj et al. 2016; Mago & Madyira 2018).

Wall (2021a: 38) asserts: 'Ransomware has evolved into a sophisticated billion-dollar business, supported by a "professional" ecosystem driven by cybercrime's profitability and high returns.' Over the past decade, research into ransomware has unveiled a complex ecosystem (Martin & Whelan 2023; Matthijsse, van 't Hoff-de Goede & Leukfeldt 2023) involving diverse actors, services and data across various stages of an attack (Hacquebord, Kenefick & Mercês 2022; Wall 2021b).

CRG CRIMINOLOGY RESEARCH GRANT

Ransomware groups have increased significantly in size and sophistication across this period. These groups can emerge and shut down quickly, with individual cybercriminals moving between ransomware groups as the ecosystem adapts to various pressures and opportunities (Lubin 2022).

One of the most troubling developments in recent years has been the rise of ransomware-as-a-service (RaaS; Lusthaus, van Oss & Amann 2023; Ryan 2021). RaaS distinguishes a core ransomware group from affiliates (Gray et al. 2022; Wall 2021a), with the former developing and distributing malware, recruiting, and managing victim payments and leak sites (Gray et al. 2022; Madhira et al. 2023; Wall 2021a; Warikoo 2023). Affiliates, on the other hand, are commissioned workers responsible for compromising victim systems, deploying ransomware and engaging in negotiations to extort ransoms (Paquet-Clouston & García 2022; Stevens 2009). The relationship between core and affiliate groups is market based and ephemeral, and affiliates will often switch between ransomware groups in response to incentives such as an increased share of ransoms (Wilner et al. 2019).

The current study

The current study aims to enhance knowledge about ransomware criminal groups. Our focus is on ransomware criminal groups that targeted organisations (rather than individuals; see Voce & Morgan 2021) in Australia, Canada, New Zealand and the United Kingdom between 2020 and 2022, based on insights from all known ransomware extortion sites during this period. For the purposes of this paper, we focus on the evolution and lifespan of ransomware criminal groups and the characteristics of their victims.

Data and methods

This research examines ransomware attacks conducted within Australia, Canada, New Zealand and the United Kingdom across a three-year period from 2020 to 2022, with an emphasis on understanding which ransomware groups conducted the attacks and how these attacks were carried out.

Data

Data were initially collected from Recorded Future, a cybersecurity company that offers, among other things, reports that provide data and analysis about adversaries, infrastructure and targets of cybercrime (see https://www.recordedfuture.com/). Recorded Future collects data from various sources available on both the clearnet and the darknet, including open-source intelligence, darknet forums, network traffic analysis and partnerships with other cybersecurity entities. Recorded Future largely collects these data for commercial purposes, such as providing insights into cyber threats for various private corporations, so the data collected may not meet the requisite standards for scientific research. To address this, we supplemented the data collected from Recorded Future with other open-source data, to develop a richer dataset to inform our analysis.

The Recorded Future database was queried to obtain a list of ransomware attacks conducted within the countries of interest during the period of interest (2020–2022). Recorded Future began collecting these data from 2020, and we collected these data over three calendar years. It is important to note that we collected a narrow set of data points and did not collect any victim data that had been uploaded on leak sites.

Victim organisations were de-identified and assigned to a specific industry sector which correlated best to the industry in which they operated (for more details, see *Analytical approach*). Industry sectors loosely followed the Global Industry Classification Standard (MSCI 2023), as shown in Table 1, but were expanded slightly to capture a range of otherwise unclassified companies.

Table 1: Industry classification definitions

Industry	Definition
Communications	Facilitate communication and offer related content and information through platforms, including telecommunications and internet service providers, organisations that provide media and entertainment services such as advertising, broadcasting, publishing, movies, entertainment, interactive media and services
Construction	Engage in construction projects, from residential constructions to large-scale infrastructure developments by building, renovating and developing land, while offering specialised structural and installation services
Consumer goods	Manufacturing, supply or distribution of goods such as vehicles and components, household goods, leisure products, food and beverages
Education	Organisations providing formal education services, including primary and secondary schools, registered training providers and universities
Energy	Within the energy equipment and services industry, which covers equipment and services companies and oil and gas drilling; oil, gas and consumable fuel industry, including companies engaged in exploration, production, refining, marketing, storage and transportation
Financial services	Banking, finance, capital markets and insurance
Government	Public sector responsible for administering and delivering government-operated services and initiatives, including domains such as government services, public safety and infrastructure
Healthcare	Healthcare services, manufacture and distribute healthcare equipment, including pharmaceuticals and hospitals
Industrial	Manufacture and distribute capital goods, such as building products and electrical equipment, or offer construction and engineering services
Legal services	Legal services industry, encompassing legal firms and legal professionals, providing expertise and services within various fields of law and legal practice
Materials	Manufacturing and distribution of chemicals, construction equipment, packing products, minerals and mining
Other	Sector that is not included in this framework, such as small political parties and unions. The sectors that organisations classified as 'other' belong to are too small, niche and infrequently occurring to develop into an independent category.
Real estate	Real estate development and operation
Technology	Develop and offer software and information technology services and manufacture and distribute technology hardware
Transportation	Industrial sector including services to transport people or goods and sit within industries such as logistics and air freight or airlines, marine, road and rail, along with their respective infrastructures
Utilities	Utilities such as electricity, gas and water supply and distribution

Analytical approach

The analytical approach adopted in this research was quantitative, using Python for the data analysis. The first section of the quantitative analysis delineated and tallied the frequency of ransomware attacks by three key attributes: the ransomware organisation responsible for the attack, the location of the entity attacked, and the industrial sector of the entity attacked. The first and second of these three attributes were extracted directly from the data collected by Recorded Future. The data collected from Recorded Future outlined the ransomware organisation responsible for the attack, the entity attacked, the date that the attack was conducted, and the location of the entity attacked.

The third of these three attributes, the industrial sector of the entity targeted, was assigned using artificial intelligence. Specifically, OpenAI's gpt-3.5-turbo model was accessed via the OpenAI API and used to assign industrial sectors (specified in Table 1) to each of the entities targeted by ransomware attacks in our event list. Once this process was complete, we conducted a validation procedure as a check on the automated classification process. To accomplish this, we constructed a stratified random sample of 10 percent of the total number of entities on our event list to manually verify the gpt-3.5-turbo model's allocation. We found that the gpt-3.5-turbo had correctly assigned entities to sectors in 89 percent of cases, which we deemed to be sufficient to proceed with the analysis.

Ethical considerations

This project obtained ethical approval from Deakin University Human Research Ethics Committee (approval number 2023-024).

Results

The results from this study are organised in two sections. Firstly, we present our results for ransomware group activities in terms of attack frequency and lifespan over the period. Secondly, we concentrate on the profile of victims of ransomware attacks, including across a range of industry sectors and countries over the period.

Ransomware groups

The following subsections analyse ransomware attacks by year (2020, 2021, 2022) to show how the ransomware landscape has shifted over time. In total, 865 ransomware attacks were included in these data, including 135 from Australia, 346 from Canada, 18 from New Zealand and 366 from the United Kingdom.

Table 2 outlines the total number of attacks by the top 30 percent most active ransomware criminal groups over our period. A significant number of groups were not active for the entire period under examination, with only three groups being active across all three years. The median number of active years for ransomware organisations listed in Table 2 is 1.76, whereas the median number of years active for all ransomware organisations in the dataset was 1.36, showing that larger and more active ransomware organisations have a longer lifespan. Some ransomware groups rebranded under different identities (see Whelan, Bright & Martin 2024), and this undoubtedly impacted our findings.

Conti was by far the most active group (*n*=141 attacks). If we combine the three iterations of LockBit, however, this group is responsible for 129 attacks. Conti and LockBit have therefore been far more active than other ransomware groups, with the next most active being Pysa (48 attacks). Notably, Pysa ceased operating in late 2021, whereas Conti and LockBit are among the few that remained active across all three years (although Conti closed down in mid-2022). Groups that remained active throughout the period and adopted a RaaS model tended to be responsible for a higher proportion of attacks.

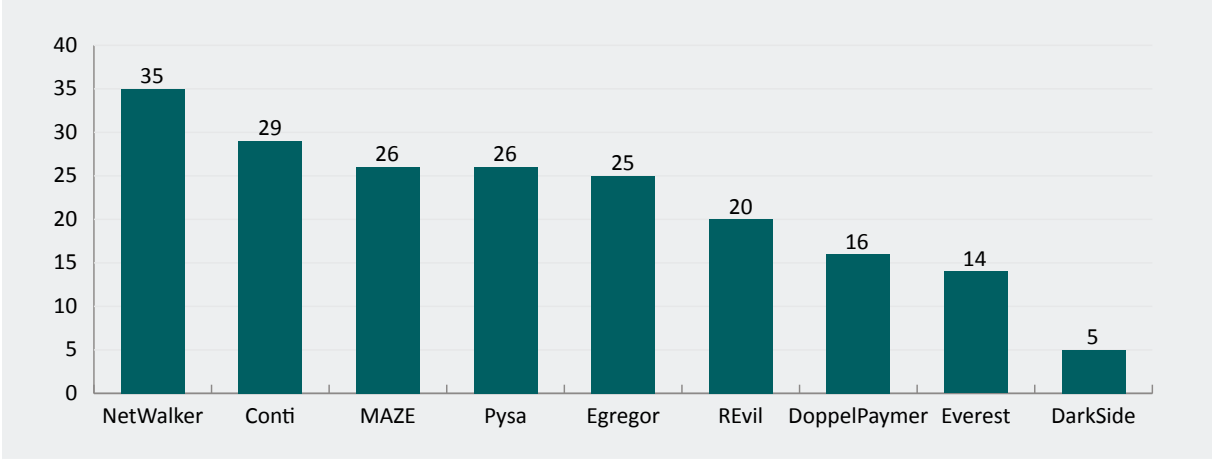
Table 2: Most active 30% of ransomware criminal groups' careers and attack frequencies (*n*)

Ransomware group	Frequency			
	2020	2021	2022	Total
Conti	29	88	24	141
LockBit	0	52	19	71
Pysa	26	22	0	48
REvil	20	23	0	43
NetWalker	35	2	0	37
LockBit 3.0	0	0	36	36
Karakurt	0	0	28	28
ALPHV (BlackCat)	0	0	26	26
Everest	14	3	9	26
MAZE	26	0	0	26
Avaddon	3	22	0	25
Egregor	25	0	0	25
Vice Society	0	4	20	24
LockBit 2.0	0	0	22	22
DoppelPaymer	16	5	0	21
Clop	2	14	4	20
Hive	0	8	10	18
AvosLocker	0	11	5	16
Black Basta	0	0	15	15
Quantum	0	2	13	15
BianLian	0	0	14	14
Grief	0	11	1	12
LV	0	10	2	12

2020

In total, 218 attacks were executed by 19 ransomware organisations. Figure 1 shows the number of attacks by ransomware groups in 2020, with a threshold of a minimum of five attacks. Several ransomware organisations were responsible for a large percentage of attacks. Figure 1 shows that NetWalker was responsible for the greatest number of attacks (*n*=35). Notably, in 2020, NetWalker moved to a RaaS model, which may explain this trend.

Figure 1: Number of attacks by ransomware groups in 2020



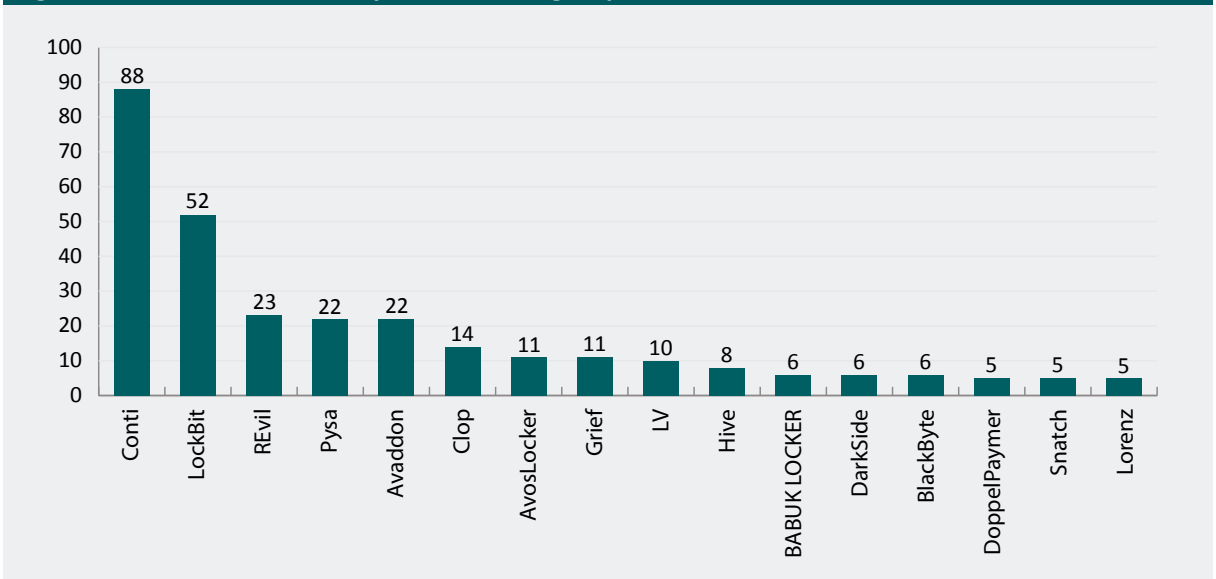
Note: A threshold of a minimum of five attacks was imposed

Conti was the second most prominent ransomware organisation (*n*=29). Conti first emerged in 2019 (Warikoo 2023) and rose to prominence because of its effectiveness in targeting government organisations, particularly healthcare networks (Alzahrani, Xiao & Sun 2022). MAZE and Pysa were prominent ransomware organisations in 2020 (*n*=26 attacks). REvil (also known as Sodinokibi) conducted 20 attacks in 2020. REvil is a Russian-based ransomware organisation and is known to have adopted a RaaS model as of 2020 (Westbrook 2021). Everest is known for its high-profile attack on US communications provider AT&T in 2022 (Searchlight Cyber 2023). DarkSide, which emerged in 2020 (Warikoo 2023) and is known to have implemented a RaaS scheme (Westbrook 2021), conducted five ransomware attacks in 2020. Other ransomware organisations present in 2020 were each responsible for fewer than five ransomware attacks.

2021

In total, 338 ransomware attacks were conducted in 2021, notably higher than in 2020. Figure 2 shows the number of attacks by ransomware groups in 2021, with a threshold of a minimum of five attacks. The number of ransomware organisations conducting attacks also increased, with 38 active ransomware organisations in 2021 (compared with 19 in 2020).

Figure 2: Number of attacks by ransomware groups in 2021



Note: A threshold of a minimum of five attacks was imposed

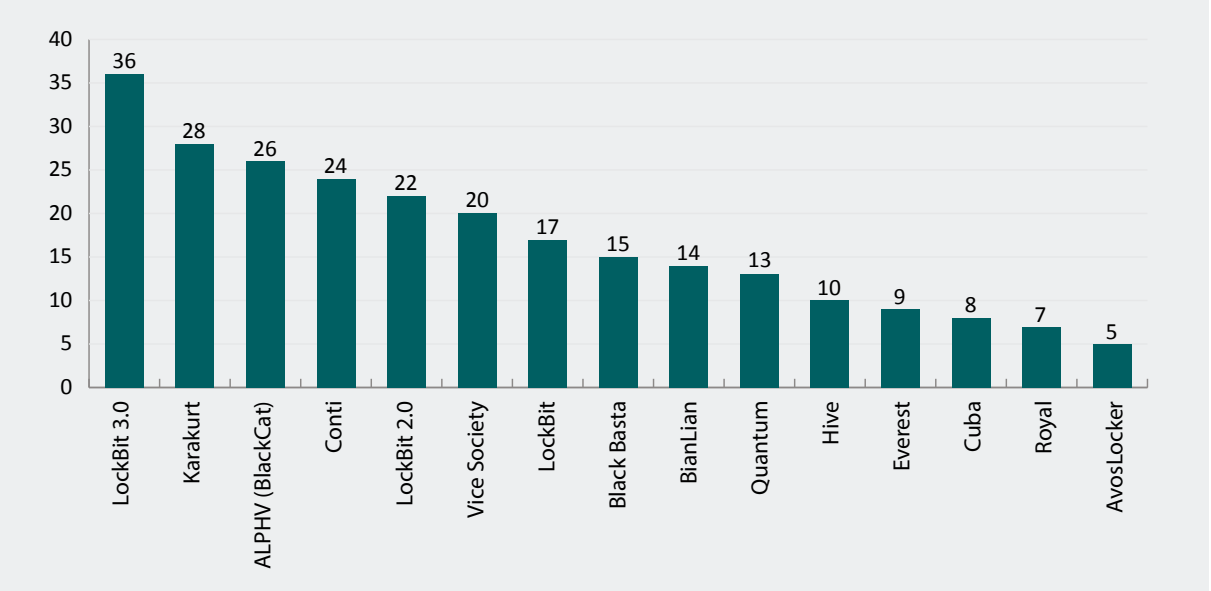
The ransomware landscape changed significantly between 2020 and 2021. Conti was one of several major ransomware organisations that perpetrated more attacks in 2021; with the decline of NetWalker, Conti became the most prolific ransomware organisation within the time period. Conti (*n*=88 attacks) was responsible for significantly more attacks than the second most prominent ransomware organisation, LockBit (*n*=52 attacks). LockBit successfully operates a RaaS scheme and was the most active ransomware group in the world in 2022, based on the number of victims posted on their extortion site (Australian Signals Directorate 2023). Other ransomware organisations were able to increase their attacks, with Avaddon increasing from three attacks in 2020 to 22 in 2021 (Georgescu 2022). Clop increased its attacks to 14, from two in 2020. However, some major ransomware organisations decreased their attacks. A series of law enforcement actions instigated by United States authorities (Department of Justice 2021) may have caused a significant reduction in the number of attacks conducted by NetWalker. Other notable examples of major ransomware organisations committing fewer attacks in 2021 include Pysa (down from 26 in 2020 to 22 in 2021) and Everest (down from 14 in 2020 to three in 2021).

While there were some shifts in the prevalence of ransomware organisations, there were also new organisations entering the landscape, and others leaving. This is probably impacted by certain groups that are believed to have rebranded during this and later time periods. MAZE is an example of a ransomware organisation leaving the landscape between 2020 and 2021. Egregor, suspected of having links with MAZE, also committed no additional attacks after 2020, following a series of arrests of affiliates in Ukraine (Abrams 2021). Conversely, LockBit emerged in 2021 and, as discussed, was the second most active ransomware organisation, responsible for 52 attacks. Other ransomware organisations, such as Grief, AvosLocker, LV, Hive, BABUK LOCKER, BlackByte, Snatch, Vice Society, Prometheus, Cuba and Marketo, emerged in 2021; each was responsible for a small number of attacks.

2022

In 2022, ransomware attacks dipped slightly; 309 attacks were perpetrated by 42 ransomware organisations. Figure 3 shows the number of attacks by ransomware groups in 2022, with a threshold of a minimum of five attacks.

Figure 3: Number of attacks by ransomware groups in 2022



Note: A threshold of a minimum of five attacks was imposed

A range of ransomware organisations emerged in 2022. The most notable development was the emergence of LockBit 3.0, which was responsible for the greatest number of attacks (Australian Signals Directorate 2023). Karakurt emerged in 2022 and was the second most prominent ransomware organisation (*n*=28 attacks). Karakurt is reported to have close ties with Conti (Greig 2023). The ALPHV (also known as BlackCat) ransomware organisation and RaaS entity emerged in late 2021 and is alleged to have links with BlackMatter and DarkSide (Australian Signals Directorate 2022). In 2022, it was the third most prominent ransomware organisation, responsible for 26 attacks. Black Basta, Hive and Quantum all emerged in 2022 (Warikoo 2023), as did BianLian and Royal. BianLian and Black Basta were the most prominent of these newly present ransomware organisations, committing 14 and 15 attacks respectively. Quantum and Hive perpetrated 13 and 10 respectively, followed by Royal (*n*=7 attacks). Some ransomware organisations that were present in previous years increased their number of attacks significantly: Vice Society rose from four attacks in 2021 to 20 in 2022; Everest's attacks increased to nine in 2022, from three in 2021; and Cuba's attacks increased from two in 2021 to eight in 2022.

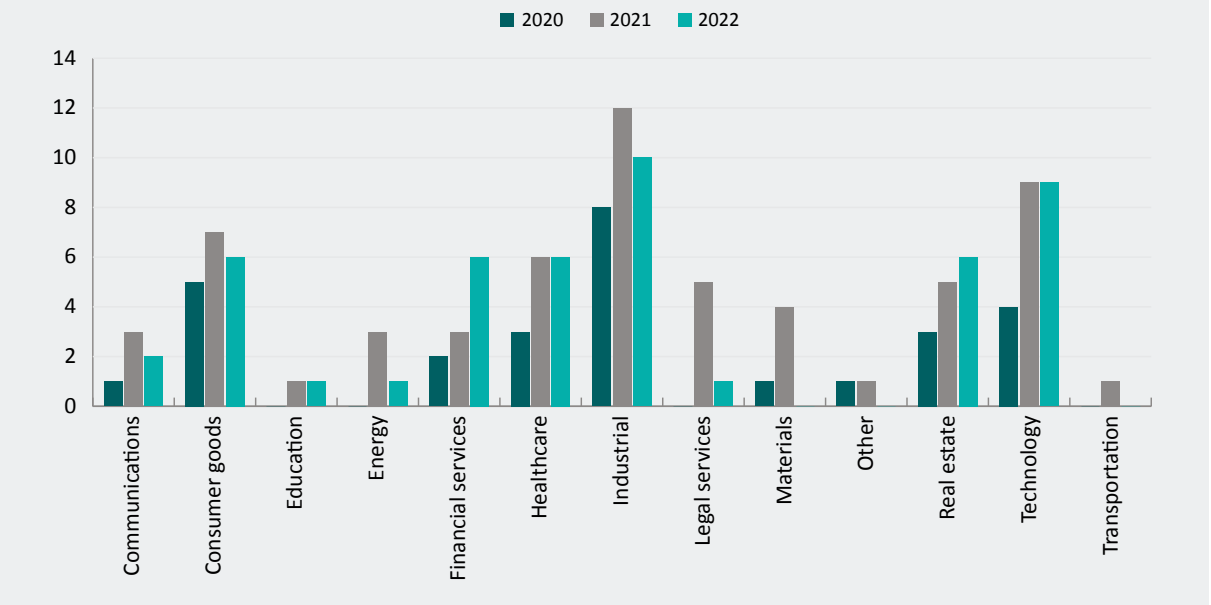
Several ransomware organisations prominent in previous years saw large declines in attack volume in 2022. One of the most notable was Conti, which was responsible for just 24 attacks in 2022 (compared with 88 in 2021). This shift is attributable to Conti voluntarily shutting down in 2022 (Warikoo 2023). Other ransomware organisations that had significant declines in attacks include Clop (*n*=4 attacks, compared with 14 in 2021). The year 2022 also saw the disappearance of several high-profile ransomware organisations. Avaddon, which rose from the 11th most prominent ransomware organisation in 2020 to fifth in 2021, disappeared entirely. Pysa, which was the equal third most prominent ransomware organisation in 2020 and fourth in 2021, was not present in 2022, for unknown reasons. REvil, which ranked in the top 10 ransomware organisations in both 2020 and 2021, also disappeared in 2022 following a series of arrests and other law enforcement interventions from both the United States and Russia (Gatlan 2021). Ransomware group DarkSide is believed to have had links to REvil and was implicated in the Colonial Pipeline attack; it also completely disappeared following the same series of arrests by Russian authorities that targeted REvil (Gatlan 2021).

Ransomware victims

Australia

Figure 4 documents the 135 ransomware attacks against Australian organisations between 2020 and 2022.

Figure 4: Ransomware attacks in Australia, by sector, 2020 to 2022 (*n*)



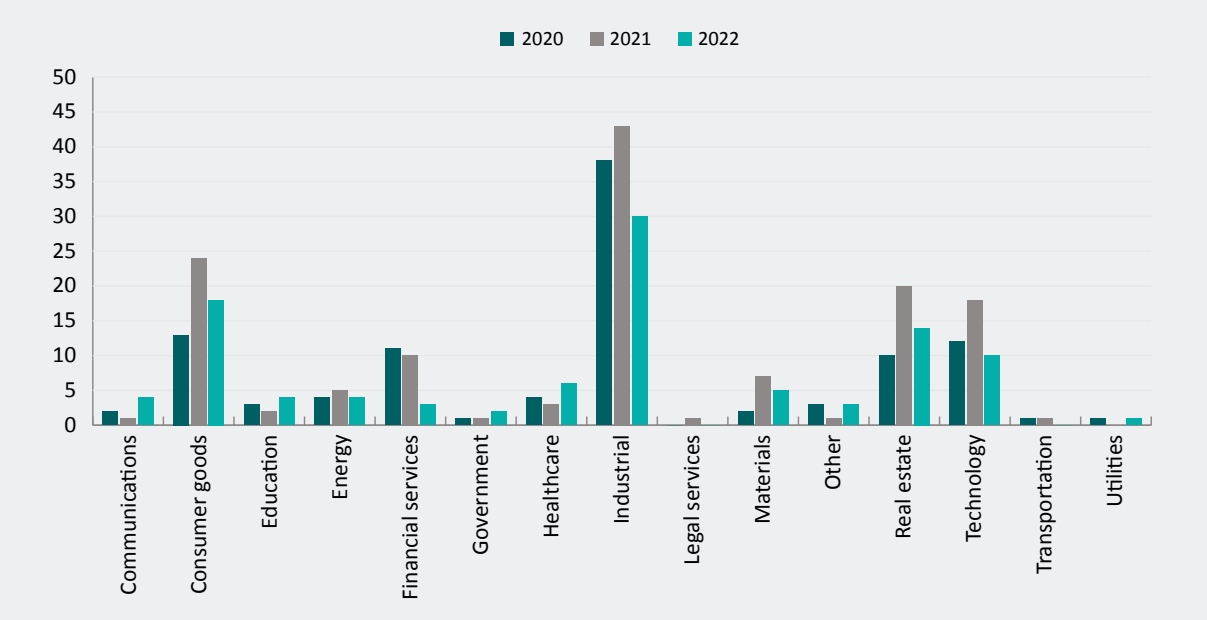
In 2020, the industrial sector was the most targeted in Australia (*n*=8 attacks). This was followed by the consumer goods sector (*n*=5 attacks) and the technology sector (*n*=4 attacks). Other sectors that faced multiple, but fewer, attacks included health care and real estate (*n*=3 attacks), while other sectors faced few attacks. The industrial sector continued to be a primary target in 2021 (*n*=12 attacks). Attacks on consumer goods also increased (*n*=7), as did those on the technology sector (*n*=9) and health care (*n*=6). Ransomware targeting materials companies increased, from one attack to four, along with legal services and communications (*n*=5 and *n*=6 respectively).

In 2022, the industrial sector remained the most targeted sector (*n*=10 attacks). The technology sector saw a notable increase in ransomware attacks, becoming the second most targeted sector (*n*=9 attacks). Financial services, which was not among the top sectors in previous years, saw a notable increase (*n*=6), making it the fourth most targeted sector in that year. Other sectors continued to attract fewer attacks.

Canada

Figure 5 documents the 346 ransomware attacks against Canadian organisations between 2020 and 2022. There was a greater array of industry sectors targeted by ransomware organisations than in Australia.

Figure 5: Ransomware attacks in Canada, by sector, 2020 to 2022 (*n*)



In 2020, the Canadian industrial sector faced 38 ransomware attacks, making it the most targeted sector. The consumer goods and technology sectors experienced a substantial number of attacks, with 13 and 12 incidents respectively. Financial services and real estate were also targeted, with 11 and 10 attacks respectively. The energy and healthcare sectors experienced a series of attacks, while other sectors received comparatively few attacks.

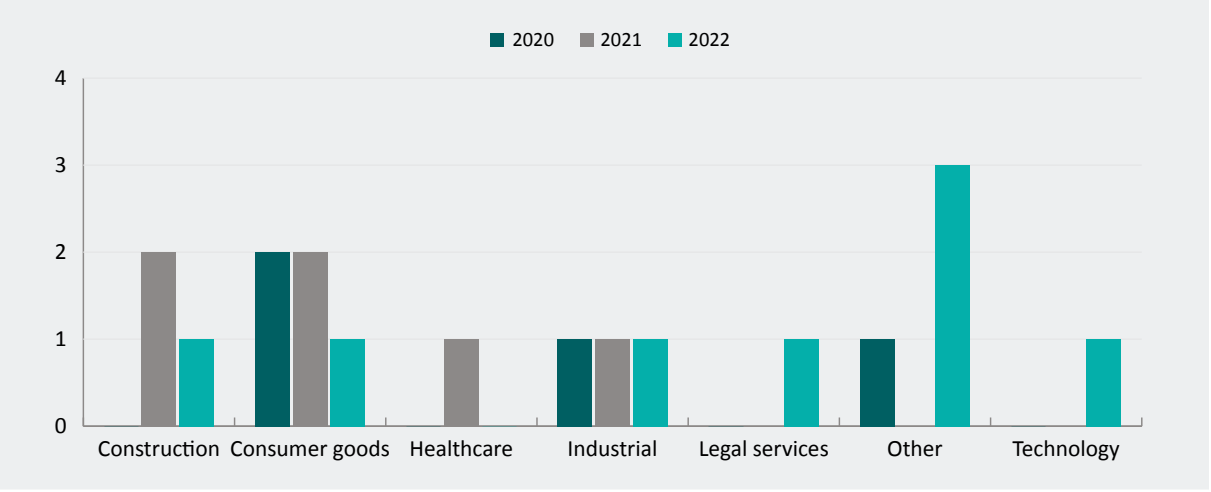
In 2021, the industrial sector maintained its position as the most targeted sector (*n*=43 attacks). Consumer goods and real estate continued to be highly targeted sectors and saw an increase in attacks in 2021. Attacks on the technology sector increased to 18; despite this, it still dropped to fourth most targeted sector, from third in 2020. Attacks on financial services decreased marginally (from 11 in 2020 to 10 in 2021). Other sectors that continued to be targeted, but only minimally, include energy, communications, education, transportation and legal services.

Ransomware attacks dropped to their lowest volume in Canada in 2022, with just 104 recorded. The industrial sector, while remaining the most targeted, encountered a substantial drop to 30 incidents. Consumer goods and real estate both saw a decrease in attacks, down to 18 and 14 respectively.

New Zealand

Figure 6 documents the 18 ransomware attacks against organisations in New Zealand between 2020 and 2022. New Zealand experienced the lowest volume of attacks of any country included in the analysis.

Figure 6: Ransomware attacks in New Zealand, by sector, 2020 to 2022 (*n*)



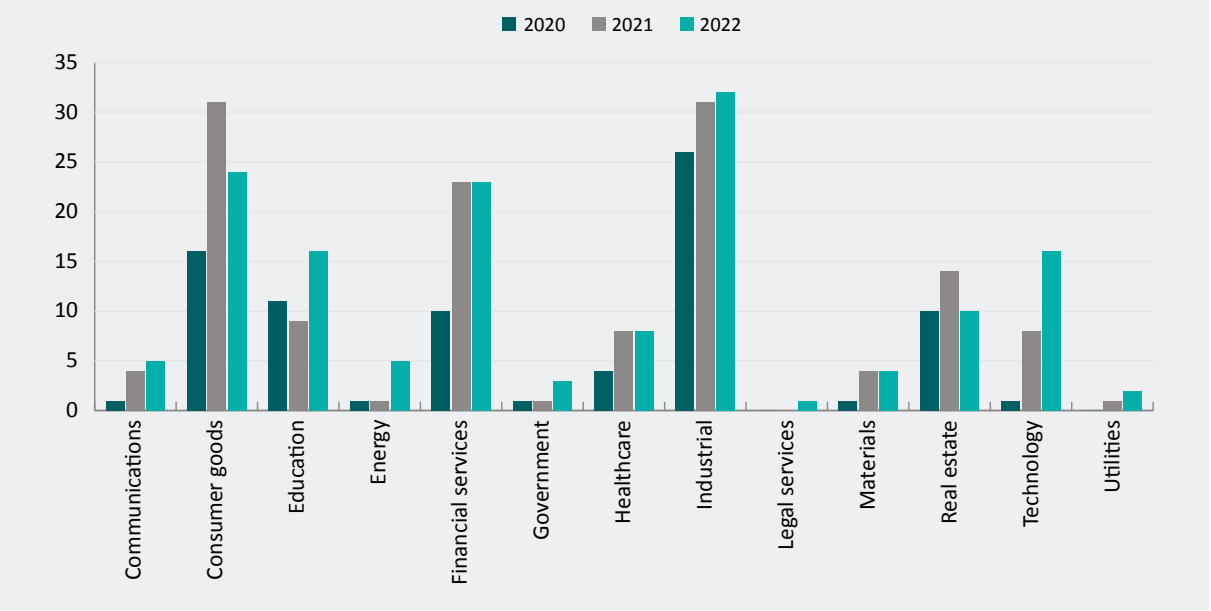
In 2020, only two known sectors (along with a union classified as 'other') were targeted—consumer goods and industrial. There were five ransomware attacks in 2021, compared with four in 2020. Both the consumer goods and industrial sectors faced several attacks in 2020, and construction and healthcare companies were also targeted.

There were eight ransomware attacks targeting New Zealand companies in 2022. The construction, industrial and consumer good sectors continued to be targeted, as were technology and legal services.

United Kingdom

Figure 7 documents the 366 ransomware attacks against organisations in the United Kingdom between 2020 and 2022. The United Kingdom experienced the greatest volume of attacks of any country included in the analysis. The array of sectors targeted in the United Kingdom was comparable to that of Canada.

Figure 7: Ransomware attacks in the United Kingdom, by sector, 2020 to 2022 (*n*)



In 2020, the United Kingdom's industrial sector was the most targeted of any sector (*n*=26 attacks). As with Canada and Australia in 2020, consumer goods was the second most targeted sector in the United Kingdom (*n*=16). Notably, education, rarely targeted in other national contexts, was the third most targeted sector in the United Kingdom (*n*=11 attacks). Financial services and real estate were targeted with around the same frequency (*n*=10). While the technology sector regularly ranked among the most targeted in other national contexts, the UK technology sector was targeted with only one attack in 2020. Other sectors were not widely targeted.

The industrial sector remained the dominant target of ransomware groups (*n*=31 attacks) in 2021 but was matched by the consumer goods sector. Financial services saw a notable increase, with 23 recorded ransomware attacks. Attacks on real estate companies increased too; that remained a regularly targeted sector. Education, health care and technology were targeted by a small number of attacks. Communications, materials, energy, government and utilities were targeted by fewer still.

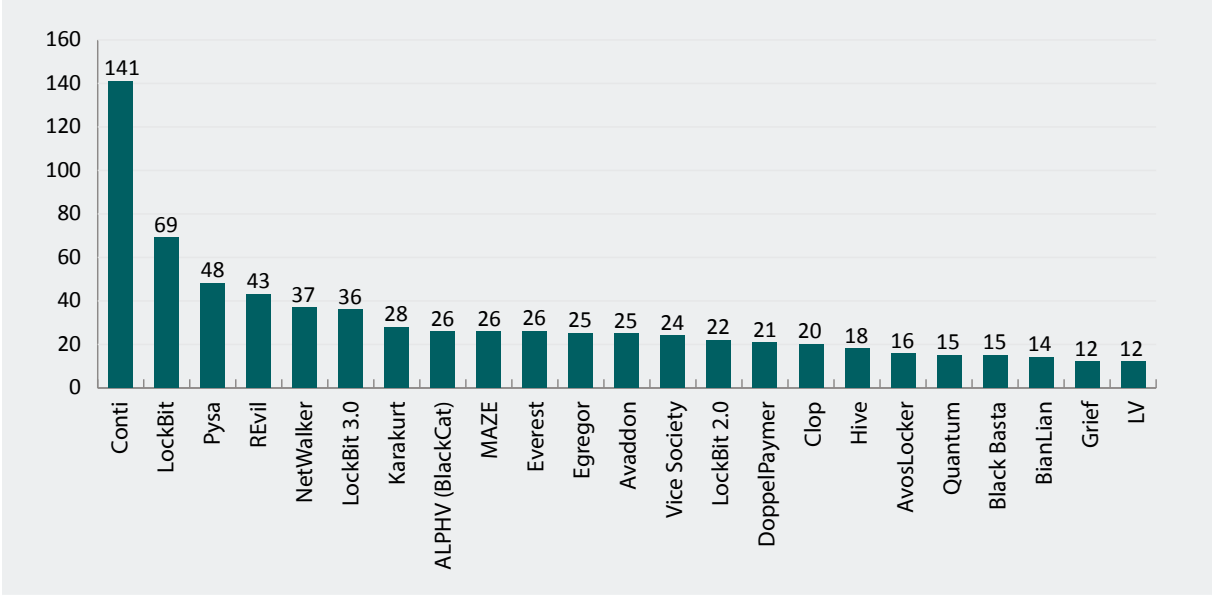
In 2022, the industrial sector continued to be the most targeted; also, the highest number of attacks against the industrial sector was recorded, at 32. Consumer goods remained the second most targeted sector (*n*=24 attacks), followed closely by financial services (*n*=23). Education continued to be a prominently targeted sector, and the technology sector increased significantly, from eight attacks recorded in 2021 to 16 attacks in 2022. The remaining sectors were targeted less frequently.

Discussion and conclusion

Ransomware groups

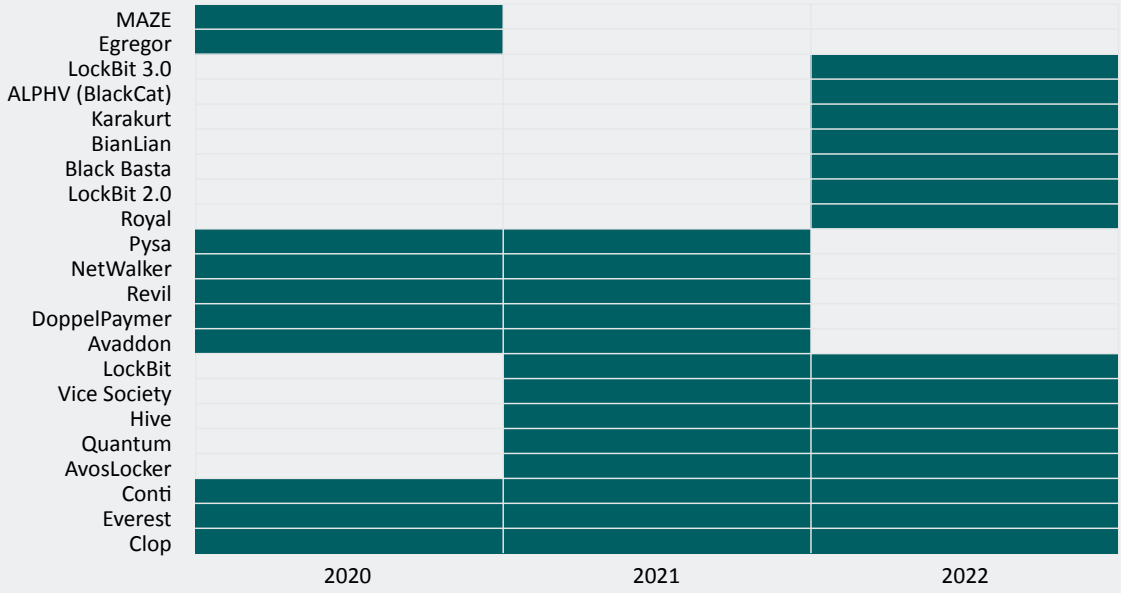
Figure 8 shows that Conti was by far the most active group, being responsible for 141 attacks. Figure 9 shows the lifespan of the top 30 percent most active ransomware criminal groups, ordered by the total years active and which years active—ascending from 2020 to 2022. Figure 9 shows that Conti was active across all three of the years included in this study, which partly explains the high frequency of attacks. If we combine the three iterations of LockBit, however, that group is responsible for 129 attacks and was active in both 2021 and 2022. Conti and LockBit were therefore far more active than other ransomware groups, with the next most active being Pysa (48 attacks). Notably, as Figure 9 shows, Pysa ceased operating in late 2021, whereas Conti and LockBit are among the few that remained active throughout the entire period under examination (although Conti closed down in mid-2022; see Martin, Whelan & Bright 2024). Some other groups that were active throughout the period adopted different structures or were less active for other reasons; for example, there is some evidence that Vice Society does not operate a RaaS model (Gumarin 2022). Groups that remained active throughout the period and which adopted a RaaS model tended to be responsible for a higher proportion of ransomware attacks.

Figure 8: Attacks conducted by most active 30% of ransomware groups, 2020 to 2022 (*n*)



While groups like Conti and LockBit were dominant in terms of attacks and lifespan, several ransomware groups had a short lifespan but were responsible for a significant number of attacks. Examples of these short-lived, highly active ransomware groups are MAZE and Egregor—both of which were only active in 2020 but managed to conduct 26 and 25 attacks respectively. Conversely, other ransomware groups were present across the entire dataset but were responsible for relatively few attacks. Examples include Everest and Clop, responsible for 26 and 20 attacks over the whole period.

Figure 9: Lifespan of the most active 30% of ransomware criminal groups



Ransomware victims

Several sectors were targeted disproportionately by ransomware attacks, regardless of their national context. The most prevalent of these is the industrial sector, which was consistently within the top three most targeted sectors in each year in each country and was regularly the most targeted sector. The consumer goods sector was also consistently one of the most targeted sectors across all years and countries. However, as Table 3 shows, the consumer goods sector faced fewer ransomware attacks (*n*=150) than the industrial sector (*n*=239). This may reflect the size of the industrial sector or may be due to other reasons. (It may represent a softer target for ransomware operators or access brokers or may be an attractive target because of the need to maintain production lines at all costs, suggesting that they may also be perceived to be more inclined to pay ransoms). The real estate (*n*=93), financial services (*n*=93) and technology (*n*=92) sectors were all regularly targeted across all years and all national contexts with a comparable frequency. Figure 10 represents these data by line graph by country.

Figure 10: Ransomware victim sectors by country, 2020 to 2022 (*n*)

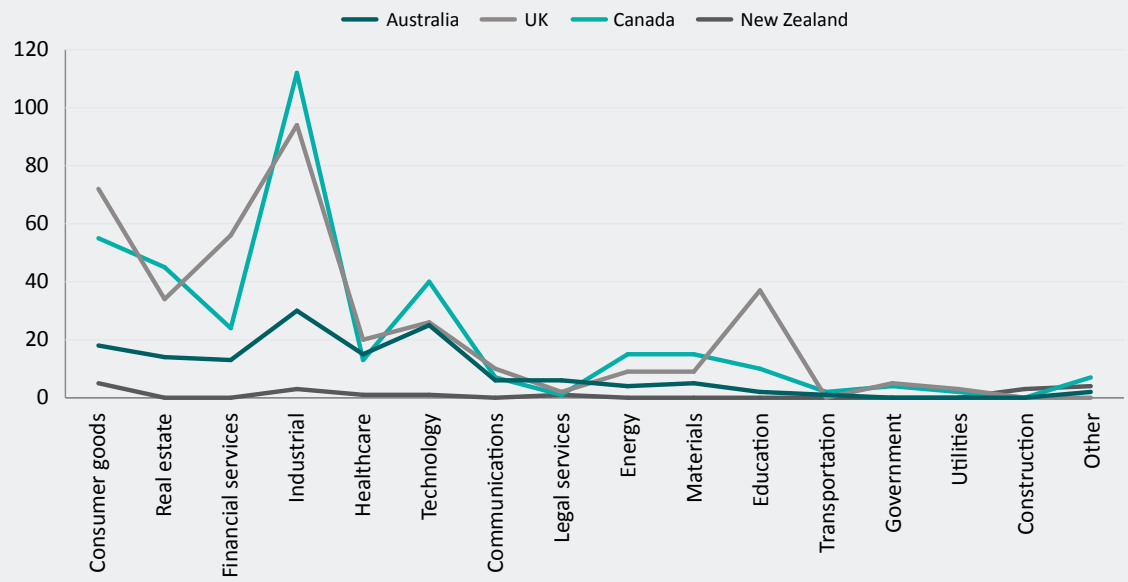


Table 3: Ransomware victims by sector and country, 2020 to 2022 (*n*)

Sector	Australia	United Kingdom	Canada	New Zealand	Total
Industrial	30	94	112	3	239
Consumer goods	18	72	55	5	150
Real estate	14	34	45	0	93
Financial services	13	56	24	0	93
Technology	25	26	40	1	92
Healthcare	15	20	13	1	49
Education	2	37	10	0	49
Materials	5	9	15	0	29
Energy	4	9	15	0	28
Communications	6	10	7	0	23
Other	2	0	7	4	13

Only three companies in the entire dataset were targeted by more than one attack, by more than one ransomware organisation. This is noteworthy because it has been previously found that, once a ransomware organisation successfully attacks a victim, that victim is six times more likely to be targeted again (Hendery 2023).

Limitations

The key limitation of this dataset concerns missing data. There are three primary mechanisms for missing data in this project. Firstly, it is possible that some ransomware groups and/or victims did not appear in the final dataset because they were not coded correctly in Recorded Future's threat intelligence database. Secondly, because the event list was generated based on extortion site data, we are missing ransomware attacks that did not appear on extortion sites. Ransomware victims may not appear on extortion sites for several reasons. Thirdly, the availability of reliable data about known ransomware attacks is limited. Despite the extensive strategies we employed to obtain reliable data, there are many ransomware attacks where there are gaps in the available data.

In addition to data limitations, there may have been errors in the categorisation of industries that influenced overall results. We collected data on only four countries, which may reduce the generalisability of the findings. Finally, we focused on ransomware groups and not on a more fine-grained analysis of actors of such groups. The focus on the macro level may mean that other, finer grained conclusions were not reached.

Policy implications

This research has enhanced knowledge and understanding of the activities and careers of ransomware criminal groups and their targeting preferences (ie victims). In particular, the study identified the fact that certain sectors appear to be at greater risk of victimisation than others. The study thus provides the foundations for further analysis, to build an understanding of the careers of ransomware criminal groups and their activities. To assist with this further analysis, we emphasise the need for better collaboration between government and researchers—particularly in relation to data sharing—and the critical importance of multidisciplinary research collaborations (Dupont & Whelan 2021).

Several policy implications based on the findings of this research pertain to the evolution and targeting preferences of ransomware groups. Prevention strategies tailored to the unique needs and vulnerabilities of sectors may help to reduce the risk and impact of ransomware attacks. These strategies could focus on running targeted awareness programs that educate employees about the risks and signs of ransomware attacks within their sector, conducting cybersecurity audits, and developing advanced threat detection systems. Tailored prevention strategies appear most needed in high-risk sectors such as industrial, consumer goods, real estate, financial services and technology. Further, our results can inform the development of targeted disruption activities against ransomware criminal groups (Whelan & Martin 2023). Evaluating the effects of disruptions is critical and requires significant further thought and collaboration between law enforcement and researchers.

References

URLs correct as at April 2025

Abrams L 2021. DarkSide ransomware gang returns as new BlackMatter operation. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/darkside-ransomware-gang-returns-as-new-blackmatter-operation/

Alzahrani S, Xiao Y & Sun W 2022. An analysis of Conti ransomware leaked source codes. *IEEE Access* 10: 100178-100193. https://ieeexplore.ieee.org/document/9895237

Australian Signals Directorate 2023. *Understanding ransomware threat actors: LockBit.* Australian Signals Directorate. https://www.cyber.gov.au/about-us/advisories/understanding-ransomware-threat-actors-lockbit

Australian Signals Directorate 2022. *2022-004: ASD's ACSC ransomware profile—ALPHV (aka BlackCat)*. Australian Signals Directorate. https://www.cyber.gov.au/about-us/advisories/2022-004-asdacsc-ransomware-profile-alphv-aka-blackcat

Bhardwaj A, Avasthi V, Sastry H & Subrahmanyam G 2016. Ransomware digital extortion: A rising new age threat. *Indian Journal of Science and Technology* 9(14): 1–5

Brill A & Thompson E 2019. Ransomware, a tool and opportunity for terrorist financing and cyberwarfare. *Defence Against Terrorism Review* 12

Datta PM & Acton T 2022. Ransomware and Costa Rica's national emergency: A defense framework and teaching case. *Journal of Information Technology Teaching Cases*: 20438869221149042

Department of Justice 2021. *Department of Justice launches global action against NetWalker ransomware*. Media release, 27 January. Office of Public Affairs, United States Department of Justice. https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware

Dupont B & Whelan C 2021. Enhancing relationships between criminology and cybersecurity. *Journal of Criminology* 54(1): 76–92

Gatlan S 2021. Biden asks Putin to crack down on Russian-based ransomware gangs. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/biden-asks-putin-to-crack-down-on-russian-based-ransomware-gangs/

Georgescu E 2022. *Avaddon Ransomware: Everything You Need to Know*. Heimdal Security. https://heimdalsecurity.com/blog/avaddon-ransomware/

Gray IW, Cable J, Brown B, Cuiujuclu V & McCoy D 2022. *Money over morals: A business analysis of Conti ransomware*. In *Proceedings of the 2022 APWG Symposium on Electronic Crime Research, eCrime 2022*. IEEE Computer Society: 1–12

Greig J 2023. Cybercrime groups find a new target: Religious institutions. *The Record*. Recorded Future. https://therecord.media/cybercrime-groups-find-new-target-churches

Gumarin JR 2022. *Vice Society: Profiling a persistent threat to the education sector.* Unit 42. https://unit42.paloaltonetworks.com/vice-society-targets-education-sector/

Hacquebord F, Kenefick I & Mercês F 2022. *A deep dive into Water Roc, one of the most relentless ransomware groups*. Trend Micro Research. https://vblocalhost.com/conference/presentations/a-deep-dive-into-water-roc-one-of-the-most-relentless-ransomware-groups/

Hendery S 2023. Ransomware victims clobbered by repeat attacks. *SC Media*. https://www.scmagazine.com/news/ransomware-victims-clobbered-by-repeat-attacks

Kara I & Aydos M 2022. The rise of ransomware: Forensic analysis for windows based ransomware attacks. *Expert Systems with Applications* 190: 116198

Lee H & Choi KS 2021. Interrelationship between Bitcoin, ransomware, and terrorist activities: Criminal opportunity assessment via cyber-routine activities theoretical framework. *Victims & Offenders* 16(3): 363–384

Lubin A 2022. The law and politics of ransomware. *Vanderbilt Journal of Transnational Law* 55: 1177–1216

Lusthaus J, van Oss J & Amann P 2023. The Gozi group: A criminal firm in cyberspace? *European Journal of Criminology* 20(5): 1701–1718

Madhira N, Pelletier JM, Johnson D & Mishra S 2023. Code red: A nuclear nightmare-navigating ransomware response at an Eastern European power plant. *Journal of Information Technology Teaching Cases*: 20438869231155934

Mago M & Madyira FF 2018. Ransomware software: Case of WannaCry. *International Research Journal of Advanced Engineering and Science* 3(1): 258–261

Martin J & Whelan C 2023. Ransomware through the lens of state crime. *State Crime Journal* 12(1): 4–28

Martin J, Whelan C & Bright D 2024. Ransomware HR: Human resources practices and organizational support in the Conti Group. *Deviant Behavior*. Advance online publication. https://doi.org/10.1080/01639625.2024.2419905

Matthijsse SR, van 't Hoff-de Goede M & Leukfeldt ER 2023. Your files have been encrypted: A crime script analysis of ransomware attacks. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-023-09496-z

MSCI 2023. Definitions of GICS Sectors effective close of March 17, 2023. https://classification.codes/classifications/industry/gics

Paquet-Clouston M & García S 2022. On the motivations and challenges of affiliates involved in cybercrime. *Trends in Organized Crime* December: 1–30

Ryan M 2021. *Ransomware revolution: The rise of a prodigious cyber threat*. Berlin/Heidelberg, Germany: Springer

Searchlight Cyber 2023. Everest Ransomware group increases initial access broker activity. Searchlight Cyber Analysts. https://www.slcyber.io/everest-ransomware-group-increases-initial-access-broker-activity/

Stevens K 2009. The underground economy of the Pay-Per-Install (PPI) business. https://www.blackhat.com/presentations/bh-dc-10/Stevens_Kevin/BlackHat-DC-2010-Stevens-Underground-wp.pdf

Voce I & Morgan A 2021. *Ransomware victimisation among Australian computer users*. Statistical Bulletin no. 35. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78382

Wall DS 2021a. Cybercrime as a transnational organized criminal activity. *The Routledge Handbook of Transnational Organized Crime*. Routledge

Wall DS 2021b. The transnational cybercrime extortion landscape and the pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending. *European Law Enforcement Research Bulletin* 22

Warikoo A 2023. Perspective chapter: Ransomware. In B Eduard (ed), *Malware*. Rijeka: IntechOpen

Westbrook AD 2021. A safe harbor for ransomware payments: Protecting stakeholders, hardening targets and defending national security. *New York University Journal of Law and Business* 18(2): 391–469

Whelan C, Bright D & Martin J 2024. Reconceptualising organised (cyber)crime: The case of ransomware. *Journal of Criminology* 57(1): 45–61

Whelan C & Martin J 2023. 'Hacking the hackers': Reflections on state implemented disruption as a 'new model' for cyber policing. *Current Issues in Criminal Justice*. Advance online publication. https://doi.org/10.1080/10345329.2023.2281071

Wilner A et al. 2019. On the social science of ransomware: Technology, security, and society. *Comparative Strategy* 38(4): 347–370

Chad Whelan is a Professor of Criminology and Deputy Director, Deakin Cyber Centre for Research and Innovation at Deakin University.

David Bright is a Professor of Criminology in the School of Humanities and Social Sciences at Deakin University.

James Martin is a Senior Lecturer in Criminology in the School of Humanities and Social Sciences at Deakin University.

Callum Jones is a Research Fellow in the School of Humanities and Social Sciences at Deakin University.

Benoît Dupont is a Professor of Criminology and holder of the Canada Research Chair in Cyber-Resilience and the Research Chair in the Prevention of Cybercrime at Université de Montréal.

General editor, *Trends & issues in crime and criminal justice* series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology. Note: *Trends & issues in crime and criminal justice* papers are peer reviewed. For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website: www.aic.gov.au

ISSN 1836-2206 (Online) ISBN 978 1 922877 97 0 (Online)

https://doi.org/10.52922/ti77970

GPO Box 1936
Canberra ACT 2601, Australia

Tel: 02 6268 7166

www.aic.gov.au