NETTITUDE

AN LRQA COMPANY

The Current Threat Landscape: Ransomware

Contents

01 Introduction

Ransomware—or the crypto-ransomware that we are so accustomed to today—has been around for over a decade. This threat category is a type of malicious software [malware] that has resulted in catastrophic financial, reputational, and operational consequences for organisations worldwide. This problem continues to grow rather than fade into obscurity despite even the best efforts to eradicate it from existence. Ransomware's method of action can be gathered from its name; it will infect your file system and hold it for ransom.

While the majority of ransomware is known to enumerate the file system of infected devices and encrypt individual files, the capabilities and manner in which data and entire devices are compromised and victims are enticed to pay the ransom has continued to evolve. This type of malware has been and continues to be, very profitable with varying levels of effort required to develop, maintain, and successfully spread to affect the greatest number of potential victims possible.

Users have always been the weakest link in organisations and this trend continues throughout the entirety of 2022. As such, ransomware is trivial to spread and is a top payload for a quick turnaround in terms of profit [4], especially when targeted entities are major organisations with large user bases with large financial capabilities.

02 Revisiting Our Past Statistical Analysis of Ransomware

Previously, Nettitude conducted research on ransomware trends looking at new strains, variants, and financial impact to produce an article describing the findings [1]. This was back in March 2019, and since then, significant changes have been observed.

To summarise the trends observed from that report were early evidence of what we are seeing today. Ransomware continued to grow exponentially in prevalence year after year. As such, the sophistication and number of unique strains and variants also dramatically increased, and the financial burden related to ransomware infections skyrocketed. [4]

The Evolution of Ransomware

Early Ransomware

- Early ransomware utilised simple methods of spreading and infecting targeted devices. The most common method of infection was via Trojan horses that were distributed through phishing e-mail campaigns. While phishing is still the most common method of spreading ransomware, the manner in which more sophisticated modern ransomware spreads from device to device has evolved.

First Major Evolution

- The first major evolution was observed in the manner in which devices were infected. The first form of ransomware was spread on a one-to-one basis. Phishing e-mails were distributed, and individuals were infected on a per-device basis, but ransomware did not have the capability to self-replicate throughout a network.
- One of the early methods of self-replication in the wild was via the ability to enumerate open network shares accessible by an infected device. However, this initial implementation could only enumerate and infect additional open network shares that were already mapped to the victim device and assigned a drive letter.

Additional Methods of Spread

- Malvertising is malicious advertisements. Even with ad-blocking software, it is common to see advertisement banners on popular websites that one would believe to be benign. However, attackers began bidding on and purchasing advertisements that contained embedded code that would exploit vulnerabilities in browser software triggering malicious software to be downloaded and executed upon the advertisement loading. This allowed for malicious software to be installed from advertisements hosted on even legitimate, well-known, trusted websites that were not even compromised themselves.
- Exploit kits utilise landing pages that contain embedded code that, similar to malvertising, launch an exploit of a known or zero-day vulnerability in a web browser utilised by an unknowing client on the internet. Exploit kits can be offered as services and rented out, making them much more available to even low-level threat actors. Such software would fingerprint a user's web browser version and any plugins, determine if the browser itself or any installed plugins suffer from any vulnerabilities in the arsenal of the exploit kit instance and if so, would transparently redirect the user to a landing page that would deliver and execute the malicious payload installing ransomware and/or other malware.

Second Major Evolution:

- The second major evolution was the new ransomware sub-classification cryptoworms. This type of ransomware would function as a worm, where the initially infected device would be deemed patient zero. From there, the networks accessible by patient zero would be scanned and hosts on the network affected by the same vulnerability or additional vulnerabilities that the ransomware is capable of exploiting would be taken advantage of in an automated fashion. This led to entire networks and entire organisations running flat networks being completely compromised by ransomware and oftentimes rendered inoperable.
- Infection Methods Associated with the Second Major Evolution:
- Additional methods of infection were then introduced. Increased utilisation of zero-day vulnerabilities, manual device compromise, and payload execution are examples of this. There have been entire families of ransomware that have been delivered by miscreants searching for remote administration services such as Microsoft Windows Remote Desktop Protocol (RDP) exposed to the Internet, manually attacked to gain access to the device, and then a payload downloaded and executed by the attacker in manual rather than automated fashion.

Modern Ransomware Spread Methods:

- Throughout 2021 and 2022, supply chain attacks have been utilised for some of the largest and most successful compromises involving ransomware. Supply chain attacks involve compromising a vendor or service provider that manages and pushes out software and patches for popular applications that they manage, for example, from the cloud. Compromising such providers to push out ransomware instead of a legitimate patch or attacking the provider's website where the legitimate software is distributed and replacing the legitimate software with malicious software, has resulted in widely successful and extremely damaging attacks.
- However, phishing remains the top method of malware spread and successful infection, as well as the increased ease in accessing and utilising ransomware-as-a-service (RaaS) offerings.

03 History of Major Ransomware Families/Strains

Several well-known ransomware families/strains have made headlines over the past decade. Take note of the financial impact that resulted from the attacks conducted by threat actors developing and distributing these ransomware instances. A few notable examples are described below:

CryptoLocker

- One of the first major ransomware outbreaks that many people still reference today, albeit often in an incorrect fashion. Before ransomware was known and classified as 'ransomware' many people referred to such infections as 'CryptoLocker' which is actually just a family of ransomware.
- CryptoLocker was widespread between September 2013 and May 2014.
- The global cost of CryptoLocker infection is estimated to be approximately 3 million USD. [4]

TeslaCrypt

- TeslaCrypt was widespread between February and April 2015.
- In the first two months of its operation, hackers extorted approximately 76,000 USD by locking video game-related files on victims' computers. [4]

SamSam

- SamSam was widespread throughout 2015.
- It was estimated that since its release in 2015, the SamSam operators raked in nearly 6 million USD in ransom payments.
- The highest ransom payment made related to a SamSam infection was reported to be 64,000 USD. [4]

CryptoWall

- CryptoWall became the famous upgraded version of CryptoLocker due to its success in terms of overall destruction and financial gain for the attackers responsible for developing and distributing it.
- There were several versions of CryptoWall released; the most infamous being CryptoWall 3.0, but there have been reports of CryptoWall 5.1 being discovered in the wild.
- CryptoWall 3.0 alone was believed to have generated more than 325 million USD in ransom payments since its initial release. [4]

Cerber

- Cerber became a major player in the ransomware scene and was alleged to have been responsible for 26% of all ransomware infections worldwide in early 2017.
- The threat actors behind the Cerber ransomware are believed to have earned nearly 1 million USD in just a single year of operation.
- There have been no new instances or active operations related to the Cerber ransomware since 2018. [4]

NotPetya

- The NotPetya ransomware was notorious due to its destructive nature as a malicious malware that was disguised to be a functional ransomware, despite the lack of an efficient and successful decryption mechanism.
- Widespread throughout 2017, and it has been estimated that the total cost of NotPetya infections exceeds 10 billion USD in damages worldwide. [4]

WannaCry

- WannaCry was widespread throughout 2017 and is believed to have infected approximately 200,000 devices worldwide.
- First launched in May 2017, WannaCry took advantage of a security hole in Microsoft Windows XP now dubbed 'EternalBlue' and was allegedly developed by miscreants of North Korean descent.
- Attacks on average lasted five days before being successfully contained.
- Found to have impacted victims across a total of 150 different countries worldwide.
- The initial ransom amount demanded was 300 USD, but after seven days of non-payment, the ransom amount demanded doubled to a total of 600 USD.
- Was reported to have had a serious impact on the budget of the UK National Health Service, placing a dent of 73 million pounds in the budget due to damages as a result of infection. [4]

Ryuk

- Ryuk first appeared in the wild in August 2018.
- In the first four months of its operations, it was reported to have generated over 3.7 million USD in revenue for its operators. [4]

04 2021 Ransomware Trends

Throughout 2021, ransomware continued its meteoric rise in prevalence and sophistication. In fact, there are a few statistics compiled from various reports and research papers that highlighted the ransomware landscape throughout 2021.

Key Statistics

- Ransomware was a part of **10% of all breaches**; ransomware showed a 100% increase—double from the previous year—in frequency in 2021.
- It was reported that approximately **37% of global organisations** fell victim to ransomware in some fashion during 2021.
- The FBI's Internet Crime Complaint Center (IC3) reported that throughout just the first seven months of 2021 (between January and July 31, 2021) **2,084 ransomware complaints** were submitted. This indicates a **62% year-over-year increase.**
- While **90%** of ransomware incidents did not result in any loss, in **95%** of the cases where there were costs pertaining to a successful ransomware infection, the median loss was 11,150 USD.

However: the losses incurred by affected organisations ranged from a low of 70 USD to a **high of 1.2 million USD.**

- **12% of victims** paid out on ransomware attacks in the third quarter of 2021.
- In the **first six months** of 2021, there were **590 million USD** in ransomware-related costs reported.

This is a significant increase as per FinCEN who reported a total of 416 million USD in ransomware-related costs throughout the **entire year of 2020.**

Source: [3]

2021 Ransomware Statistics by Industry

The below table lists industries affected by ransomware and are ranked from top to bottom by the total volume of ransomware-related incidents by industry.

RANK	INDUSTRY
1	Education
2	Retail
3	Business, Professional, and Legal Services
4	Central Government
5	Information Technology
6	Manufacturing
7	Energy and Utility Infrastructure
8	Healthcare
9	Local Government
10	Financial Services

Table 1 – 2021 Ransomware Statistics by Industry

2021 Ransomware Statistics – BleepingComputer Analysis

The website BleepingComputer **(https://www.bleepingcomputer.com)** provides knowledge with articles and community research. Their weekly roundups every Friday summarise newly disclosed breaches, newly discovered ransomware strains, variants and decryption utilities and are the source of the following compiled data sheets and reports. The statistics that follow pertain to the data enumerated from the weekly roundups published on BleepingComputer.

Weekly Roundup Statistics Throughout the Year 2021

Data Breaches	141
New Ransomware Strains	110
New Ransomware Variants	236
New Ransomware Decryptors	16
New Ransomware-as-a-Service (RaaS) Offerings	3
New Wiper	1
New MBRLocker	1
New Ransomware Builder	1

Source: [2]

2021 Ransomware Strains by Quantity of Newly Discovered Variants

RANK	RANSOMWARE STRAIN	# ASSOCIATED VARIANTS
1	DHARMA	71 Variants
2	STOP	68 Variants
3	Xorist	9 Variants
4	Phobos	8 Variants
5	HiddenTear	5 Variants
6	Makop	5 Variants
7	Conti	3 Variants
8	JCrypt	3 Variants
9	Matrix	3 Variants
10	Nefilim	3 Variants
11	SFile	3 Variants
12	BigLock	2 Variants
13	Flamingo	2 Variants
14	Hakbit	2 Variants
15	HelloKitty	2 Variants
16	Rapid	2 Variants
17	REvil	2 Variants
18	Thanos	2 Variants
19	VHD	2 Variants
20	VoidCrypt	2 Variants
21	Zeppelin	2 Variants

Table 2 – 2021 Ransomware Strains by Quantity of Newly Discovered Variants [2]

* In addition to the above, a total of 36 ransomware strains were logged with one newly discovered variant

05 2022 Ransomware Trends

The ascension of ransomware increased throughout 2022. Statistics related to ransomware activity throughout November 2022 are listed below:

Key Statistics

- Cybersecurity and Infrastructure Security Agency (CISA) reported in February 2022 that it has been brought to their attention that there have been ransomware incidents targeting **14** of the **16 US critical infrastructure sectors.**
- After the first quarter of 2022, it has been estimated that businesses are victimised by ransomware attacks **every 40 seconds.**
- It has been estimated that by the end of 2022 there will be a business victimised by a ransomware attack **every 11 seconds.**
- In terms of potential financial impact, it is estimated that the global cost of damages resulting from ransomware-related attacks will be approximately **20 billion USD** annually.

It has also been hypothesized that ransomware generates approximately **1 billion USD** in revenue for cybercriminals on an annual basis.

- While the sophistication of ransomware itself continues to increase, and new spread methods are consistently being developed and utilised, infection via phishing e-mails continues to be the top method of infection.

Phishing e-mails continue to be the root cause of **two-thirds of all ransomware** infections.

- It is estimated that approximately **9% of the American population** has been a victim of a ransomware attack at some point.

Source: [3]

2022 Ransomware Statistics – BleepingComputer Analysis

The below statistics relate to data gathered and reported between 1st January 2022 and 18th November 2022.

Weekly Roundup Statistics Throughout the Year 202

Data Breaches	96
New Ransomware Strains	100
New Ransomware Variants	229
New Ransomware Decryptors	18
New Ransomware-as-a-Service (RaaS) Offerings	2
New Wiper	3

Source: [2]

2022 Ransomware Strains by Quantity of Newly Discovered Variants

RANK	RANSOMWARE STRAIN	# ASSOCIATED VARIANTS
1	STOP	131 Variants
2	Phobos	18 Variants
3	DHARMA	15 Variants
4	Chaos	11 Variants
5	VoidCrypt	10 Variants
6	Xorist	5 Variants
7	Babuk	4 Variants
8	MedusaLocker	4 Variants
9	Zeppelin	3 Variants
10	Dcrtr	2 Variants
11	Makop	2 Variants
12	Snatch	2 Variants
13	Sojusz	2 Variants

* In addition to the above, a total of 20 ransomware strains were logged with one newly discovered variant

Table 3 – 2022 Ransomware Strains by Quantity of Newly Discovered Variants [2]

2022 Data Breaches Related to Ransomware Infection – BlackFog Analysis

BlackFog is an information security provider that also conducts research and analysis and produces reports highlighting key statistics pertaining to ransomware. The below data reflects BlackFog's The State of Ransomware in 2022 report that details data enumerated throughout the first five months of 2022 (from January to May) regarding disclosed data breaches because of a ransomware infection.

2022 Ransomware-Related Data Breaches by Country

RANK	COUNTRY (% OF BREACHES)
1	United States of America [USA] (47%)
2	Rest of World [ROW] {Non-Major Market Countries} (23%)
3	United Kingdom [UK] (8%)
4	Canada (5%)
5	Japan (4%)
6	Germany (4%)
7	France (3%)
8	Australia (3%)
9	Italy (2%)
10	India (2%)

Table 4 – 2022 Ransomware-Related Data Breaches by Country [5]

2022 Ransomware-Related Data Breaches by Industry

RANK	INDUSTRY
1	Education
2	Government
3	Healthcare
4	Technology
5	Manufacturing
6	Services
7	Retail
8	Utilities
9	Finance
10	Other

Table 5 – 2022 Ransomware-Related Data Breaches by Industry [5]

2022 Ransomware Exfiltration Activity by Country

RANK	COUNTRY (% OF ACTIVITY)
1	Rest of World [ROW] {Non-Major Market Countries} (54%)
2	China (25%)
3	Russia (19%)
4	Ukraine (1%)
5	Iran (1%)

Table 6 – 2022 Ransomware Exfiltration Activity by Country [5]

2022 Ransomware-Related Data Breaches by Ransomware Strain

RANK	RANSOMWARE STRAIN (% OF BREACHES)
1	Other (33%)
2	LockBit (14.4%)
3	BlackCat (12.6%)
4	Conti (11.5%)
5	Hive (11.5%)
6	Vice Society (6.9%)
7	Lapsus$ (5.7%)
8	BlackByte (4.6%)

Table 7 – 2022 Ransomware-Related Data Breaches by Ransomware Strain [5]

2022 Known Ransomware-Related Data Breaches by Month Source: [5]

January 2022 (27 Breaches)

1. Bay & Bay Transportation
2. Belarusian Railways
3. Bernalillo County
4. Brookson Group
5. Carthage Schools
6. Crawford County
7. Curo Fund Services
8. Delta Electronics
9. Denso
10. Durham Johnston School
11. FinalSite
12. Griggsville-Perry School District
13. Hensoldt
14. Impresa
15. Indonesia Central Bank
16. John Diefenbaker International Airport
17. Linn County
18. Maryland Department of Health
19. Ministry of Justice in France
20. Moncler
21. Montreal Tourism Agency
22. New Bedford Police Department
23. Pembroke Pines in Florida
24. RR Donnelly
25. Subex
26. Thales Group
27. Weldco-Beales Manufacturing

February 2022 (28 Breaches)

1. Bridgestone-Firestone
2. Centralia College
3. Emil Frey
4. Expeditors
5. Extend Fertility
6. Hays USD 489
7. iTCo
8. Jawaharlal Nehru Port Trust
9. Jax Spine and Pain Centers
10. KP Snacks
11. LA: Spine Diagnostic & Pain
12. Lapus$
13. McDonalds
14. Meyer
15. Mizuno
16. Morley Companies Inc.
17. Neenah School District
18. New Zealand Uniforms
19. NFL's San Francisco 49ers
20. Nvidia Corporation
21. Ohlone Community College District
22. Oiltanking GmbH
23. Optionis Group
24. Swissport
25. Syndicat Intercommunal d-Informatique
26. Taylor Regional Hospital
27. The Royal Dublin Society
28. University of Neuchatel (UniNE)

March 2022 (25 Breaches)

1. Altoona Area School District
2. Aluminerie Alouette
3. AON
4. Bexar County Appraisal District
5. Bridgestone Americas
6. Denso Automotive
7. East Tennessee Children's Hospital
8. Fleetwood Area School District
9. Hellenic Post (ELTA)
10. Memorial Hospitality of Carbon County
11. Mercado Libre
12. Microsoft
13. NRA
14. Oklahoma City Indian Clinic
15. Okta
16. Partnership HealthPlan of California
17. Plainfield County
18. Rompetrol
19. Samsung
20. The Rehab Group
21. The Scottish Association for Mental Health (SAMH)
22. Toyota
23. TransUnion
24. Ubisoft
25. Vodafone

April 2022 (25 Breaches)

1. A&T University
2. American Dental Association (ADA)
3. Austin Peay State University (APSU)
4. Becker Law Office
5. Coca-Cola
6. Costa Rican Government
7. Deutsche Windtechnik
8. Elgin County
9. Florida International University
10. Funky Pigeon
11. Globant
12. HP Hood Dairy
13. Nordex
14. Panasonic
15. Parker Hannifin
16. Perusahaan Gas Negara (PGN)
17. Rio de Janeiro Finance Department
18. Russian Orthodox Church
19. Snap On
20. The Ince Group
21. The Works
22. Toei Animation
23. TrustFord
24. Ward Hadaway
25. Wyandotte County

May 2022 (26 Breaches)

1. AGCO
2. Auction.com
3. Austrian State of Carinthia
4. Bank of Zambia
5. Bulgarian Refugee Agency
6. Christus Health
7. Costa Rican Social Security Fund (CCCS)
8. De MontFort School
9. Fort Summer Municipal Schools
10. Hanesbrands
11. Kellogg Community College
12. Martin University
13. Mercyhurst University
14. Nikkei Inc.
15. North Orange County Community College
16. Omnicell
17. Onleihe
18. Opus Interactive
19. Quincy, Massachusetts
20. Regina Public Schools
21. Somerset County
22. SpiceJet
23. Top Aces
24. Vivalia
25. Washington Local Schools
26. Westchester County Library System

June 2022 (31 Breaches)

1. AMD
2. Arte Radiotelevisivo Argentino Group (Artear)
3. Brooks County in Texas
4. Buncombe County's Council on Aging
5. Cape Cod Regional Transit Authority
6. City of Alexandria
7. City of Palermo
8. Diskriter
9. FastShop
10. Fitzgibbon Hospital
11. Geographic Solutions
12. Glenn County Office of Education
13. Goodman Campbell Brain and Spine
14. Grand Valley State University
15. Macmillan Publishers
16. Mainzer Stadtwerke AG (MSW)
17. Medical University of Innsbruck
18. Montrose Environmental Group
19. Napa Valley College
20. Nichirin Co.
21. Pivotal Homes
22. Plainedge Public Schools
23. TB Kawashima
24. Tenafly Public Schools
25. The Shoprite Group
26. Unified Government of Wyandotte County and Kansas City
27. University of Pisa
28. Wabtec
29. Walmart
30. Wiltshire Fine Foods
31. Yuma Regional Medical Center (YRMC)

July 2022 (21 Breaches)

1. Agenzia delle Entrate
2. Bandai Namco
3. Baton Rouge Medical Center
4. Canadian College MontMorency
5. Canadian Town of Marys in Ontario
6. College of the Desert in California
7. Entrust
8. Gateway Rehab
9. Knauf Group
10. La Poste Mobile
11. Lamoille Health Partners
12. Mattituck-Cutchogue School District
13. Mooresville Schools
14. Narragansett Bay Commission
15. Port Phillip Prison
16. Professional Finance Company
17. Unnamed Company in South Korea [operating a 'call tax system']
18. Water Resource Department (WRD)
19. Waterloo Region District School Board
20. Wooton Upper School
21. WordFly

August 2022 (39 Breaches)

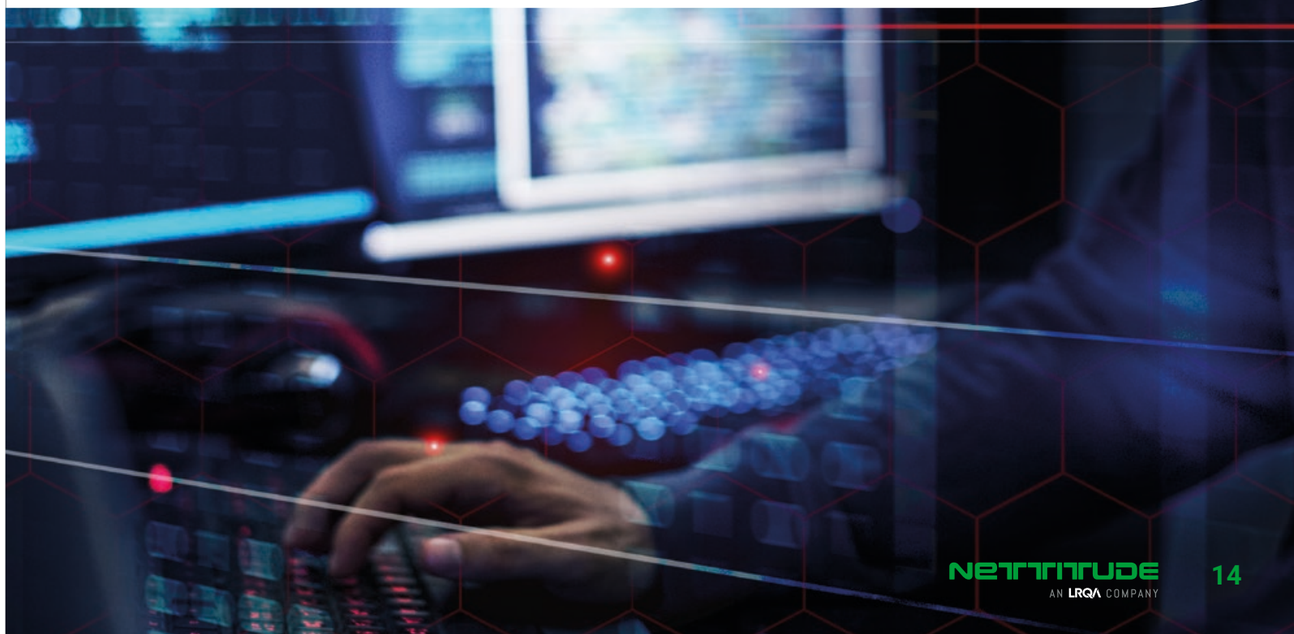
1. 7-Eleven in Denmark
2. Aceitera General Deheza
3. Advanced
4. Avamere Health Services LLC
5. Baker & Taylor
6. Chile's National Consumer Service (SERNAC)
7. Cisco
8. Colosseum Dental Benelux
9. Creos Luxembourg S.A.
10. DESFA
11. Disabilityhelpgroup.com
12. EmergeOrtho
13. ENI
14. Fremont County in Colorado
15. General Health System
16. German Chamber of Industry and Commerce (DIHK)
17. Holdcroft Motor Group
18. Instituto Agrario Dominicano (IAD)
19. Linn-Mar School District
20. Mansfield Independent School District
21. Montenegro's Parliament
22. Moon Area School District
23. OneTouchPoint
24. Onyx Technology
25. Orion Innovation
26. OSDE
27. Practice Resources LLC
28. Quebec Farmers Union (UPA)
29. Semikron
30. Sheppard Robson
31. Sierra College
32. Simon-Marius Gymnasium
33. South Staffordshire Water
34. Spanish National Research Council (CSIC)
35. Spinney's
36. TAP Air Portugal
37. The Center Hospitalier Sud Francilien (CHSF)
38. Valent U.S.A. LLC
39. Ypsilianti-area Utility

September 2022 (33 Breaches)

1. Alegria Family Services (AFS)
2. Aoyuan Healthy Life Group
3. Bell Canada
4. Bosnia and Herzegovina Government
5. Buenos Aires Legislator
6. Can Fin Homes
7. Chilean Court Systems
8. City of Bardstown in Kentucky
9. City of Wheat Ridge in Denver
10. Columbia County Charter of The Arc New York (NYSARC)
11. Damart
12. Daylesford Organic
13. Elbit Systems of America
14. Empress EMS (Emergency Medical Services)
15. FMC Services
16. Holiday Inn
17. Los Angeles Unified (LAUSD)
18. Medical Associates of Lehigh Valley
19. Minamiboso City Board of Education
20. NCG Medical
21. New York Racing Association
22. NJVC
23. North Macedonia's Agriculture Ministry
24. Oakbend Medical Center in Texas
25. Optus
26. redONE
27. Savannah College of Art and Design
28. Sierra College
29. South Redford School District
30. Suffolk County
31. TAP Air Portugal
32. Tift Regional Medical Center
33. Uber Technologies Inc.

October 2022 (44 Breaches)

1. 911 Services in Douglas County
2. Advanced
3. Aesthetic Dermatology Associates
4. ARVIG
5. Asahi Group Holdings
6. Ascension St. Vincent's Coastal Cardiology
7. AT&T
8. Bank of Brasilia (BRB)
9. CommonSpirit
10. Dialog
11. Electricity Company of Ghana (ECG)
12. Enlighten Designs
13. ESKOM
14. Esquimal
15. Ferrari
16. ForceNet
17. Hartnell College
18. Heilbronn Stimme
19. Hopital Pierre Rouques – Les Bluets
20. ID-Ware
21. Indianapolis Housing Agency
22. Johnson Fitness and Wellness
23. Kenosha Unified School District
24. Kingfisher Insurance
25. Marktel
26. Mars Area School District
27. Massy Stores
28. Medibank
29. MiTCON
30. Municipality of Chihuahua
31. Oomiya
32. Pendragon
33. Pinnacle
34. Record TV
35. Saskatoon Obstetrics and Gynecology Clinic
36. Simex Defense
37. State Bar of Georgia
38. Tata Power
39. The Ecuadorian Join Command of the Armed Forces
40. The Hibbert Group
41. Unimed Belem
42. Universidad Nacional De Educacion De Peru
43. Universidad Piloto de Colombia
44. Whitworth University



06 Summary

In conclusion, ransomware continues to be problematic and is not going anywhere anytime soon. The potential for high revenue and relative ease of distribution make ransomware a go-to weapon in the arsenal for financially motivated threat actors. While there are several cases where zero-day exploits are utilised to infect devices, social engineering remains the primary infection vector of ransomware.

Security awareness training, maintaining compliance, and proper implementation and enforcement of both administrative and operational controls by organisations are all imperative to ensure that a strong security posture is attained and maintained.

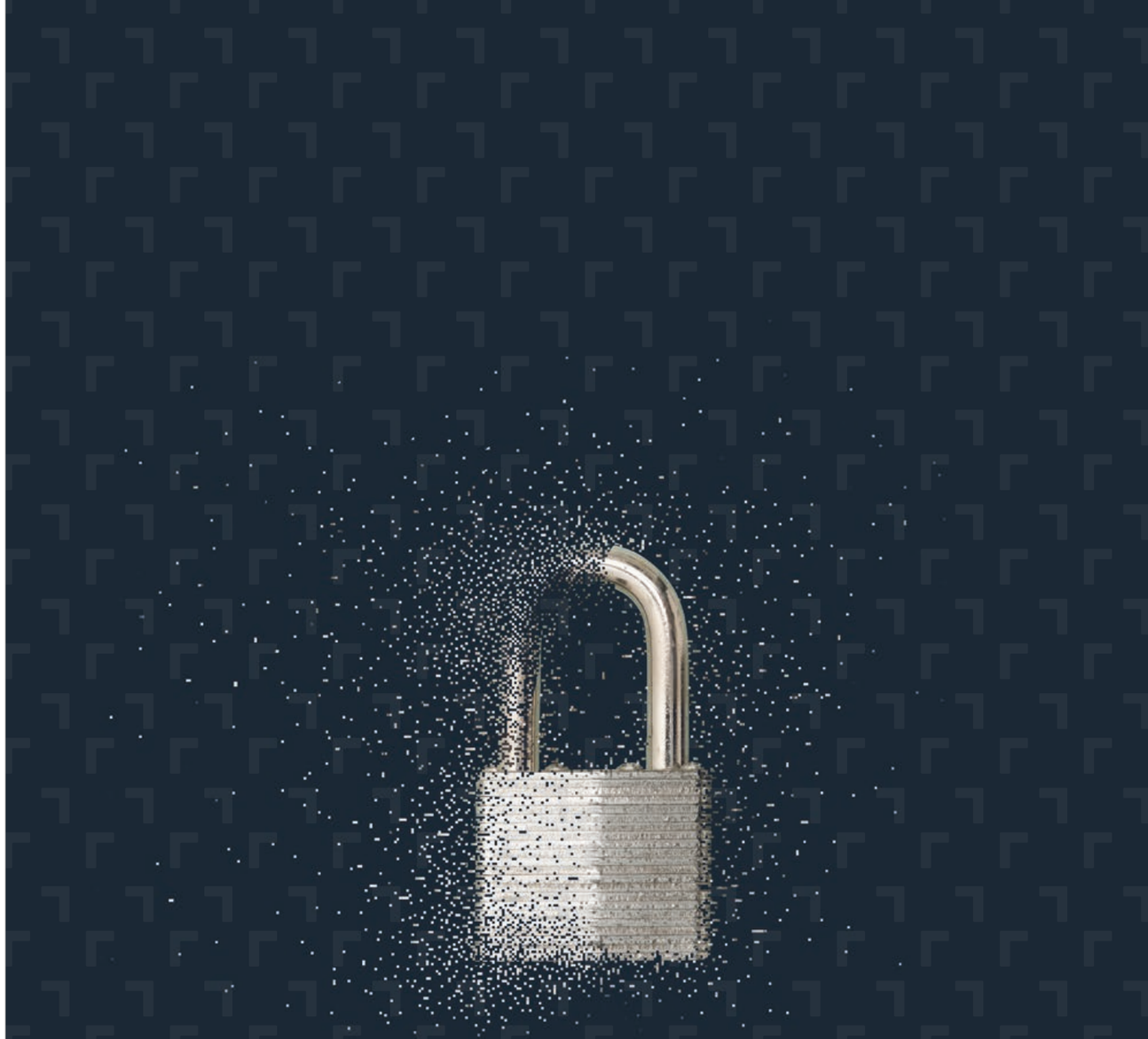
Nettitude can assist organisations in several ways to ensure that they possess and maintain a strong security posture to prevent the likelihood of successful compromise via multiple paths including through the deployment and execution of ransomware payloads.

Nettitude offers several services including penetration testing to assess an organisation's infrastructure from both an external and internal perspective. Assessment of the configuration and security of depolyed web servers and web applications. We can also support your organisation by assessing your ransomware resilience through a team of skilled experts with extensive experience of dealing with complex cyber investigations and ransomware attacks supported by cutting-edge technologies.

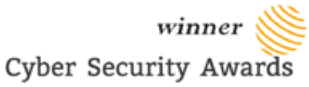
Appendix

Sources

1. Nettitude Blog – Ransomware: Where are we now?
   https://blog.nettitude.com/ransomware-where-are-we-now
2. BleepingComputer
   https://www.bleepingcomputer.com
3. TechTarget – "Ransomware trends, statistics and facts in 2022"
   https://techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts
4. DataProt – "Ransomware Statistics in 2022: From Random Barrages to Targeted Hits"
   https://dataprot.net/statistics/ransomware-statistics/
5. BlackFog – "The State of Ransomware in 2022"
   https://blackfog.com/the-state-of-ransomware-in-2022/



NETTITUDE
AN LRQA COMPANY



NETTITUDE
AN LRQA COMPANY

UK Head Office
Jephson Court, Tancred Close, Leamington Spa, CV31 3RZ

Americas
50 Broad Street, Suite 403, New York, NY 10004

Asia Pacific
18 Cross Street, #02-101, Suite S2039, Singapore 048423

Europe
Leof. Siggrou 348
Kallithea, Athens, 176 74
+30 210 300 4935

Follow Us

solutions@nettitude.com
www.nettitude.com