Ransomware: Emerging Opportunities in Threat Management

Introduction

Ransomware attacks are escalating all around the world at an alarming rate, especially in the wake of the COVID-19 pandemic. To highlight the severity and the implications of ransomware attacks, a recent speech by Lindy Cameron, UK's National Cyber Security Centre (NCSC) CEO, called ransomware the "most immediate danger to the UK, UK businesses and most other organizations."[1] In the US, a senior official in the Department of Justice commented, "ransomware attacks are to get a similar priority as terrorism."[2] This was following the Colonial Pipeline ransomware attack, which lasted several days and resulted in panic and gas price hikes across the East Coast of the US. There have been other attacks lately, such as ransomware attacks that exposed police files in Washington D.C. and the recent disruption of Ireland's hospital systems amid the Covid-19 breakdown. In addition, new vulnerabilities are identified as well as exploited daily. For example, in early December, a massive flaw in Log4j, a Java-logging library that is distributed free as open-source software by the nonprofit Apache Software Foundation, was discovered. According to The Wall Street Journal, Log4j "has been downloaded millions of times and is among the most widely used tools to collect information across corporate computer networks, websites and applications."[3] There have already been several ransomware attacks that have used Log4j, such as an attack on a crypto platform in late December as well as VMware's Horizon systems.[4,5]

As such attacks result in huge financial burdens (the 2017 WannaCry attack alone cost $4 billion on the global economy) and adversely affect people's personal safety, it is important that the governments, enterprises, and individuals take adequate measures to prevent and defend against ransomware.[6] This is where the major Cybersecurity companies come into the picture, with new focused tools and enhanced existing offerings, to provide protection and recovery from ransomware attempts and attacks.

In this report, we will provide an overview of ransomware and cover recent ransomware trends and attacks. We will also discuss important cybersecurity technologies and cyber security companies' product offerings.

What is Ransomware?

According to the United States Cybersecurity and Infrastructure Security Agency (CISA), "Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption."[7] The European Union Agency for Cybersecurity states that these attacks typically occur via the same traditional channels of malware, "like via phishing email, water holing – and other drive-by attacks," and "in rare occasions and for high profile targets ransomware might be planted by more sophisticated methods in a direct, targeted attack."[8] Ransomware can be used to restrict access to critical data through encryption, and in other instances, ransomware has been used to take control of an entire system. In addition, if the ransom isn't paid, ransomware actors typically threaten to sell or leak the data or information that is behind held for ransom.

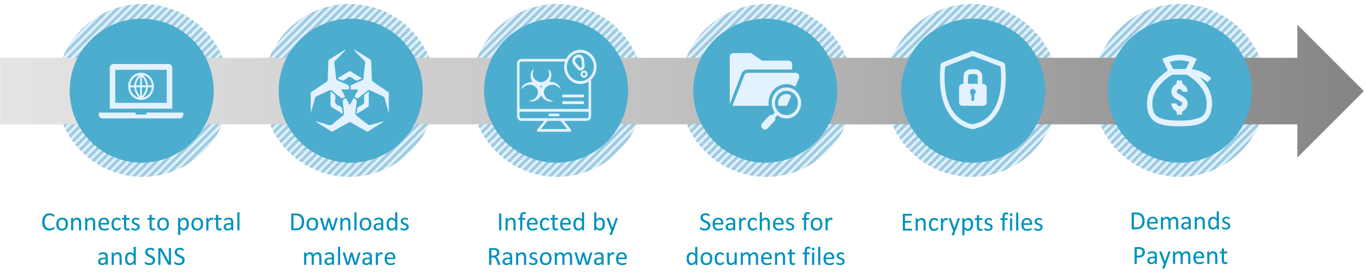
So how does a ransomware attack occur? The Computer Security Resource Center (CSRC), part of the National Institute of Standards and Technology in the US Department of Commerce, provided a straightforward example of how a ransomware attack might occur.[9]

Ransomware Attack Process:

1. A user is tricked into clicking on a malicious link that downloads a file from an external website.
2. The user executes the file, not knowing that the file is ransomware.
3. The ransomware takes advantage of vulnerabilities in the user's computer and other computers to propagate throughout the organization.
4. The ransomware simultaneously encrypts files on all the computers, then displays messages on their screens demanding payment in exchange for decrypting the files.

(Source: CSRC)

Figure 1: Ransomware Attack Process Chart



(Source: Gartner & AhnLab, Inc. [10] and Nasdaq)

Rise of Ransomware

Cybersecurity Ventures, a leading researcher of the global cyber economy, expects cybercrime to cost the world more than $6 trillion by the end of 2021 and expects the cost to grow even higher to $10.5 trillion by 2025.[11] Not surprisingly, ransomware is, and will be contributing to the rise in these cybercrime costs. For example, in another Cybersecurity Ventures report, global ransomware damage could reach $250 billion by 2031.[12]

In addition, ransomware's growth rate is startling. In a Sophos "The State of Ransomware 2021 Report," "the number of organizations that paid the ransom increased from 26% in 2020 to 32% in 2021, although fewer than one in ten (8%) managed to get back all of their data."[13] To make matters worse, year over year, the average total cost of recovery from a ransomware attack more than doubled between 2020 to 2021, rising from $761,106 to $1.85 million, respectively, an increase of over 143%.[14] Palo Alto Networks' cybersecurity consulting group, Unit 42, reported that the "average ransomware payment climbed 82% since 2020 to a record $570,000 in the first half of 2021" after already rising 171% in 2020.[15]

The business model behind ransomware attacks is also evolving as threat actors continue to evolve and innovate. With the recent rise of attacks as well as the rise of the monetary value of the ransoms, Ransomware-as-a-Service (RaaS) has emerged as a standalone business model. RaaS providers supply the market with a subscription services for cybers criminals, providing them with ready-made ransomware software tools to help them carry out ransomware attacks. This means that the barriers to entry to initiate ransomware attacks are low, as RaaS enables less skilled and less well funded criminal actors to participate in the ransomware activity.

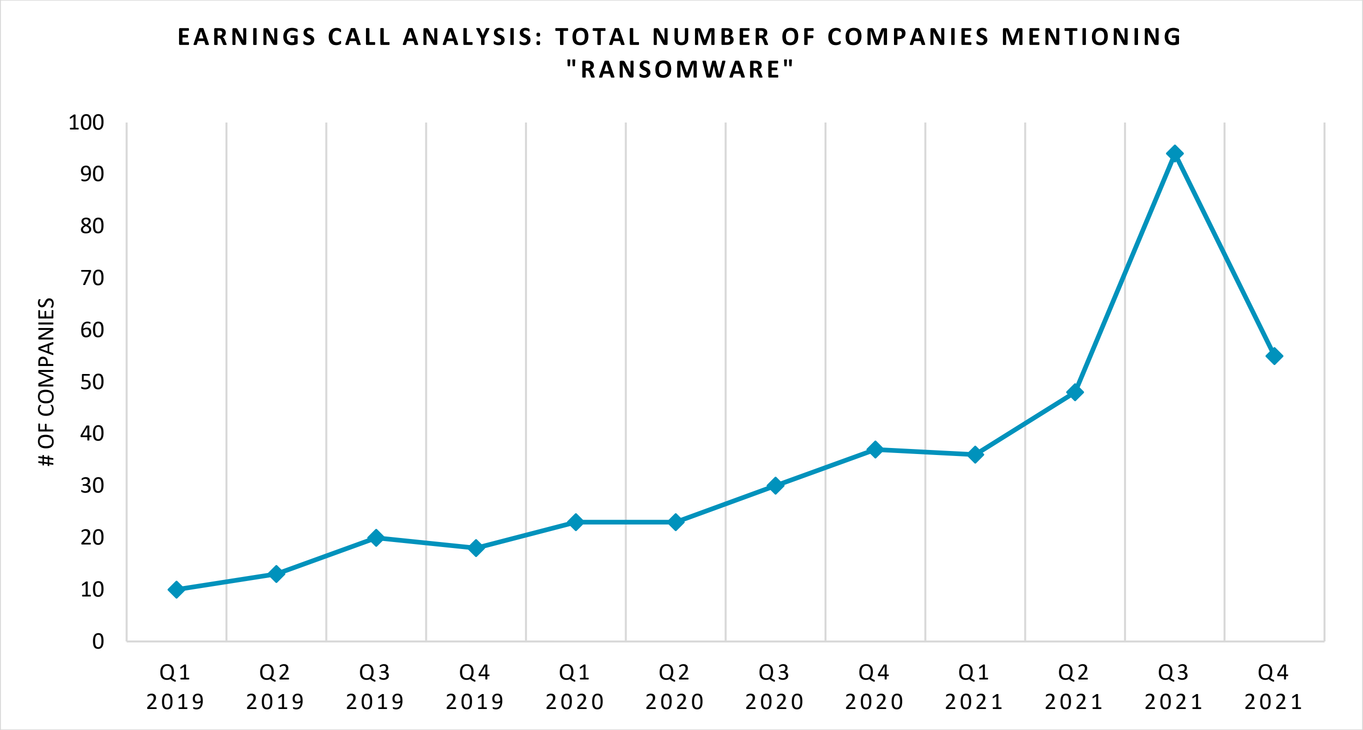
Recent Ransomware Attacks: 2021

Given the rise in ransomware attacks, we wanted to provide a summary of the most recent high-profile attacks, as it provides insight into the severity and breadth of the ransomware problem. Below is a summary of the most recent ransomware attacks that have wreaked havoc on critical infrastructure, businesses, and organizations, updated through December 31, 2021.

- The most high-profile ransomware attack in 2021 was the Colonial Pipeline attack in the US, which has been linked by the FBI to the DarkSide group. According to Reuters, the attack on the Colonial Pipeline "occurred using a legacy Virtual Private Network (VPN) system that did not have multifactor authentication in place."[16] The ransomware attack resulted in the company shutting down operations and freezing their IT systems. The ransomware led to a shutdown of Colonial Pipeline's pipeline system, which meant that nearly half of the East Coast lost or experienced a decrease in the supply of gasoline, diesel, home heating oil, jet fuel, and military supplies. The ransomware attack drew headlines as some locations experienced panic buying, escalating the fuel shortage even more.[17] Colonial Pipeline stated they paid a ransom of nearly $5 million in cryptocurrency to regain access to their system.
- In Q3 2021, Kaseya, a provider of software tools to Managed Service Providers (MSP), received a ransomware demand for $70 million.[17] The virus infiltrated Kaseya's remote monitoring VSA platform and affected the customers of the MSPs, the attackers exploited a zero-day vulnerability, possibly with a SQL Injection (SQLi), to remotely access internet facing VSA Servers.[18] The gravity of the issue soon started to sink in when thousands of small businesses were impacted with their systems getting locked. REvil, a cyberattack organization, claims that 1 million systems were infected. Pennsylvania-based Famous Smoke Shop, Morgan County Schools in Tennessee, U.S. were some of the victims. According to Raconteur, a publisher, apparently a universal decryption key was obtained on 22 July through a "trusted third party" and Kaseya escaped paying any ransom amount.[19]
- Natural gas supplier, Super Plus, was a victim of a ransomware attack in mid-December 2021 that caused a disruption to their systems. According to CPO Magazine, "Superior Plus is a multi-billion-dollar company supplying energy-related products and services to over 780,000 customer locations in the United States and Canada." [20]
- Danish wind turbine giant Vestas Wind Systems detected cyber security breach on November 19, and immediately shut down its IT systems across multiple business units and locations. [21] The company later confirmed that ransomware was indeed used, and the incident resulted in data getting compromised, but the wind turbine and supply chain operations were unaffected.
- Some of the other organizations affected by ransomware attacks in recent months include the Swiss online customer outlet Comparis, American fashion brand and retailer Guess, municipality of Anhalt-Bitterfeld (located in eastern Germany), and Cloudstar (a Florida based company that provides technology for hundreds of title companies and lenders). [22]

Increase in Ransomware Mentions on Earnings Calls

The rise of ransomware attacks has coincided with a rise of ransomware mentions on earnings calls. Looking at earnings call transcripts from FactSet,[23] companies mentioning "ransomware" increased significantly between 2020 and 2021. For example, through the first nine months of 2021, "ransomware" mentions more than doubled on a year-over-year (YoY) basis. There was also a 95% increase in the number of companies mentioning "ransomware" between Q2 to Q3 2021, coinciding with the spike in ransomware attacks highlighted above. The number of companies declined back to Q2 levels as the number of attacks and concerns subsided. It will be interesting to see if this picks up in Q1 2022 as a result of the recent Log4j vulnerability.



Source: FactSet & Nasdaq

How are Cybersecurity Companies Combating Ransomware?

Two key technologies are being deployed to combat and protect against ransomware: Artificial Intelligence (AI) and an offshoot of AI, Machine Learning (ML). AI is vital to stopping ransomware because, according to AI Magazine, "AI can rapidly – if not immediately – detect when attackers are moving through systems before the ransomware deploy button is hit. This is because AI can contextualize and consolidate the wide variety of signals and markers left by attackers as they move through systems to reach their intended goal."[24] According to CrowdStrike, a leading cybersecurity company, ML becomes critical to combating ransomware because "it can teach a machine how to predict the answer to a question it has never encountered before, replacing processes that would otherwise require arduous and protracted human analysis."

Most AI and ML technologies are deployed in endpoint protection platforms (EPP) and endpoint detection and response (EDR) solutions. EPPs tend to provide businesses and organizations with anti-malware solutions, such as scanning and analysis, while EDRs provides threat detection, investigation, remediation, and recovery solutions for endpoints (which include end-user devices that access networks and systems, such as laptops, mobile devices, desktops, etc.). EDRs are becoming popular because, according to DarkReading, they provide "continuous monitoring and threat detection" and "automated response to threats discovered during monitoring," which help to prevent and control ransomware.[25] Another technology that is similar, yet different, than EDR is Extended Detection and Response (XDR). While EDR focuses on protecting the endpoints, XDR provides a single proactive solution, and as its name implies, XDR provides an "extended" view of a company's network and endpoints, providing a wide view across all security endpoints as well as email, cloud computing, and other connections. According to Dark Reading, XDR "will typically analyze the collected data, act upon the threats, and send unified alerts and action items to security analysts," producing security analysts with the ability to "focus their time and energy on the most critical incidents."[26]

Examples of Cybersecurity Companies Providing Anti-Ransomware Solutions & Products

Which companies are combating ransomware through end-point protection and anti-malware solutions? The table below provides a snapshot of some (but not all) of the cybersecurity companies and tools that provide ransomware protection, detection, and remediation & recovery solutions.

Cybersecurity Ransomware Protection Products & Technologies

Company Name	Approach/actions to prevent or stop Ransomware	Major Product/ Service Name
Trend Micro Incorporated (4704-JP)	• *Email and Web Protection* - XGen (combines machine learning, exploit detection, and sandboxing) based email protection to prevent ransomware (phishing emails are often the most common way of ransomware infection). • *End Point Protection* - Using XGen security's capabilities, like behavioral analysis and high-fidelity machine learning, XGen helps prevent ransomware attacks. • *Network & Server Protection* - tools to block ransomware attacks in networks and prevent servers from ransomware attacks.	Deep Discovery Inspector (click here)
Palo Alto Networks (*PANW-US*)	• *Extended Detection & Response* – Cortex, a Security Operations Center tool, provides instantaneous threat stoppage in all locations, through end point, cloud, and network protection. • *Artificial Intelligence* - Palo Alto uses Artificial Intelligence (AI) to prevent threats and machine-learning (ML) models to stop zero day or unknown threats. • *Response & Visibility* - Cortex XSOAR and Cortex Xpanse provide incident response and visibility, respectively.	Cortex (click here)
Cisco (*CSCO-US*)	• *Enterprise Network Security* - Umbrella provides a portfolio of products that span from networks to the DNS layer to email to the endpoint; to prevent the multifrontal attacks and threats. • *EDR & XDR* – The Secure Endpoint tool provides both EDR and XDR capabilities to detect and respond to cyber threats, such as ransomware.	Cisco: Umbrella / Secure Endpoint (click here)
CrowdStrike (*CRWD-US*)	• *Endpoint Protection* - The company uses its existing product Falcon platform to fight Ransomware attacks. • CrowdStrike uses AI-powered ML and behavioral indicators of attack (IOAs) to identify and block ransomware.	Falcon (click here)
Rapid7 (*RPD-US*)	• Rapid7 helps in identifying and prioritizing assets which are more prone to malware attacks through its vulnerability risk management program. • *Vulnerability Management* – InsightVM provides insight into vulnerabilities through cloud-based security and data analytics • *Detection* - Its cloud SIEM InsightIDR helps in detecting ransomware using the endpoint agents and configured foundational event sources.	InsightVM (click here), InsightIDR (click here)
Check Point Software Technologies Ltd (CHKP-US)	• *Endpoint Protection* – Harmony Endpoint provides endpoint protection to counter ransomware. • It uses ML algorithms and behavioral analysis to shutdown malwares, and automated recovery solutions.	Harmony Endpoint (click here)

Ransomware’s Impact on the Cybersecurity Investment Theme

With the increase in the number of ransomware attacks coupled with the adaptability and sophistication of the attacks, demand for ransomware protection products and services is expected to increase. Moreover, the recent availability of Ransomware-as-a-Service (RaaS, enabling less-skilled criminal actors to participate in the ransomware activity), and attacks on third party providers increased the complications and depth of ransomware threat. With the increasing cybercrimes cost (to reach $10.5 trillion by 2025 according to Cybersecurity Ventures) major cybersecurity providers are expected to invest more on product development and services to address the new threats.[27] In fact, it is predicted that the ransomware protection software industry itself expected to grow at a compound annual growth rate (CAGR) of 15.2% over the 2020 – 2027 time period.[28] Thus, cybersecurity companies are going to play an even more important role in how businesses and organizations conduct day-to-day operations as the world moves increasingly into the cloud and data becomes more vulnerable.

Nasdaq's Cybersecurity Indexes offer investors a simple way to incorporate this theme into their portfolios through companies protecting data from data breaches and cyberattacks. To learn more about Nasdaq’s Cybersecurity Indexes, please visit the Nasdaq Cybersecurity Indexes website.

[1] https://www.ncsc.gov.uk/speech/lindy-cameron-first-year

[2] https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/

[3] https://www.wsj.com/articles/what-is-the-log4j-vulnerability-11639446180

[4] https://www.bankinfosecurity.com/crypto-platform-suffers-log4j-related-ransomware-attack-a-18219

[5] https://www.bleepingcomputer.com/news/security/night-sky-ransomware-uses-log4j-bug-to-hack-vmware-horizon-servers/

[6] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

[7] https://www.cisa.gov/stopransomware

[8] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/ransomware

[9] https://csrc.nist.gov/projects/ransomware-protection-and-response

[10] https://www.gartner.com/imagesrv/media-products/pdf/ahnlab/ahnlab-1-2VS6RBW.pdf

[11] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[12] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

[13] https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year.aspx

[14] https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year.aspx

[15] https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/

[16] https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

[17] https://www.forbes.com/sites/daveywinder/2021/07/05/70-million-demanded-as-revil-ransomware-attackers-claim-1-million-systems-hit

[18] https://news.sophos.com/en-us/2021/07/02/kaseya-vsa-supply-chain-ransomware-attack/

[19] https://www.raconteur.net/technology/the-five-most-important-ransomware-attacks-of-2021/

[20] https://www.cpomagazine.com/cyber-security/natural-gas-supplier-superior-plus-suffers-a-ransomware-attack-similar-to-colonial-pipelines/

[21] https://www.securityweek.com/wind-turbine-giant-vestas-confirms-ransomware-involved-cyberattack

[22] https://www.blackfog.com/the-state-of-ransomware-in-2021/

[23] Using FactSet transcript data, the total number of earnings call transcripts per year varied from a low of 6,475 in Q2 2020 to a high of 9,611 in Q1 2019. In the study, the average number of transcripts analyzed was 7,902. (Data source: FactSet). Total earnings transcripts in Q1 2019: 9,611 with 10 companies mentioning "ransomware". Total earnings transcripts in Q4 2021: 7,171 with 55 "ransomware" mentions.

[24] https://aimagazine.com/technology/why-ai-critical-weapon-war-ransomware

[25] https://www.darkreading.com/edge-articles/xdr-101-what-s-the-big-deal-about-extended-detection-response-

[26] https://www.darkreading.com/edge-articles/xdr-101-what-s-the-big-deal-about-extended-detection-response-

[27] https://globalnews.ca/news/7955903/ransomware-cyber-attacks/

[28] https://www.businesswire.com/news/home/20210707005445/en/14.5-Billion-Worldwide-Ransomware-Protection-Industry-to-2027---Impact-Analysis-of-COVID-19---ResearchAndMarkets.com

Nasdaq® is a registered trademark of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence and carefully evaluate companies before investing. ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.