Student Occasional Paper Series No. 7 | April 2024

Lorenz Ransomware: The Impact of Standalone Ransomware on Businesses

By Ryan Mason

Editor. Aaron Brantly

Abstract

Ransomware poses an escalating and persistent threat to businesses, facilitating large scale theft and encryption of sensitive files and documents. This research delves into the impact of ransomware on companies, with a specific focus on instances where internal data is publicly exposed by hackers. By analyzing the aftermath of the Lorenz ransomware group attacks, we assess the extent of file theft, the overall breach size, and the companies affected by the cyber-attacks, including their size, their industry, and their location. Our findings reveal vast quantities of vital records compromised, including emails, financial data, blueprints, and social security numbers. This showcases ransomware's potential for severe financial and reputational damage to businesses, impacting not only their operations but also their customer base. The study highlights the importance of cyber resilience through technologies, training, and transparency. It underscores ransomware's complex repercussions, necessitating coordinated technological, policy, and human readiness efforts to develop security and mitigate potential societal harms.

Introduction

Ransomware is a form of malware designed to extort its victims. Once it infects a system, this malicious code will encrypt every file it can to render it useless. This can include everything from photos, to emails, to the browser you use every day. It is designed in such a way to pressure victims into paying a ransom to regain access to their data or prevent their data from getting leaked. Since its inception, ransomware has continually evolved alongside technological advancements to expand its capabilities.

Ransomware dates to 1989. At that time, the internet was in its infancy, and society was just beginning to grasp the intricacies of this new technology. In December of 1989, Joseph Popp, an evolutionary biologist with a Harvard education, developed what would later become known as PC Cyborg, or the AIDS Trojan. Popp obtained stolen mail subscriber lists from well-connected sources: the World Health Organization's AIDS conference and PC Business World Magazine.[1] Using these lists, Popp distributed 20,000 seemingly harmless floppy disks, each labeled "AIDS Information Introductory Diskette".[2] These disks contained surveys that claimed to predict an individual's risk of contracting AIDS.[3] These disks contained surveys that claimed to predict an individual's risk of contracting AIDS.[4]

Upon inserting the malicious floppy disk, nothing would immediately happen. The program would run as expected, presenting researchers with the survey[5]. However, beneath the surface lurked a ticking time bomb. After the computer had been turned on and off approximately 90 times, the AIDS trojan would execute, encrypting the names of all files on the C: drive. Upon encryption a red screen would appear reading "It is time to pay for your software lease from PC Cyborg Corporation.[6] Complete the INVOICE and attach payment for the lease option of your choice."[7] The victims were instructed to pay $189 - about $465 USD in 2023. Victims were instructed to send their payment to a Panama P.O. box.[8] Victims were instructed to send their payment to a Panama P.O. box.[9]

The infection wrought havoc among its victims. While some realized that the encryption employed by the AIDS trojan was a weak symmetric algorithm and easily remedied it, others were less fortunate[10]. Worried that their files were unrecoverable, victims wiped their hard drives, losing valuable documents. Soon, security researchers released tools to assist the victims. With those tools and the complexity of sending money to Popp's P.O. box kept him from profiting off his malware.[11]

A month later in January 1990, Popp was arrested at Amsterdam airport. Dr. Popp was returning from an AIDS conference in Nairobi, where the trojan was a highly discussed topic. He caught the attention of Amsterdam police at the Schipol Airport after he wrote "DR. POPP HAS BEEN POISONED" on a fellow traveler's suitcase.[12] Upon investigation and an ensuing search of Dr. Popp's bag, they discovered a case labeled "PC Cyborg Corp".[13] Not long after, Popp was arrested in Ohio and extradited to the UK for ten counts of blackmail and criminal damage[14].

Upon his arrest, Popp became increasingly erratic and showed signs that he was unfit to stand trial.[15] The doctor reportedly wore condoms on his nose, a cardboard box on his head, and curlers in his beard to thwart the risk of radiation[16]. In November of 1991, the UK judge ruled that he was unfit to stand trial and deported him back to the US, where he remained free until his death in 2007.[17]

Controversy remained over the subject even after the trial. Virus Bulletin released a report detailing Popp's plan, calling into question how premeditated of a plan the AIDS trojan really was.[18] Reports claimed that he had planned to send out an additional 2 million copies of the virus.[19]

While the AIDS trojan was certainly impactful, it had several limiting factors. First, disseminating the trojan was a long and laborious process. Without the modern connectivity that would enable remote injection of malicious code, Popp had to resort to the mail system and unwitting victims inserting the disk into their device. He did not know if a computer had been infected, or if a user had sent the payment until he had received it. Second, simple symmetric encryption made it easy for victims to decrypt. A victim would merely need the key or passphrase to decrypt the files. Third, payment through a P.O. box proved too much of a hassle for victims to follow through.

Our increasingly interconnected world opens vast gateways for communication and data transfer, but also makes hackers' lives much easier. Hackers no longer rely on snail mail to infect a system. The advent of asymmetric cryptography filled a much-needed hole for data security related matters, but also gave ransomware hackers vastly more power once they gained access to a victim machine. Now, victims need a hacker's private key, which is nearly impossible to discover without a leak of hacker data. The introduction of ecommerce allows for fast, convenient payments in online marketplaces, and anonymizing blockchain technologies allow bad actors to receive payment with little to no trace.

Specific advances facilitated the rapid development of ransomware. The 2010s brought about cryptocurrency, a digital, decentralized, and encrypted medium of financial exchange.[20] The most popular early cryptocurrency was Bitcoin. Bitcoin made it possible for hackers to secure payments in an accessible and anonymous manner through criminal enterprise. In 2013 CryptoLocker took the anonymity of Bitcoin and added more powerful encryption.[21] This set the precedent for most ransomware throughout the rest of the 2010s. Thousands of ransomware programs through the decade were found to leverage the same architecture due to their profitable nature.

Ransomware is increasingly prevalent and sophisticated. Ransomware attacks typically render the data of target individuals or organizations inaccessible or unusable until a ransom is paid. *Encryptor* is the most prevalent form of ransomware. It will encrypt a system's files, effectively locking victims out of their own data.[22] The effects of encryptor ransomware can be devastating. A well-known variant of encryptor ransomware is WannaCry. WannaCry encrypts all files on an infected system and includes Bitcoin ransom demand to decrypt it. Additionally, some Encryptor ransomware variants have a chat function for victims to contact hackers to negotiate the ransom terms and to facilitate instructions on how to pay.

Locker ransomware denies access to a user's system. Unlike encryptor ransomware, it does not delete or encrypt files. Instead, it prevents users from logging into their devices unless they pay a ransom. Locker ransomware typically displays a lock screen with instructions on how to pay the ransom and a countdown timer to foster a sense of urgency. The lock screen may attempt to imitate a form of government body to intimidate the victim. Intimidating victims by falsely claiming that the victim has engaged in an illegal activity and must pay the ransom to avoid punishment.[23] For instance, the FBI MoneyPak (Reveton) ransomware masqueraded as an FBI operation, alleging illegal activity had been detected on the victim's device. Reveton would put the system into a logic loop, restricting the victim from their web browser or application the malware infected.[24] The malware would demand $100 to $400 for unlocking the device.[25]

Scareware is another form of ransomware that uses intimidating advertisements, pop-ups, and emails to pressure victims into paying for phony software. Once installed, scareware will alert the user to some form of fake malware running on the user's system and demand they pay for the software to get rid of any malware. Once installed, scareware will either do nothing and report the problem was fixed or insert its own malicious software into the system, often demanding more money to fix new phony problems.[26] Malicious actors use this and other social engineering tactics to break into a system to steal data and install their own malicious software.

Doxware, or leakware, threatens to leak sensitive information if a ransom is not paid. Once a system is infected, hackers will search for sensitive information and offload it for their own use. Once they have gotten the data, the hackers will demand a ransom to not leak the sensitive data.[27] In 2021, Apple contractor and MacBook manufacturer Quanta was attacked by REvil ransomware authored by the Russian hacking group Sodinokibi. The ransom was set at $50 million. The hackers demanded payment of the ransom and threatened to leak the schematics for new MacBooks. Apple and Quanta refused to pay the ransom which resulted in massive leaks of new designs and prototypes for then-upcoming MacBooks and iMacs.[28]

Of the four categories examined, ransomware can also be a standalone software or sold as a service (Ransomware as a Service). Both categories have shown success, achieved through different means. Standalone ransomware provides hackers the advantage of control over all ransom payments. This strategy incurs heavy upfront costs to build and test the malware, posing a larger risk associated with target selection. One of the most well-known and damaging standalone ransomware attacks to date was WannaCry. In May 2017, millions of Windows laptops were infected by this Encryptor ransomware, suspected to be developed by the Lazarus Group, a North Korea-affiliated hacking ring. The malware exploited the EternalBlue zero-day vulnerability in Windows operating systems, initially identified by the National Security Agency. It infected victims' computers via remote SMBv2 code execution, installing a malicious dropper payload that searched for and encrypted files like .mp3, .doc, and .zip, demanding Bitcoin payment for decryption. WannaCry infected approximately 230,000 Windows devices, causing an estimated $4 billion in global damage. The hackers demanded $300 in Bitcoin from victims, raising the price to $600 if the ransom was not paid within a certain time.[29] The malicious software would check to see if it could connect to a certain URL, and if it was successful, it would shut down and not complete the encryption. Security researcher Marcus Hutchins discovered this kill switch and bought the domain WannaCry was seeking, effectively putting an end to all new WannaCry infections.[30] This singular attack crippled critical infrastructure, businesses, and public internet access. While WannaCry's authorship is unconfirmed, the consensus is that the North Korean-backed Lazarus Group was responsible. In September 2018, the U.S. Department of Justice charged the North Korean hacker Park Jin Hyok for ties to the WannaCry attacks.[31]

Like WannaCry, Lorenz is considered a standalone ransomware. Unlike WannaCry, it lacked a vulnerability as powerful as EternalBlue to spread quickly across millions of devices. This is a problem not exclusive to Lorenz. For standalone ransomware groups, it can be challenging to find

vulnerabilities that can be both consistently exploited and allow them to perform the tasks they need to do. Not only that, but manually checking networks for vulnerabilities is time consuming and expensive. Over its two-year lifespan, only 70 companies were posted on Lorenz's blog site - a mere fraction of what WannaCry achieved.

To solve this problem of discovering vulnerable networks, the Ransomware as a Service business model was born. Ransomware as a Service (RaaS) is a pre-built ransomware that a hacking group sells on dark web forums. Hackers agree to pay RaaS organizations a cut of the ransom payment, and in exchange the RaaS group will handle the payment process, the customer support, and any post-operation activity. The "hacker customer" merely needs a vulnerability to exploit. This makes RaaS a much more enticing solution for most hackers.

RaaS groups can vastly increase the scope of their target by outsourcing finding vulnerabilities and infecting systems. Before it was shut down, the LockBit 3.0 blog showcased roughly a thousand companies' data, and the Hive ransomware is estimated to have infected 1,300 systems, bringing in an estimated $100 million in ransom payments.[32]

Ransomware attacks can be carried out using a variety of methods, including email phishing campaigns, malicious websites, and infected software downloads. Once the malware has infected a system, it can quickly spread to other computers and devices on the same network, causing widespread damage and disruption.

Until relatively recently hackers used ransomware to encrypt devices on a company's network and hold them hostage. More recently, hackers have started using a "double extortion" tactic. This double extortion not only locks down the victim's computers and encrypts their backups, but also threatens the victim that their data will be leaked if they do not comply and pay the ransom within a certain period. Victims then face a decision: pay the ransom and hope to get their data unlocked (studies show that 24% of victims never get their data back even after paying the ransom)[33] or refuse to pay and suffer the financial and reputational consequences of sensitive data getting leaked out into the dark web. Companies must evaluate the impact a ransomware attack has on them and the public. Critical sectors, such as the medical industry, must make plans to mitigate the risk of ransomware both before and after an attack. Failure to do so may result in the loss of critical infrastructure. Extortion innovations have given way to a new "triple extortion" model. It takes data theft and data encryption and adds on another cyber-attack to coerce victims into paying.

Ransomware is a challenging scenario for companies. FTC Title 16 CFR Section 318 mandates companies to report data breaches to customers and the media.[34] The law, however, does not require companies to report what method by which their data was breached, which can discourage companies from being fully transparent in their reports. A company's net worth can take a hit depending on how its systems were breached and what data was stolen. After a federal investigation, it was discovered that although claiming it had industry-leading cyber security, Equifax had been using decades-old infrastructure and extremely weak security to protect its data.[35] Although not a ransomware attack, the bad press from this breach resulted in a loss of $4 billion in market capitalization as well as fines for the mismanagement of user data.[36] Smaller companies may not be able to recover from such a loss, and because of this are reluctant to be transparent about data breaches. It is difficult to find granular information on smaller companies' data breaches, such as the ransom amount, date of breach, and overall effect of the breach on the companies.

More recently, Colonial Pipeline made headlines for a cyber-attack that affected them. In May of 2021, United States oil company Colonial Pipeline was shut down due to a ransomware attack that crippled the company's IT infrastructure. DarkSide, the hacking group responsible for the attack, exploited an exposed password for a VPN account which provided them access to the company's network. The hackers were able to steal 100 gigabytes of company data within two hours and infect the IT network with ransomware. Offices including accounting and billing were affected by the attack. Colonial Pipeline shut down all operations while they were locked out of their accounts, subsequently halting nearly all gas shipments to the East Coast of the United States. After days without gas and mounting pressure from the government for Colonial Pipeline to resume operations, the company ultimately paid DarkSide's ransom to get the decryption key.[37]

Lorenz Ransomware

In April 2022, Canadian telecom company Mitel released a statement documenting a critical vulnerability in several of their VoIP (Voice over Internet Protocol) devices. This was a critical vulnerability that left the MiVoice Connect service open to remote attacks through insufficient data validation, and when properly exploited could lead to threat actors using the device as a launch point into victims' networks (See Figure 1). With this statement came avenues for remediation: an update to all systems running the service that had been released prior to June 2022.

The first example of the Lorenz group exploiting this vulnerability occurred in September of that same year. Companies, who for a variety of possible reasons did not update to patch the vulnerability, were left exposed to the ransomware. Exploiting the Mitel VoIP device via malicious commands, the threat actors were able to break into a system and wait for up to a month before making any further progress. Security researchers found that Lorenz leveraged TCP/UDP tunneling tool Chisel to leapfrog from the Mitel phone system into the victim network (See Figure 1). The hackers would then compromise administrator accounts to escalate privileges and install programs to offload files and encrypt files in the target environment. Once the data has been encrypted and the files have been offloaded, Lorenz employs a double extortion strategy. Not only will it encrypt the victims' files, but it will threaten to leak sensitive data onto the hacking group's website on the dark web.[38] The ransom for Lorenz ranged from $500,000 to $700,000. Victims who did not pay the ransom are posted on the Lorenz site, with over 50 companies listed on the site. Data is available for anyone to download for about 25% of posted companies.

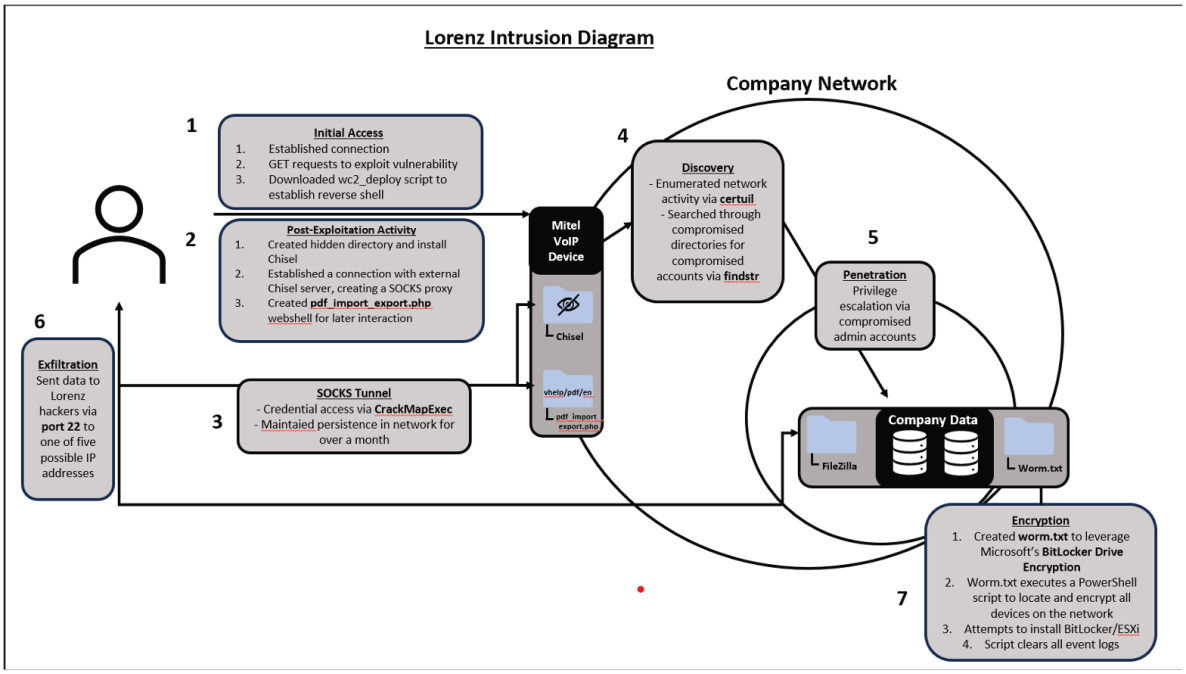


Figure 1: Lorenz Intrusion Diagram

The gravity of potential harm arising from the theft of these files is profound. Virtually all the stolen files harbor sensitive information, encompassing the vital operational, financial, and confidential data of the afflicted organizations or individuals. Stolen files include emails, financial records, and even architectural blueprints and schematics, illustrating the broad spectrum of

information at stake. Lorenz's practice of disclosing these files not only engenders the immediate loss of data's intrinsic value but also creates the risk of public exposure. Organizations falling prey to these attacks face multifaceted consequences, including significant downtime and the task of reconstruction, often at their expense, financially and reputationally. Such repercussions may translate into plummeting stock values, revenue erosion, and, in the worst case, bankruptcy. Frequently, ransomware groups set their demands in the tens of thousands to hundreds of thousands of dollars, which smaller to medium-sized enterprises may struggle to fulfill. Fortunately for Lorenz victims, a decryption key has been published so victims can recover their data. This is not the case for every ransomware attack, however, and victims of Lorenz still face the problem of all their data being published to the Lorenz Tor site.

Methods

Hacking groups live on the dark web. Their published activities are on sites that cannot be accessed by a traditional web browser. This research used the Tor browser to access databases on the dark web made by these hacking groups. To collect the data, the research utilized Kali Linux to interface with Tor and extract data from the databases. Through the project's data collection, the research was able to collect 70 examples of data breaches performed by the Lorenz Ransomware. To get industry information on breaches and ransomware at large, research involved several articles concerning the state of ransomware on businesses, including Verizon's data breach report, and on a more granular scale how specific ransomware operated, including CVE reports from Bleeping Computer and Arctic Wolf. Of the 70 companies posted to the blog, 18 had data available to be accessed and downloaded for analysis. The data retrieved from Lorenz's database was analyzed using JMP Pro to find the most common file types (See Figure 2)

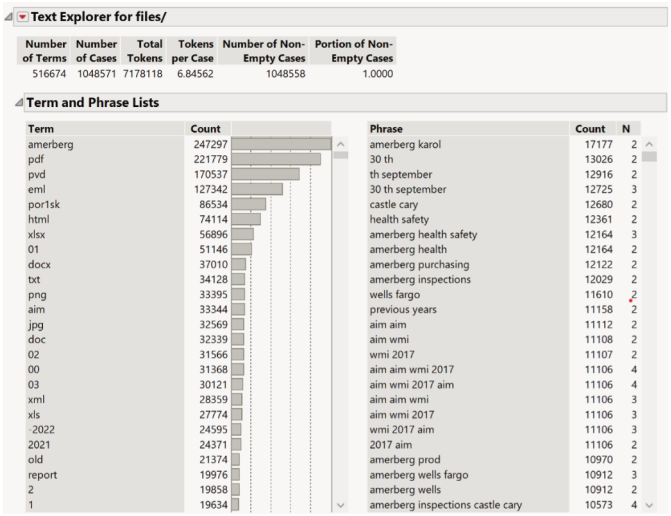


Figure 2: JMP Lorenz File Analysis

Research also worked to categorize the businesses that were posted on the Lorenz dark web blog. By analyzing the blog, we extracted company names, websites, and dates of breaches. Using this data, we created a database categorizing businesses by industry, size, and headquarters location using business analysis tools zoominfo.com and zippia.com. We categorized business sizes according to the Organization for Economic Cooperation and Development's (OECD) employee number categories for Micro (<10 employees), Small (10-100 employees), Medium (100-250 employees), and Large (>250 employees) businesses.[39]

Results

From what the database has provided, data breaches can be catastrophic to businesses. Of the data collected, the lowest number of documents stolen from an individual company was over 52,000, and at its peak over 4 million. Reported file sizes averaged in the hundreds of gigabytes. The most common files stolen were .PDF, followed closely by .PVD, .EML, and .HTML. The quality of data leaked ranged widely in topics, but many breaches included some form of financial information, from both the victim company itself and the customers of the victim. This data can give the public a look into the information that the company did not want out about themselves. Of the studied companies, 23% appeared to be in the manufacturing industry, and 11% were financial firms. Disclosed ransoms ranged in the tens of thousands of dollars, with some reaching over a million. The ransomware groups all had blogs to post data from the victim companies as well as a portal to communicate and pay for the ransom.

Our analysis examined the types of files most frequently targeted by Lorenz. The findings reveal a clear pattern in the types of files that Lorenz cybercriminals have stolen. The most stolen file type was PDF, with 221,779 instances documented within our dataset. Following closely behind, we observed 170,537 instances of .PVD files, 127,342 instances of .EML files, and 74,114 instances of .HTML files. Additionally, the ransomware frequently targeted .XLSX files (56,896 instances), .DOCX files (37,010 instances), .TXT files (34,128 instances), .PNG files (33,395 instances), .AIM files (33,344 instances), .JPG files (32,569 instances), and .DOC files (32,339 instances). These findings underscore the diverse range of file types that Lorenz threat actors have prioritized, potentially highlighting the ransomware's intent to maximize the disruption and monetary gain from their attacks.

Prior research articles reporting on the ransomware indicate that the malware was able to access and encrypt or delete data backups. The Lorenz ransomware did so through a known vulnerability through a telephony bug in the Mitel VoIP system. The attacker first sent a GET request to the vulnerable device, exploiting the vulnerability. Once the connection had been verified through the GET request, the attackers downloaded wc2_deploy, a tool that created an SSL-encrypted reverse shell from the device to the attacker's own device. With the reverse shell established, the attackers were able to install the TCP tunneling tool Chisel directly into the Mitel VoIP device. This tool enabled a direct connection from the attacker, past the Mitel device, and into the network. Notably, the attackers did not immediately attack once they gained access. They were observed to wait several weeks before continuing their mission. Once they returned, they attempted to gain higher credential access via CrackMapExec, then after enumerating domains and networks, searched through compromised directories for passwords. The attackers were able to successfully gain access to administrative accounts, allowing them to move laterally through the network to a domain controller. From there, the attackers exfiltrated the data via FileZilla and encrypted the victim's files via BitLocker. This resulted in the victim network's devices becoming encrypted and unusable.

Data breaches often resulted in the theft of sensitive personal and financial information. One attack by Lorenz exposed over 400,000 social security numbers, leaving victims vulnerable to identity theft and fraud. Another exposed blueprints for a middle school and a healthcare facility. These attacks not only affect the companies but have a ripple effect on the public at large (See Figures 3 and 4).

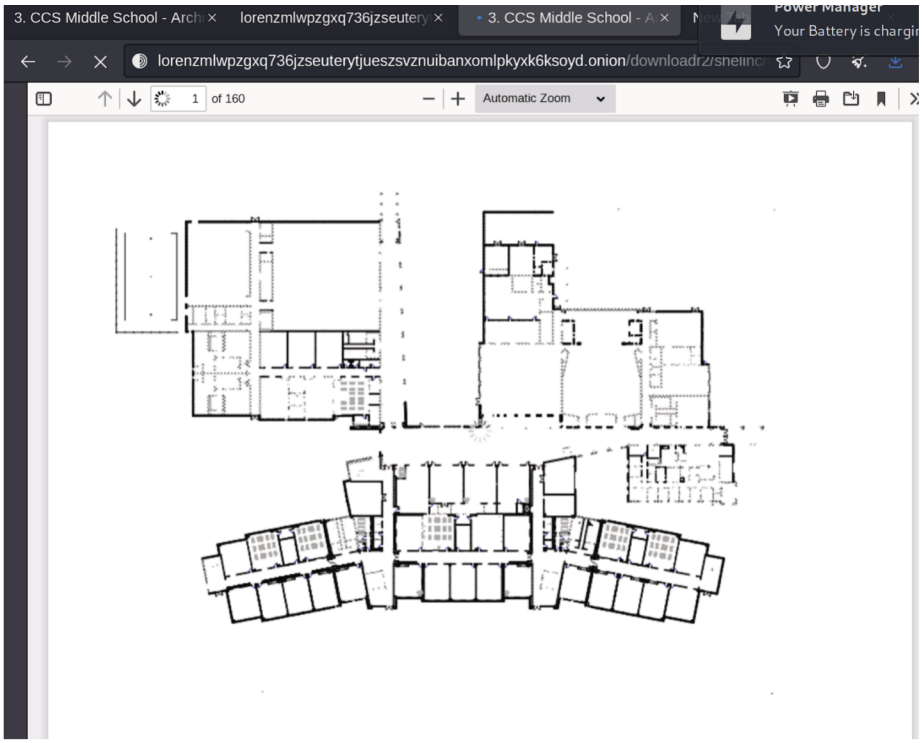


Figure 3: Lorenz Stolen File Example 1

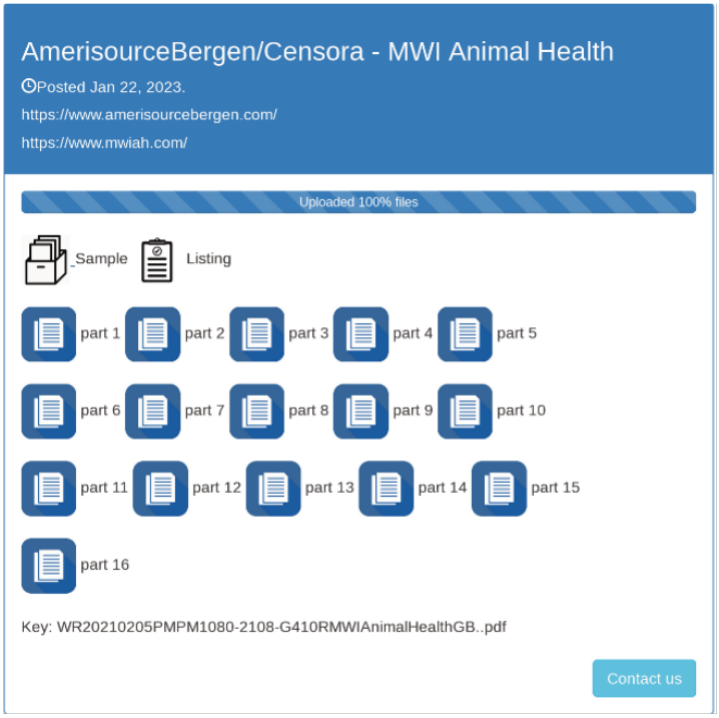


Figure 4: Lorenz Stolen File Example 2

Through our business analysis, we found multiple interesting takeaways. Of the companies posted, there are 0 micro (sized) companies, 12 small companies, 30 medium companies, and 27 large companies. The mean employee count of affected companies is 434 and the median employee count is 200. One company did not appear in any of our analysis and the link provided by the Lorenz blog was dead. Lorenz appeared to target companies indiscriminately across a variety of different industries. 18 companies posted on the site are in the manufacturing Industry, 8 were in the technology industry, and 7 are in the financial sector. All but 10 companies posted on the Lorenz blog are headquartered in the United States.

Discussion

The research project yields valuable insights into the serious impact of ransomware attacks on businesses. The collected data showcases the potential for hackers to steal vast quantities of sensitive information, which can affect the well-being of the business's customers. It emphasizes the significance of businesses taking proactive measures to safeguard their data, which includes regularly backing up data to secure offsite locations, adopting robust security protocols, and training employees on identifying and avoiding phishing scams and other commonplace methods used by hackers to gain unauthorized access to company networks.

Company-level analysis provides new insights. The most common industry was manufacturing, indicating their priorities do not lie with cybersecurity. As manufacturers become more connected and rely on digital devices for their processes, the likelihood of having a vulnerability in their networks increases. Oftentimes manufacturers rely on Internet of Things (IoT) devices, like the Mitel VoIP service. Due to their lightweight design, creators of these devices do not often include security features found in other more robust systems. Companies do not often think about thermostats or phones as points of vulnerability, but these weaknesses can cause serious damage. The manufacturing industry is estimated to have lost $240 billion in revenue and 42,220 jobs from 2002 to 2012 due to cyber-attacks.

Conclusion

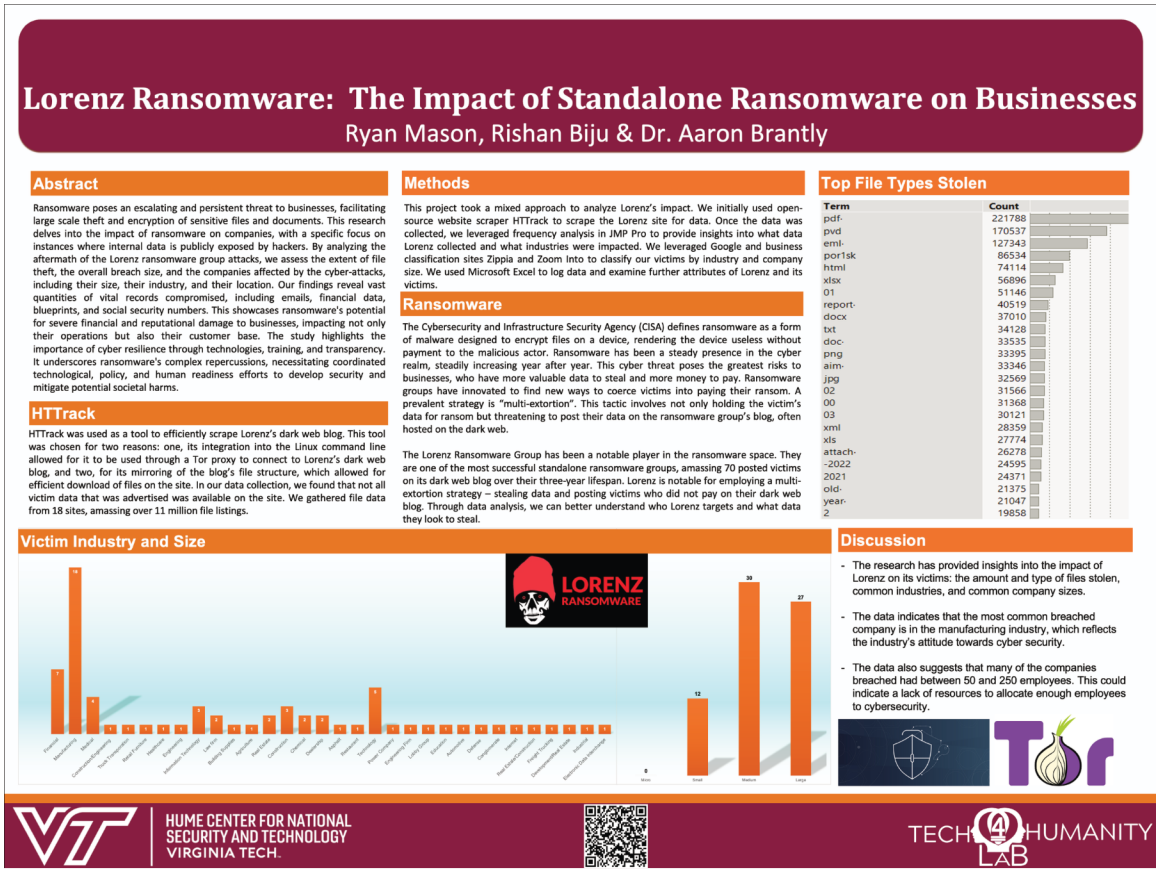
Ransomware poses a serious and growing threat to businesses of all sizes. As this paper has shown, attacks can result in massive theft of sensitive files and documents, with recent cases compromising hundreds of thousands or even millions of files. The research reveals the breadth of data at risk, including financial records, emails, architectural plans, social security numbers, and

more. Both the scale and sensitivity of stolen information can severely impact companies financially and reputationally.

Beyond the direct effects on businesses, attacks also endanger customers when personal information is leaked publicly. The research underscores how poor cybersecurity has ripple effects throughout society. With double extortion tactics, refusing to pay ransoms also risks sensitive data exposure. This highlights the difficult decisions companies face.

To mitigate harm from ransomware, businesses must take a proactive approach to security. Regular backups, robust protocols, and employee training are critical safeguards. Transparency about breaches, as mandated by law, is important but can be encouraged through policy changes that reduce liability based on hack method.

In conclusion, ransomware remains an evolving but potentially devastating threat to businesses and consumers given the sensitivity of data compromised. Developing resilience requires technological and human readiness along with policy solutions that promote transparency and cooperation against cybercrime. As this paper has shown, a complex array of factors underlies ransomware impacts, necessitating multifaceted solutions.



Bibliography

Abrams, Lawrence. "Meet Lorenz - A New Ransomware Gang Targeting the Enterprise," 2021. https://www.bleepingcomputer.com/news/security/meet-lorenz-a-new-ransomware-gang-targeting-the-enterprise/.

Ashford, Kate. "What Is Cryptocurrency?" Forbes Advisor, February 16, 2023. https://www.forbes.com/advisor/investing/cryptocurrency/what-is-cryptocurrency/.

Avertium. "An In-Depth Look at Lorenz Ransomware," 2022. https://www.avertium.com/resources/threat-reports/an-in-depth-look-at-lorenz-ransomware.

Belcic, Ivan. "What Is CryptoLocker Ransomware and How to Remove It." Avast, February 27, 2020. https://www.avast.com/c-cryptolocker#:~:text=CryptoLocker%20ransomware%20is%20a%20type, May%20of%20the%20following%20year.

Campbell, Mikey. "REvil Ransomware Group That Targeted Apple Supplier Gets Hacked, Taken Offline," October 22, 2021. https://appleinsider.com/articles/21/10/22/revil-ransomware-group-that-targeted-apple-supplier-gets-hacked-in-multinational-operation.

CrowdStrike. "5 Types of Ransomware." 5 Types of Ransomware, January 30, 2023. https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/.

"CrowdStrike2023GlobalThreatReport.Pdf," n.d.

GAO. "DATA PROTECTION Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach," August 2018.

Gatlan, Sergiu. "FBI: Hive Ransomware Extorted $100M from over 1,300 Victims." Bleeping Computer, November 17, 2022. https://www.bleepingcomputer.com/news/security/fbi-hive-ransomware-extorted-100m-from-over-1-300-victims/#google_vignette.

Greenberg, Andy. "The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet," May 12, 2020. https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/.

Ilascu, Ionut. "Lorenz Ransomware Gang Plants Backdoors to Use Months Later." Accessed March 18, 2023. https://www.bleepingcomputer.com/news/security/lorenz-ransomware-gang-plants-backdoors-to-use-months-later/.

Kaspersky. "Ransomware WannaCry: All You Need to Know." Accessed March 1, 2024. https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry.

Lim, Paul J. "Equifax's Massive Data Breach Has Cost the Company $4 Billion So Far," September 12, 2017. https://money.com/equifaxs-massive-data-breach-has-cost-the-company-4-billion-so-far/#:~:text=Equifax's%20Massive%20Data%20Breach%20Has%20Cost%20the%20Company%20%244%20Billion%20So%20Far,-By%3A%20Paul%20J&text=Has%20also%20written%3A, About%20History's%20Longest%20Bull%20Market.

"Live Ransomware Statistics," n.d.

Mujezinovic, Damir. "AIDS Trojan: The Story Behind the First Ever Ransomware Attack." Make Use of, November 28, 2021. https://www.makeuseof.com/aids-trojan-the-first-ransomware-attack-in-history/.

Neis, Markus, Ross Phillips, Steven Campbell, Teresa Whitmore, and Alex Ammons. "Chiseling In: Lorenz Ransomware Group Cracks MiVoice and Calls Back for Free," September 12, 2022. https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/.

OECD. "Enterprises by Business Size." Accessed February 28, 2024. https://data.oecd.org/entrepreneur/enterprises-by-business-size.htm#:~:text=SMEs%20are%20further%20subdivided%20into, employ%20250%20or%20more%20people.

Permana, Ghifari Ramadhika, Thomas Eric Trowbridge, and Bradley Sherborne. "Ransomware Mitigation: An Analytical Investigation into the Effects and Trends of Ransomware Attacks on Global Business," 2022. https://doi.org/10.31234/osf.io/ayc2d.

Robertson, Jordan, and William Turton. "Colonial Hackers Stole Data Thursday Ahead of Shutdown," May 8, 2021. https://web.archive.org/web/20210509150415/https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown.

Veeam. "2022 Ransomware Trends Report," 2022.

Waddell, Kaveh. "The Computer Virus That Haunted Early AIDS Researchers," May 10, 2016. https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/.

Wilding, Edward. "Trojan Horse: AIDS Disk." *Virus Bulletin*, January 1, 1990.

Wismer, David. "Hand-To-Hand Combat With The Insidious 'FBI MoneyPak Ransomware Virus,'" February 6, 2013. https://www.forbes.com/sites/davidwismer/2013/02/06/hand-to-hand-combat-with-the-insidious-fbi-moneypak-ransomware-virus/?sh=146c8157504a.

Wu, Dazhong, Anqi Ren, Wenhui Zhang, Feifei Fan, Peng Liu, Xinwen Fu, and Janis Terpenny. "Cybersecurity for Digital Manufacturing." *Journal of Manufacturing Systems* 48 (2018): 3–12. https://doi.org/10.1016/j.jmsy.2018.03.006.

Endnotes

[1] Damir Mujezinovic, "AIDS Trojan: The Story Behind the First Ever Ransomware Attack," Make Use of, November 28, 2021, https://www.makeuseof.com/aids-trojan-the-first-ransomware-attack-in-history/.

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Ibid.

[11] Kaveh Waddell, "The Computer Virus That Haunted Early AIDS Researchers," May 10, 2016, https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] Edward Wilding, "Trojan Horse: AIDS Disk," *Virus Bulletin*, January 1, 1990.

[19] Ibid.

[20] Kate Ashford, "What Is Cryptocurrency?," Forbes Advisor, February 16, 2023, https://www.forbes.com/advisor/investing/cryptocurrency/what-is-cryptocurrency/.

[21] Ivan Belcic, "What Is CryptoLocker Ransomware and How to Remove It," Avast, February 27, 2020, https://www.avast.com/c-cryptolocker#:~:text=CryptoLocker%20ransomware%20is%20a%20type,May%20of%20the%20following%20year.

[22] CrowdStrike, "5 Types of Ransomware," 5 Types of Ransomware, January 30, 2023, https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/.

[23] Ibid.

[24] David Wismer, "Hand-To-Hand Combat With The Insidious 'FBI MoneyPak Ransomware Virus,'" February 6, 2013, https://www.forbes.com/sites/davidwismer/2013/02/06/hand-to-hand-combat-with-the-insidious-fbi-moneypak-ransomware-virus/?sh=146c8157504a.

[25] Ibid.

[26] CrowdStrike

[27] Ibid.

[28] Mikey Campbell, "REvil Ransomware Group That Targeted Apple Supplier Gets Hacked, Taken Offline," October 22, 2021, https://appleinsider.com/articles/21/10/22/revil-ransomware-group-that-targeted-apple-supplier-gets-hacked-in-multinational-operation.

[29] "Ransomware WannaCry: All You Need to Know," Kaspersky, accessed March 1, 2024, https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry.

[30] Andy Greenberg, "The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet," May 12, 2020, https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/.

[31] "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." Office of Public Affairs | United States Department of Justice, September 6, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[32] Sergiu Gatlan, "FBI: Hive Ransomware Extorted $100M from over 1,300 Victims," Bleeping Computer, November 17, 2022, https://www.bleepingcomputer.com/news/security/fbi-hive-ransomware-extorted-100m-from-over-1-300-victims/#google_vignette.

[33] Veeam, "2022 Ransomware Trends Report."

[34] Title 16 CFR Part 318: § 318.1

[35] GAO, "DATA PROTECTION Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach," August 2018.

[36] Paul J. Lim, "Equifax's Massive Data Breach Has Cost the Company $4 Billion So Far," September 12, 2017, https://money.com/equifaxs-massive-data-breach-has-cost-the-company-4-billion-so-far/#:~:text=Equifax's%20Massive%20Data%20Breach%20Has%20Cost%20the%20Company%20%244%20Billion%20So%20Far,-By%3A%20Paul%20J&text=Has%20also%20written%3A,About%20History's%20Longest%20Bull%20Market.

[37] Jordan Robertson and William Turton, "Colonial Hackers Stole Data Thursday Ahead of Shutdown," May 8, 2021, https://web.archive.org/web/20210509150415/https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown.

[38] Neis et al., "Chiseling In: Lorenz Ransomware Group Cracks MiVoice and Calls Back for Free."

[39] "Enterprises by Business Size," OECD, accessed February 28, 2024, https://data.oecd.org/entrepreneur/enterprises-by-business-size.htm#:~:text=SMEs%20are%20further%20subdivided%20into,employ%20250%20or%20more%20people.