biggest ransomware attacks in history

Biggest Ransomware Attacks in History: Unraveling the Digital Heists That Shook the World

biggest ransomware attacks in history have not only disrupted global businesses but also reshaped the way organizations approach cybersecurity. These cyber incidents, involving malicious software that locks victims' data until a ransom is paid, have grown in sophistication and scale over the years. From crippling hospital systems to halting multinational corporations, ransomware attacks have evolved into a formidable threat in the digital age. Let's take a deep dive into the most notorious ransomware attacks that have made headlines, the lessons learned, and how organizations can better prepare themselves against such digital extortion.

Understanding Ransomware: A Quick Primer

Before diving into the biggest ransomware attacks in history, it's essential to grasp what ransomware is and how it operates. Ransomware is a type of malware that infects a computer or network, encrypts files or locks the system, and demands a ransom—usually in cryptocurrency—to restore access. Attackers often leverage phishing emails, software vulnerabilities, or compromised credentials to infiltrate systems.

The impact of ransomware extends beyond financial loss; it can cause operational paralysis, reputational damage, and legal consequences. The rise of ransomware-as-a-service (RaaS) has lowered the entry barrier for cybercriminals, leading to a surge in attacks worldwide.

Notorious Ransomware Attacks That Shaped Cybersecurity

WannaCry: The Global Wake-Up Call

In May 2017, the WannaCry ransomware attack swept across 150 countries, affecting hundreds of thousands of computers. Exploiting a vulnerability in Microsoft Windows (known as EternalBlue), WannaCry encrypted files on infected machines and demanded Bitcoin payments to release them.

What made WannaCry particularly alarming was its rapid spread, impacting critical infrastructure such as the UK's National Health Service (NHS), which faced appointment cancellations and disrupted emergency services. The attack exposed how outdated software and lack of timely patches can have catastrophic consequences.

NotPetya: More Than Just Ransomware

Shortly after WannaCry, in June 2017, the NotPetya attack emerged, masquerading as ransomware

but actually functioning as a destructive cyberweapon. Originating in Ukraine, it spread globally, hitting companies like Maersk, Merck, and FedEx hard.

Unlike traditional ransomware, NotPetya irreversibly encrypted data, making recovery impossible even if the ransom was paid. The attack resulted in hundreds of millions of dollars in damages, highlighting how ransomware can be used as a tool for geopolitical sabotage.

Ryuk: Targeted and Ruthless

Ryuk ransomware made headlines around 2018 and 2019 due to its focus on high-value targets including hospitals, government agencies, and large enterprises. Unlike the broad-brush approach of WannaCry, Ryuk attackers conduct detailed reconnaissance to maximize ransom payouts.

The attackers behind Ryuk often combine their ransomware with other malware strains like TrickBot to gain persistent access to networks. This multi-stage attack strategy underscores the increasing complexity of ransomware operations.

Colonial Pipeline Attack: Impact Beyond Cybersecurity

In May 2021, the Colonial Pipeline, a major US fuel pipeline operator, suffered a ransomware attack by the DarkSide group. The breach forced the company to shut down its pipeline temporarily, leading to fuel shortages and panic buying across several states.

This incident was a wake-up call illustrating how ransomware can disrupt critical infrastructure and have tangible effects on daily life. The attackers demanded a multimillion-dollar ransom, which Colonial Pipeline eventually paid, sparking debates about whether paying ransoms encourages more attacks.

Kaseya VSA Supply-Chain Attack

July 2021 saw a sophisticated supply-chain ransomware attack targeting the IT management software provider Kaseya. The REvil ransomware gang exploited vulnerabilities in Kaseya’s VSA software to distribute ransomware to thousands of downstream clients worldwide.

This attack demonstrated how ransomware can propagate through trusted software channels, amplifying its reach. It underscored the need for organizations to scrutinize the security of their supply chains and software dependencies.

Common Themes in the Biggest Ransomware Attacks

Analyzing these major ransomware incidents reveals patterns and tactics that cyber defenders must recognize:

- **Exploitation of Software Vulnerabilities:** Many attacks leveraged unpatched systems or zero-day vulnerabilities, emphasizing the importance of regular updates.
- **Phishing and Social Engineering:** Initial access often comes through deceptive emails or compromised credentials.
- **Multi-Stage Attacks:** Attackers frequently use multiple malware strains to establish footholds before deploying ransomware.
- **Targeting Critical Infrastructure:** Healthcare, energy, and supply chain sectors are increasingly targeted due to their essential services and willingness to pay ransoms.
- **Ransom Payments and Negotiations:** The debate around paying ransoms continues, balancing operational recovery against encouraging future attacks.

How Organizations Can Defend Against Ransomware

Given the rising tide of ransomware, prevention and preparedness have become vital. Here are some effective strategies to mitigate ransomware risks:

Regular Software Updates and Patch Management

Ensuring that all systems and applications are up to date with the latest security patches is crucial. Many ransomware attacks exploit known vulnerabilities that could be easily fixed.

Robust Backup and Recovery Plans

Maintaining offline, encrypted backups allows organizations to restore data without succumbing to ransom demands. Testing recovery procedures regularly ensures readiness when disaster strikes.

Employee Training and Awareness

Since phishing remains a common entry point, educating staff on recognizing suspicious emails and safe online practices can reduce infection chances.

Network Segmentation and Access Controls

Limiting access privileges and segmenting networks can contain the spread of ransomware within an organization.

Incident Response Planning

Having a clear, practiced ransomware incident response plan allows faster containment, communication, and recovery when an attack occurs.

The Growing Complexity of Ransomware Threats

The biggest ransomware attacks in history have pushed cybersecurity to evolve rapidly. Today's ransomware gangs often operate like businesses, with customer support lines and "ransomware negotiation" services. Some even threaten to leak sensitive data if victims refuse to pay, adding extortion layers beyond encryption.

Moreover, ransomware attacks are increasingly targeting Internet of Things (IoT) devices and leveraging artificial intelligence to evade detection. Governments and international coalitions are also stepping up efforts to combat ransomware through regulations and law enforcement cooperation.

Understanding these evolving trends is essential for businesses and individuals alike to stay ahead of cybercriminals.

The landscape of ransomware is a stark reminder of the vulnerabilities in our interconnected digital world. By learning from the biggest ransomware attacks in history and adopting proactive security measures, organizations can better protect their data, maintain trust, and contribute to a safer cyberspace for everyone.

Frequently Asked Questions

What was the biggest ransomware attack in history?

The WannaCry ransomware attack in May 2017 is considered one of the biggest ransomware attacks in history, affecting over 200,000 computers across 150 countries.

How did the WannaCry ransomware attack spread so rapidly?

WannaCry exploited a Windows vulnerability called EternalBlue, which allowed it to spread rapidly through networks without user interaction.

Which sectors were most affected by the biggest ransomware attacks?

Healthcare, government, finance, and critical infrastructure sectors have been among the most affected by major ransomware attacks.

What was the impact of the NotPetya ransomware attack in 2017?

NotPetya caused widespread disruption, particularly in Ukraine, and resulted in billions of dollars in damages globally, affecting companies like Maersk and Merck.

How do ransomware attackers demand payment from victims?

Attackers typically demand payment through cryptocurrencies like Bitcoin to maintain anonymity and make tracing the transactions difficult.

What measures can organizations take to protect themselves from ransomware attacks?

Organizations should regularly update software, maintain backups, implement strong cybersecurity protocols, and educate employees about phishing attacks.

Has ransomware evolved over time since the biggest attacks?

Yes, ransomware has become more sophisticated with tactics like double extortion, where attackers also threaten to leak stolen data if the ransom isn’t paid.

What was the significance of the Colonial Pipeline ransomware attack in 2021?

The Colonial Pipeline attack caused fuel shortages across the US East Coast, highlighting the vulnerability of critical infrastructure to ransomware.

Are ransomware attacks increasing in frequency and severity?

Yes, ransomware attacks have been increasing in both frequency and sophistication, posing a growing threat to governments and businesses worldwide.

Can paying the ransom guarantee data recovery after a ransomware attack?

Paying the ransom does not guarantee data recovery and may encourage further attacks; experts generally advise against paying and recommend restoring from backups.

Additional Resources

Biggest Ransomware Attacks in History: An Analytical Review of Cyber Extortion Epidemics

biggest ransomware attacks in history have reshaped the cybersecurity landscape, exposing vulnerabilities in both public and private sectors worldwide. These high-profile cyber incidents have not only resulted in massive financial losses but also disrupted critical infrastructures, underscoring

the urgent necessity for robust cyber defense mechanisms. From government agencies to multinational corporations, ransomware has evolved into a sophisticated tool for cybercriminals, wielding unparalleled influence over digital security paradigms.

Understanding the Scale and Impact of Ransomware

Ransomware is a type of malicious software designed to encrypt a victim’s data, rendering systems unusable until a ransom is paid, usually in cryptocurrencies like Bitcoin. The biggest ransomware attacks in history illustrate diverse attack vectors and targets, yet share common traits: exploitation of security lapses, use of social engineering, and demand for hefty ransoms. The financial damages extend beyond ransom payments to include downtime, reputational damage, regulatory fines, and remediation costs, often reaching into billions of dollars globally.

Notorious Ransomware Attacks That Shaped Cybersecurity

Several ransomware campaigns stand out for their unprecedented scale and impact. Below is a detailed examination of some of the most significant incidents:

- **WannaCry (2017):** Perhaps the most infamous ransomware outbreak, WannaCry infected over 230,000 computers across 150 countries within days. Leveraging a leaked NSA exploit called EternalBlue, WannaCry targeted machines running Microsoft Windows. The attack crippled parts of the UK's National Health Service (NHS), causing widespread disruption in healthcare services. Estimated losses reached hundreds of millions of dollars, and the attack highlighted the dangers of unpatched vulnerabilities.

- **NotPetya (2017):** Initially perceived as ransomware, NotPetya was later identified as a destructive wiper masquerading as ransomware. Originating in Ukraine, it spread globally, affecting multinational firms like Maersk and FedEx. Financial damages were staggering, with Maersk alone reporting losses up to $300 million. The attack demonstrated how ransomware could be weaponized for geopolitical objectives.

- **Ryuk (2018 - Present):** Ryuk is a sophisticated ransomware strain primarily targeting large enterprises and government entities. Unlike indiscriminate worms like WannaCry, Ryuk operators conduct extensive reconnaissance to maximize ransom payments, often demanding millions of dollars. Its persistent activity over multiple years underscores the evolving threat posed by ransomware-as-a-service (RaaS) models.

- **Colonial Pipeline (2021):** This cyberattack disrupted fuel supply across the eastern United States when the Colonial Pipeline system was hit by the DarkSide ransomware group. The attack forced a shutdown of critical infrastructure, sparking fuel shortages and price spikes. The incident underscored vulnerabilities in critical infrastructure cybersecurity and prompted regulatory scrutiny and policy debates regarding ransomware resilience.

- **Kaseya VSA Supply-Chain Attack (2021):** One of the most sophisticated supply-chain ransomware attacks, the Kaseya breach infiltrated managed service providers (MSPs) to deploy ransomware to thousands of downstream customers. The REvil ransomware gang demanded a $70 million ransom, spotlighting supply chain risks and the cascading effects ransomware can have on interconnected digital ecosystems.

Key Factors Contributing to the Success of Major Ransomware Attacks

Analyzing the biggest ransomware attacks in history reveals several common enablers of their devastating success. Understanding these factors is critical for improving defenses.

Exploitation of Unpatched Vulnerabilities

Many large-scale ransomware incidents leverage publicly known vulnerabilities that remain unpatched at the victim's end. For example, WannaCry exploited a Windows SMB protocol vulnerability patched by Microsoft months prior to the attack. Organizations failing to maintain timely updates create fertile ground for ransomware propagation.

Phishing and Social Engineering

Human error remains a significant vulnerability. Attackers frequently use phishing emails containing malicious links or attachments to gain initial footholds. These tactics enable lateral movement within compromised networks, allowing ransomware to spread widely before detection.

Ransomware-as-a-Service (RaaS) Models

The commercialization of ransomware has lowered the barrier to entry for cybercriminals. RaaS platforms provide ready-made ransomware kits and infrastructure for affiliates in exchange for revenue sharing. This business model has accelerated the proliferation and sophistication of ransomware campaigns.

Targeting of Critical Infrastructure and High-Value Targets

Attackers increasingly focus on entities where disruption can cause maximum impact and pressure victims to pay quickly. Hospitals, energy providers, and supply chains represent critical sectors vulnerable to ransomware due to their operational importance and often insufficient cybersecurity postures.

Comparative Analysis of Financial and Operational Impact

The financial consequences of the biggest ransomware attacks in history vary, but their operational disruptions tend to share common patterns. For instance:

1. **WannaCry:** Estimated financial damages approximated $4 billion globally, with NHS experiencing severe service interruptions resulting in canceled procedures and delayed treatments.

2. **NotPetya:** Caused an estimated $10 billion in damages worldwide, with companies like Maersk and Merck reporting significant operational halts and data loss.

3. **Colonial Pipeline:** Though the ransom paid was reportedly $4.4 million, the broader economic impact due to fuel shortages and public anxiety was considerably higher, highlighting indirect costs.

Such comparisons highlight that the cost of ransomware goes well beyond ransom payments, encompassing recovery efforts, legal liabilities, and long-term reputational harm.

The Role of Cryptocurrency in Ransomware Proliferation

Cryptocurrencies have facilitated the rise of ransomware by providing a semi-anonymous payment mechanism. Bitcoin, in particular, remains the payment method of choice, enabling attackers to receive ransoms while complicating law enforcement tracing efforts. However, increasing regulatory scrutiny and blockchain analytics have begun to disrupt this dynamic.

Emerging Trends and Defensive Strategies

As ransomware continues to evolve, so too must cybersecurity strategies to mitigate risk.

Zero Trust Architectures and Network Segmentation

Implementing zero-trust principles—where no user or device is inherently trusted—helps limit attackers’ lateral movement post-infection. Network segmentation confines ransomware outbreaks to isolated environments, reducing overall impact.

Backup and Disaster Recovery Planning

Reliable, offline backups remain one of the most effective defenses against ransomware. Organizations with tested recovery plans can restore systems without capitulating to ransom demands, thereby reducing attackers' leverage.

Threat Intelligence Sharing and Collaboration

Information sharing among private sector entities and government agencies enhances situational awareness and response capabilities. Early warning of emerging ransomware strains enables proactive defense measures.

Legal and Regulatory Developments

Governments worldwide are strengthening cybersecurity regulations, mandating incident reporting, and imposing penalties for inadequate safeguards. Additionally, some jurisdictions discourage ransom payments to deter financially incentivized attacks.

The biggest ransomware attacks in history serve as stark reminders of the perils inherent in an increasingly digitized world. Their scale and sophistication reveal both the ingenuity of cybercriminals and the pressing need for comprehensive, adaptive cybersecurity frameworks. As organizations grapple with emerging threats, lessons learned from these landmark incidents provide invaluable guidance for building more resilient digital infrastructures.

Biggest Ransomware Attacks In History

biggest ransomware attacks in history: *The 20 Biggest Hacks in History* Dimitrios Detsikas, 2025-02-10 We live in an era where information is more valuable than gold, and cybercriminals have become the modern-day bank robbers, manipulating systems to steal, disrupt, and influence the world at an unprecedented scale. From governments to startups, no one is immune. As technology evolves, so do cyber threats. This book is not just about the biggest hacks in history—it's about what we can learn from them. Every breach, every security failure, and every lost fortune carries an important lesson. Whether you're an entrepreneur, an IT professional, or simply a digital citizen, this book will arm you with knowledge to recognize the dangers that lurk in the cyber world and how to protect yourself. Cybersecurity is no longer just an IT issue—it's a survival issue. What's Inside? The multi-billion-dollar SWIFT banking fraud that stunned the financial world. The Mt. Gox collapse, the biggest crypto hack that cost investors millions. The Yahoo data breach, which exposed 3 billion accounts. How North Korean hackers infiltrated global banks. The Equifax hack, and how poor security practices put millions at risk. The Colonial Pipeline ransomware attack, which led to fuel shortages across the U.S. The biggest NFT and DeFi heists, stealing millions in seconds. …and 13 more shocking cyber attacks. Packed with 67 pages of compelling stories and expert insights, this book is a must-read for business leaders, cybersecurity professionals, crypto investors, and anyone concerned about digital vulnerabilities. Learning from the past equips us to safeguard the future.

biggest ransomware attacks in history: *Cyberterrorism and Ransomware Attacks* Gary

Wiener, 2018-07-15 In this digital age, it is not only conventional weapons that are used to threaten and harm others. A new and terrifying avenue is cyberspace and ransomware. This malware encrypts a user's data and demands payment in exchange for unlocking the data. Such attacks are becoming more widespread: a 2017 cyber incident attacked more than 45,000 users in countries around the world. This anthology presents a collection of global perspectives on the topic that examines the potential of such attacks and how we can secure ourselves in the future.

biggest ransomware attacks in history: Cybernetics and Control Theory in Systems Radek Silhavy, Petr Silhavy, 2024-10-16 Addressing key issues in modern cybernetics and informatics, this book presents vital research within networks and systems. It offers an extensive overview of the latest methods, algorithms, and design innovations. This book compiles the meticulously reviewed proceedings of the Networks and Systems in Cybernetics session of the 13th Computer Science Online Conference 2024 (CSOC 2024), held virtually in April 2024.

biggest ransomware attacks in history: Summary of Gregory C. Rasner's Cybersecurity and Third-Party Risk Everest Media,, 2022-06-11T22:59:00Z Please note: This is a companion version & not the original book. Sample Book Insights: #1 On December 10, 2020, ESET researchers announced they had found that a chat software called Able Desktop, part of a widely used business management suite in Mongolia, was exploited to deliver the HyperBro backdoor, the Korplug RAT, and another RAT named Tmanger. #2 On December 13, 2020, FireEye, a global leader in cybersecurity, published the first details about the SolarWinds Supply-Chain Attack, a global intrusion campaign that inserted a trojan into the SolarWinds Orion business software updates to distribute the malware. #3 The most recent attack reflects a particular focus on the United States and many other democracies, but it also provides a powerful reminder that people in virtually every country are at risk and need protection. #4 On December 17, 2020, ESET Research announced that it had detected a large supply-chain attack against the digital signing authority of the government of Vietnam, the website for the Vietnam Government Certification Authority. The website was hacked as early as July 23rd, and no later than August 16, 2020. The compromised toolkits contained malware known as PhantomNet.

biggest ransomware attacks in history: Cybersecurity – Attack and Defense Strategies Yuri Diogenes, Dr. Erdal Ozkaya, 2022-09-30 Updated edition of the bestselling guide for planning attack and defense strategies based on the current threat landscape Key FeaturesUpdated for ransomware prevention, security posture management in multi-cloud, Microsoft Defender for Cloud, MITRE ATT&CK Framework, and moreExplore the latest tools for ethical hacking, pentesting, and Red/Blue teamingIncludes recent real-world examples to illustrate the best practices to improve security postureBook Description Cybersecurity – Attack and Defense Strategies, Third Edition will bring you up to speed with the key aspects of threat assessment and security hygiene, the current threat landscape and its challenges, and how to maintain a strong security posture. In this carefully revised new edition, you will learn about the Zero Trust approach and the initial Incident Response process. You will gradually become familiar with Red Team tactics, where you will learn basic syntax for commonly used tools to perform the necessary operations. You will also learn how to apply newer Red Team techniques with powerful tools. Simultaneously, Blue Team tactics are introduced to help you defend your system from complex cyber-attacks. This book provides a clear, in-depth understanding of attack/defense methods as well as patterns to recognize irregular behavior within your organization. Finally, you will learn how to analyze your network and address malware, while becoming familiar with mitigation and threat detection techniques. By the end of this cybersecurity book, you will have discovered the latest tools to enhance the security of your system, learned about the security controls you need, and understood how to carry out each step of the incident response process. What you will learnLearn to mitigate, recover from, and prevent future cybersecurity eventsUnderstand security hygiene and value of prioritizing protection of your workloadsExplore physical and virtual network segmentation, cloud network visibility, and Zero Trust considerationsAdopt new methods to gather cyber intelligence, identify risk, and demonstrate impact with Red/Blue Team strategiesExplore legendary tools such as Nmap and Metasploit to

supercharge your Red TeamDiscover identity security and how to perform policy enforcementIntegrate threat detection systems into your SIEM solutionsDiscover the MITRE ATT&CK Framework and open-source tools to gather intelligenceWho this book is for If you are an IT security professional who wants to venture deeper into cybersecurity domains, this book is for you. Cloud security administrators, IT pentesters, security consultants, and ethical hackers will also find this book useful. Basic understanding of operating systems, computer networking, and web applications will be helpful.

biggest ransomware attacks in history: *Impact of Digital Transformation on the Development of New Business Models and Consumer Experience* Rodrigues, Maria Antónia, Proença, João F., 2022-03-11 In a highly competitive market, digital transformation with internet of things, artificial intelligence, and other innovative technological trends are elements of differentiations and are important milestones in business development and consumer interaction, particularly in services. As a result, there are several new business models anchored in these digital and technological environments and new experiences provided to services consumers and firms that need to be examined. Impact of Digital Transformation on the Development of New Business Models and Consumer Experience provides relevant theoretical and empirical research findings and innovative and multifaceted perspectives on how digital transformation and other innovative technologies can drive new business models and create valued experiences for consumers and firms. Covering topics such as business models, consumer behavior, and gamification, this publication is ideal for industry professionals, managers, business owners, practitioners, researchers, professors, academicians, and students.

biggest ransomware attacks in history: *Cybersecurity and Third-Party Risk* Gregory C. Rasner, 2021-06-11 Move beyond the checklist and fully protect yourself from third-party cybersecurity risk Over the last decade, there have been hundreds of big-name organizations in every sector that have experienced a public breach due to a vendor. While the media tends to focus on high-profile breaches like those that hit Target in 2013 and Equifax in 2017, 2020 has ushered in a huge wave of cybersecurity attacks, a near 800% increase in cyberattack activity as millions of workers shifted to working remotely in the wake of a global pandemic. The 2020 SolarWinds supply-chain attack illustrates that lasting impact of this dramatic increase in cyberattacks. Using a technique known as Advanced Persistent Threat (APT), a sophisticated hacker leveraged APT to steal information from multiple organizations from Microsoft to the Department of Homeland Security not by attacking targets directly, but by attacking a trusted partner or vendor. In addition to exposing third-party risk vulnerabilities for other hackers to exploit, the damage from this one attack alone will continue for years, and there are no signs that cyber breaches are slowing. Cybersecurity and Third-Party Risk delivers proven, active, and predictive risk reduction strategies and tactics designed to keep you and your organization safe. Cybersecurity and IT expert and author Gregory Rasner shows you how to transform third-party risk from an exercise in checklist completion to a proactive and effective process of risk mitigation. Understand the basics of third-party risk management Conduct due diligence on third parties connected to your network Keep your data and sensitive information current and reliable Incorporate third-party data requirements for offshoring, fourth-party hosting, and data security arrangements into your vendor contracts Learn valuable lessons from devasting breaches suffered by other companies like Home Depot, GM, and Equifax The time to talk cybersecurity with your data partners is now. Cybersecurity and Third-Party Risk is a must-read resource for business leaders and security professionals looking for a practical roadmap to avoiding the massive reputational and financial losses that come with third-party security breaches.

biggest ransomware attacks in history: Crime Without Borders Aaron Fichtelberg, Nicole Fox, Kai Lin, 2025-10-31 This book introduces students to the challenges related to international crime and punishment and the ways that criminal justice systems have sought to confront them. The dismantling and opening up of borders by technology, transportation, international trade, and the global flow of labor and capital have allowed those engaging in criminal behavior to work across

borders in ways that challenge the traditional nation-state and its criminal justice system, making the study of international crime and justice increasingly relevant. This book not only covers the nuts and bolts of international crime and law enforcement but also raises abstract, theoretical issues for debate and asks critical questions about the ideal ways to think about international criminal justice problems. Contemporary topics such as war crimes, genocide, crimes against humanity, terrorism, drug smuggling, human trafficking, financial crimes, environmental crimes, and cybercrime are addressed, and connections between globalization, politics, and criminal justice reflect the modern realities of international and transnational crime. Following an introductory chapter that presents the dimensions of international criminal justice, the text is organized into two major parts, the first part discussing major international crimes and why people engage in them, and the second part laying out the central structures of the international criminal justice system, including international courts, transnational law enforcement, and aspects of United States criminal justice developed to deal with international crimes. Throughout the book, the authors place global crime within the context of contemporary politics and current events. Pedagogical tools such as summaries of significant international cases, discussion questions, and a thorough bibliography aid reader engagement and understanding. This text is suitable for students in global criminology, international crime, and comparative criminology courses, and researchers and policy-makers concerned with international and transnational crime.

biggest ransomware attacks in history: *BIG BROTHER TECHNOLOGY* Axel Balthazar, 2017-12-09 The government can hack into any computer or smartphone on the planet. What sounded like a crazy conspiracy theory was exposed as truth with the 2013 NSA leaks from Edward Snowden. Since then, the deluge of CIA and NSA hacking programs filling the sky like rain hasn't stopped. This is an exposé of the software programs and techniques used by the agencies to spy on the planet. Big Brother is watching. It's time to watch back. Dozens of previously classified government surveillance programs are divulged in this alarming book! Contents include these fascinating topics: Edward Snowden; NSA; Mass Surveillance; Five Eyes; FinCEN (Financial Crimes Enforcement Network); Stuxnet; PRISM; MYSTIC; DCSNet (Digital Collection System Network); XKeyscore; DISHFIRE; STONEGHOST; Magic Lantern; ECHELON; Fairview; WikiLeaks; Vault 7; Julian Assange; Room 641A; The Doughnut; Fort Meade; Menwith Hill; Utah Data Center; ICREACH; Ransomware, Tor; "wannacry"; ShadowBrokers; and tons more. Axel Balthazar is at it again!

biggest ransomware attacks in history: Cybertax George K. Tsantes, James Ransome, 2023-04-20 Cybersecurity risk is a top-of-the-house issue for all organizations. Cybertax—Managing the Risks and Results is a must read for every current or aspiring executive seeking the best way to manage and mitigate cybersecurity risk. It examines cybersecurity as a tax on the organization and charts the best ways leadership can be cybertax efficient. Viewing cybersecurity through the cybertax lens provides an effective way for non–cybersecurity experts in leadership to manage and govern cybersecurity in their organizations The book outlines questions and leadership techniques to gain the relevant information to manage cybersecurity threats and risk. The book enables executives to: Understand cybersecurity risk from a business perspective Understand cybersecurity risk as a tax (cybertax) Understand the cybersecurity threat landscape Drive business-driven questions and metrics for managing cybersecurity risk Understand the Seven C's for managing cybersecurity risk Governing the cybersecurity function is as important as governing finance, sales, human resources, and other key leadership responsibilities Executive leadership needs to manage cybersecurity risk like they manage other critical risks, such as sales, finances, resources, and competition. This book puts managing cybersecurity risk on an even plane with these other significant risks that demand leaderships' attention. The authors strive to demystify cybersecurity to bridge the chasm from the top-of-the-house to the cybersecurity function. This book delivers actionable advice and metrics to measure and evaluate cybersecurity effectiveness across your organization.

biggest ransomware attacks in history: Computer, Communication, and Signal Processing Erich J. Neuhold, Xavier Fernando, Joan Lu, Selwyn Piramuthu, Aravindan Chandrabose, 2022-07-21 This book constitutes the refereed proceedings of the 6th International

Conference on Computer, Communication, and Signal Processing, ICCSP 2022, held in Chennai, India, in February 2022.* The 21 full and 2 short papers presented in this volume were carefully reviewed and selected from 111 submissions. The papers are categorized into topical sub-headings: artificial intelligence and machine learning; Cyber security; and internet of things. *The conference was held as a virtual event due to the COVID-19 pandemic.

biggest ransomware attacks in history: *Intelligent Technologies for Healthcare Business Applications* Athina Bourdena, Constandinos Mavromoustakis, Evangelos K. Markakis, George Mastorakis, Evangelos Pallis, 2024-08-12 This book covers a wide range of applications and scenarios of intelligent technologies for healthcare business applications. The authors adopt an interdisciplinary approach with both theoretical and practical approaches in order to be relevant to multiple audiences. This book encapsulates fundamental and cutting-edge research paradigms of intelligent healthcare environments and addresses related open-ended research issues. The authors also explore recent advances, disseminate state-of-the-art techniques, and deploy novel technologies in intelligent healthcare services and applications. The book features a broad appeal to electrical, electronic, computer, software and telecommunications engineers in the healthcare space. Covers a range of applications and scenarios of intelligent technologies for healthcare business applications Explores advances, disseminates techniques, and deploys novel technologies in intelligent healthcare services Features paradigms of intelligent healthcare environments and addresses open-ended research issues

biggest ransomware attacks in history: *Handbook of Research on Innovations in Technology and Marketing for the Connected Consumer* Dadwal, Sumesh Singh, 2019-11-15 Connected customers, using a wide range of devices such as smart phones, tablets, and laptops have ushered in a new era of consumerism. Now more than ever, this change has prodded marketing departments to work with their various IT departments and technologists to expand consumers' access to content. In order to remain competitive, marketers must integrate marketing campaigns across these different devices and become proficient in using technology. The Handbook of Research on Innovations in Technology and Marketing for the Connected Consumer is a pivotal reference source that develops new insights into applications of technology in marketing and explores effective ways to reach consumers through a wide range of devices. While highlighting topics such as cognitive computing, artificial intelligence, and virtual reality, this publication explores practices of technology-empowered digital marketing as well as the methods of applying practices to less developed countries. This book is ideally designed for marketers, managers, advertisers, branding teams, application developers, IT specialists, academicians, researchers, and students.

biggest ransomware attacks in history: *Critical Concepts, Standards, and Techniques in Cyber Forensics* Husain, Mohammad Shahid, Khan, Mohammad Zunnun, 2019-11-22 Advancing technologies, especially computer technologies, have necessitated the creation of a comprehensive investigation and collection methodology for digital and online evidence. The goal of cyber forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device or on a network and who was responsible for it. Critical Concepts, Standards, and Techniques in Cyber Forensics is a critical research book that focuses on providing in-depth knowledge about online forensic practices and methods. Highlighting a range of topics such as data mining, digital evidence, and fraud investigation, this book is ideal for security analysts, IT specialists, software engineers, researchers, security professionals, criminal science professionals, policymakers, academicians, and students.

biggest ransomware attacks in history: *Game Theory and Machine Learning for Cyber Security* Charles A. Kamhoua, Christopher D. Kiekintveld, Fei Fang, Quanyan Zhu, 2021-09-15 GAME THEORY AND MACHINE LEARNING FOR CYBER SECURITY Move beyond the foundations of machine learning and game theory in cyber security to the latest research in this cutting-edge field In Game Theory and Machine Learning for Cyber Security, a team of expert security researchers delivers a collection of central research contributions from both machine learning and game theory applicable to cybersecurity. The distinguished editors have included resources that

address open research questions in game theory and machine learning applied to cyber security systems and examine the strengths and limitations of current game theoretic models for cyber security. Readers will explore the vulnerabilities of traditional machine learning algorithms and how they can be mitigated in an adversarial machine learning approach. The book offers a comprehensive suite of solutions to a broad range of technical issues in applying game theory and machine learning to solve cyber security challenges. Beginning with an introduction to foundational concepts in game theory, machine learning, cyber security, and cyber deception, the editors provide readers with resources that discuss the latest in hypergames, behavioral game theory, adversarial machine learning, generative adversarial networks, and multi-agent reinforcement learning. Readers will also enjoy: A thorough introduction to game theory for cyber deception, including scalable algorithms for identifying stealthy attackers in a game theoretic framework, honeypot allocation over attack graphs, and behavioral games for cyber deception An exploration of game theory for cyber security, including actionable game-theoretic adversarial intervention detection against advanced persistent threats Practical discussions of adversarial machine learning for cyber security, including adversarial machine learning in 5G security and machine learning-driven fault injection in cyber-physical systems In-depth examinations of generative models for cyber security Perfect for researchers, students, and experts in the fields of computer science and engineering, Game Theory and Machine Learning for Cyber Security is also an indispensable resource for industry professionals, military personnel, researchers, faculty, and students with an interest in cyber security.

biggest ransomware attacks in history: Information Security Theory and Practice Samia Bouzefrane, Damien Sauveron, 2024-06-17 This volume constitutes the refereed proceedings of the 14th IFIP WG 11.2 International Conference on Information Security Theory and Practices, WISTP 2024, held in Paris, France. The 12 full papers presented were carefully reviewed and selected from 30 submissions. The papers presented in this proceedings focus on emerging trends in security and privacy, including experimental studies of fielded systems while exploring the application of security technology, and highlighting successful system implementations.

biggest ransomware attacks in history: Records and Information Management, Second Edition Patricia C. Franks, 2018-10-10 As Information Management put it, On the strength of its currency and coverage alone, Franks' book is poised to take over as the recommended go-to reference for both students and RIM professionals for many years to come.” The new second edition cements this work’s status as an up-to-date classic, its content updated and expanded to address emerging technologies, most notably blockchain, and evolving standards and practices. Inside, Franks presents complete coverage of the records and information lifecycle model, encompassing paper, electronic (databases, office suites, email), and new media records (blogs, chat messages, and software as a service). Informed by an advisory board of experts in the field and with contributions by noted authorities, the text addresses such key topics as the origins and development of records and information;the discipline of information governance and developing a strategic records management plan;creation/capture and classification;retention strategies, inactive records management, archives, and long-term preservation;access, storage, and retrieval;electronic records and electronic records management systems;the latest on rapidly evolving technologies such as web records, social media, and mobile devices;vital records, disaster preparedness and recovery, and business continuity;monitoring, auditing, and risk management; andeducation and training. This book’s authoritative blend of theory and practice makes it a matchless resource for everyone in the archives and records management field. Instructor/trainer extras include a set of ready-to-go, customizable PowerPoint slides to accompany the text. Examination copies are available for instructors who are interested in adopting this title for course use.

biggest ransomware attacks in history: *Handbook on Crime and Technology* Don Hummer, James M. Byrne, 2023-03-02 Examining the consequences of technology-driven lifestyles for both crime commission and victimization, this comprehensive Handbook provides an overview of a broad array of techno-crimes as well as exploring critical issues concerning the criminal justice system’s

response to technology-facilitated criminal activity.

biggest ransomware attacks in history: Machine Learning Techniques for Cybersecurity Elisa Bertino, Sonam Bhardwaj, Fabrizio Cicala, Sishuai Gong, Imtiaz Karim, Charalampos Katsis, Hyunwoo Lee, Adrian Shuai Li, Ashraf Y. Mahgoub, 2023-04-08 This book explores machine learning (ML) defenses against the many cyberattacks that make our workplaces, schools, private residences, and critical infrastructures vulnerable as a consequence of the dramatic increase in botnets, data ransom, system and network denials of service, sabotage, and data theft attacks. The use of ML techniques for security tasks has been steadily increasing in research and also in practice over the last 10 years. Covering efforts to devise more effective defenses, the book explores security solutions that leverage machine learning (ML) techniques that have recently grown in feasibility thanks to significant advances in ML combined with big data collection and analysis capabilities. Since the use of ML entails understanding which techniques can be best used for specific tasks to ensure comprehensive security, the book provides an overview of the current state of the art of ML techniques for security and a detailed taxonomy of security tasks and corresponding ML techniques that can be used for each task. It also covers challenges for the use of ML for security tasks and outlines research directions. While many recent papers have proposed approaches for specific tasks, such as software security analysis and anomaly detection, these approaches differ in many aspects, such as with respect to the types of features in the model and the dataset used for training the models. In a way that no other available work does, this book provides readers with a comprehensive view of the complex area of ML for security, explains its challenges, and highlights areas for future research. This book is relevant to graduate students in computer science and engineering as well as information systems studies, and will also be useful to researchers and practitioners who work in the area of ML techniques for security tasks.

biggest ransomware attacks in history: Real-Time and Retrospective Analyses of Cyber Security Bird, David Anthony, 2020-09-04 Society is continually transforming into a digitally powered reality due to the increased dependence of computing technologies. The landscape of cyber threats is constantly evolving because of this, as hackers are finding improved methods of accessing essential data. Analyzing the historical evolution of cyberattacks can assist practitioners in predicting what future threats could be on the horizon. Real-Time and Retrospective Analyses of Cyber Security is a pivotal reference source that provides vital research on studying the development of cybersecurity practices through historical and sociological analyses. While highlighting topics such as zero trust networks, geopolitical analysis, and cyber warfare, this publication explores the evolution of cyber threats, as well as improving security methods and their socio-technological impact. This book is ideally designed for researchers, policymakers, strategists, officials, developers, educators, sociologists, and students seeking current research on the evolution of cybersecurity methods through historical analysis and future trends.

Related to biggest ransomware attacks in history

What is the difference between "largest" and "biggest"? Compare this to 'the biggest lake'. To my mind, the largest is the one with the greatest surface area, the biggest may have a smaller surface area but be deeper and therefore contain more

In charts: 7 global shifts defining 2025 so far | World Economic Forum 2025 has been marked by significant global shifts, including increased geopolitical instability, the accelerating impact of AI and a changing labour market

Which are the world’s biggest economies by GDP? | World This year has seen global growth disrupted by the COVID-19 pandemic, with many of the world’s biggest economies in recession. And the recovery will take longer than

These are the top 3 global climate risks we face globally | World In its annual Global Risk Report, the World Economic Forum named 3 key climate risks as top global challenges: urgent action is needed to combat them. Extreme weather

Top 10 Emerging Technologies of 2025 | World Economic Forum The Top 10 Emerging

Technologies of 2025 report highlights 10 innovations with the potential to reshape industries and societies

These are the Top 10 Emerging Technologies of 2025 The World Economic Forum's latest Top 10 Emerging Technologies report explores the tech on the cusp of making a massive impact on our lives

These are the world's 10 biggest corporate giants These are the world's biggest corporations, based on market capitalization

Why do the biggest economies have such different problems? China and the US are moving in opposite directions when it comes to the cost of living. We asked experts on each of those economies to explain why

Global Risks 2025: A world of growing divisions The Global Risks Report 2025 analyses global risks to support decision-makers in balancing current crises and longer-term priorities

Global Risks Report 2025 | World Economic Forum The Global Risks Report 2025 analyses global risks to support decision-makers in balancing current crises and longer-term priorities

What is the difference between "largest" and "biggest"? Compare this to 'the biggest lake'. To my mind, the largest is the one with the greatest surface area, the biggest may have a smaller surface area but be deeper and therefore contain more

In charts: 7 global shifts defining 2025 so far | World Economic Forum 2025 has been marked by significant global shifts, including increased geopolitical instability, the accelerating impact of AI and a changing labour market

Which are the world's biggest economies by GDP? | World This year has seen global growth disrupted by the COVID-19 pandemic, with many of the world's biggest economies in recession. And the recovery will take longer than

These are the top 3 global climate risks we face globally | World In its annual Global Risk Report, the World Economic Forum named 3 key climate risks as top global challenges: urgent action is needed to combat them. Extreme weather

Top 10 Emerging Technologies of 2025 | World Economic Forum The Top 10 Emerging Technologies of 2025 report highlights 10 innovations with the potential to reshape industries and societies

These are the Top 10 Emerging Technologies of 2025 The World Economic Forum's latest Top 10 Emerging Technologies report explores the tech on the cusp of making a massive impact on our lives

These are the world's 10 biggest corporate giants These are the world's biggest corporations, based on market capitalization

Why do the biggest economies have such different problems? China and the US are moving in opposite directions when it comes to the cost of living. We asked experts on each of those economies to explain why

Global Risks 2025: A world of growing divisions The Global Risks Report 2025 analyses global risks to support decision-makers in balancing current crises and longer-term priorities

Global Risks Report 2025 | World Economic Forum The Global Risks Report 2025 analyses global risks to support decision-makers in balancing current crises and longer-term priorities

What is the difference between "largest" and "biggest"? Compare this to 'the biggest lake'. To my mind, the largest is the one with the greatest surface area, the biggest may have a smaller surface area but be deeper and therefore contain more

In charts: 7 global shifts defining 2025 so far | World Economic 2025 has been marked by significant global shifts, including increased geopolitical instability, the accelerating impact of AI and a changing labour market

Which are the world's biggest economies by GDP? | World This year has seen global growth disrupted by the COVID-19 pandemic, with many of the world's biggest economies in recession. And the recovery will take longer than

These are the top 3 global climate risks we face globally | World In its annual Global Risk

Report, the World Economic Forum named 3 key climate risks as top global challenges: urgent action is needed to combat them. Extreme weather

Top 10 Emerging Technologies of 2025 | World Economic Forum The Top 10 Emerging Technologies of 2025 report highlights 10 innovations with the potential to reshape industries and societies

These are the Top 10 Emerging Technologies of 2025 The World Economic Forum's latest Top 10 Emerging Technologies report explores the tech on the cusp of making a massive impact on our lives

These are the world's 10 biggest corporate giants These are the world's biggest corporations, based on market capitalization

Why do the biggest economies have such different problems? China and the US are moving in opposite directions when it comes to the cost of living. We asked experts on each of those economies to explain why

Global Risks 2025: A world of growing divisions The Global Risks Report 2025 analyses global risks to support decision-makers in balancing current crises and longer-term priorities

Global Risks Report 2025 | World Economic Forum The Global Risks Report 2025 analyses global risks to support decision-makers in balancing current crises and longer-term priorities

What is the difference between "largest" and "biggest"? Compare this to 'the biggest lake'. To my mind, the largest is the one with the greatest surface area, the biggest may have a smaller surface area but be deeper and therefore contain more

In charts: 7 global shifts defining 2025 so far | World Economic Forum 2025 has been marked by significant global shifts, including increased geopolitical instability, the accelerating impact of AI and a changing labour market

Which are the world's biggest economies by GDP? | World This year has seen global growth disrupted by the COVID-19 pandemic, with many of the world's biggest economies in recession. And the recovery will take longer than

These are the top 3 global climate risks we face globally | World In its annual Global Risk Report, the World Economic Forum named 3 key climate risks as top global challenges: urgent action is needed to combat them. Extreme weather

Top 10 Emerging Technologies of 2025 | World Economic Forum The Top 10 Emerging Technologies of 2025 report highlights 10 innovations with the potential to reshape industries and societies

These are the Top 10 Emerging Technologies of 2025 The World Economic Forum's latest Top 10 Emerging Technologies report explores the tech on the cusp of making a massive impact on our lives

These are the world's 10 biggest corporate giants These are the world's biggest corporations, based on market capitalization

Why do the biggest economies have such different problems? China and the US are moving in opposite directions when it comes to the cost of living. We asked experts on each of those economies to explain why

Global Risks 2025: A world of growing divisions The Global Risks Report 2025 analyses global risks to support decision-makers in balancing current crises and longer-term priorities

Global Risks Report 2025 | World Economic Forum The Global Risks Report 2025 analyses global risks to support decision-makers in balancing current crises and longer-term priorities

Related to biggest ransomware attacks in history

Japan is running out of its favorite beer after ransomware attack (6h) According to cyber security experts at the Tokyo-based group Nihon Cyber Defence (NCD), Japanese companies are increasingly

Japan is running out of its favorite beer after ransomware attack (6h) According to cyber security experts at the Tokyo-based group Nihon Cyber Defence (NCD), Japanese companies are

increasingly
Ransomware Attacks Dropped by 13% in August, New Report Finds (Homeland Security Today14d) For five consecutive months, ransomware attacks have remained below 500, according to a new report. There were 328 attacks in
Ransomware Attacks Dropped by 13% in August, New Report Finds (Homeland Security Today14d) For five consecutive months, ransomware attacks have remained below 500, according to a new report. There were 328 attacks in
Ransomware attack linked to museum break-in and theft of golden exhibits (The Register on MSN10d) PLUS: Luxury brands under fire; FBI warns crims are spoofing it again; ICE buys phone cracking software Infosec in brief
Ransomware attack linked to museum break-in and theft of golden exhibits (The Register on MSN10d) PLUS: Luxury brands under fire; FBI warns crims are spoofing it again; ICE buys phone cracking software Infosec in brief
Phishing is the Leading Cause of Ransomware Attacks in 2025, SpyCloud Identity Threat Report Finds (9d) AUSTIN, Texas, Sept. 23, 2025 (GLOBE NEWSWIRE) -- SpyCloud, the leader in identity threat protection, today released its 2025 SpyCloud Identity Threat Report , unveiling new data on the surge of
Phishing is the Leading Cause of Ransomware Attacks in 2025, SpyCloud Identity Threat Report Finds (9d) AUSTIN, Texas, Sept. 23, 2025 (GLOBE NEWSWIRE) -- SpyCloud, the leader in identity threat protection, today released its 2025 SpyCloud Identity Threat Report , unveiling new data on the surge of
Google adds AI ransomware protection to Drive for Desktop (Tech Wire Asia2d) Google added AI ransomware protection to Drive for Desktop. It spots attacks early, pauses syncing, and lets users restore
Google adds AI ransomware protection to Drive for Desktop (Tech Wire Asia2d) Google added AI ransomware protection to Drive for Desktop. It spots attacks early, pauses syncing, and lets users restore
Remote Access Abuse Biggest Pre-Ransomware Indicator (Infosecurity-magazine.com24d) Abuses of remote access software and services are the most common ‘pre-ransomware’ indicators, according to new research from Cisco Talos. Adversaries frequently leverage legitimate remote services
Remote Access Abuse Biggest Pre-Ransomware Indicator (Infosecurity-magazine.com24d) Abuses of remote access software and services are the most common ‘pre-ransomware’ indicators, according to new research from Cisco Talos. Adversaries frequently leverage legitimate remote services

Related Articles

- damar hamlin injury history
- case international 2096 service manual
- apush chapter 5 quiz

Back to Home