CYBERSECURITY FIRST PRINCIPLES

A REBOOT OF STRATEGY & TACTICS

Order the book from Amazon here.

Timelines

While writing this book, I found it useful to construct timelines for various significant events. They were too long to include in the book, so I thought I would include them here.

Cybersecurity Historical Timeline

Chaos Engineering Historical Timeline

Cybersecurity Intelligence Historical Timeline

Encryption Historical Timeline

Equifax Hack Timeline

Identity and Authentication Historical Timeline

Red Team, Blue Team Historical Timeline

RSA Security Hack Timeline

SDP (Software Defined Perimeter) Historical Timeline

Cybersecurity Historical Timeline

When I think about our relatively short 50 year infosec history, I can make the case that it roughly coalesces around four phases:

Phase 1 – The mainframe (1960 - 1981)
Phase 2 – The personal computer (1981 - 1995)
Phase 3 – The Internet (1995 - 2006)
Phase 4 – The Cloud (2006 - Present)

It's not a perfect representation but each phase represents a major disruption in how people used computers and consequently, changed how security practitioners thought about securing those computers too.

As we look at the history, certain recurring elements show up at each point.

Entities. Government, commercial and academic organizations that instigated some new idea or program or research, like how Gartner coined the term Cloud Access Service denningBroker, or CASB, for security technology that protects SaaS applications in 2011.

Adversary Playbook Names. Code names assigned to hacker attack sequences across the intrusion kill chain that researchers have noticed repeatedly in the wild like BlackByte (AKA Digital Shadows), an infamous ransomware group.

Firsts. The initial time something happens, like when Aleph One published "Smashing The Stack For Fun And Profit" in 1996, the first published document about the practice of buffer overflow attacks against software.

Papers and Books. Written research that invented new things like how Dr. Dorothy Denning published her paper, "An Intrusion Detection Model," in 1986 leading the way for the first commercial Intrusion Detection tools.

People. The humans behind the great infosec ideas like how Dr. Fred Cohen published the first papers in the early 1990s that used Defense-in-Depth to describe a common cyber defense architecture model.

Law and Standards. The legislation that governments passed to control activity in cyberspace like the European Parliament's General Data Protection Regulation, a legal framework that requires businesses to protect the personal data and privacy of European Union citizens.

Technologies. A term of art referring to an application of knowledge for practical ends like passwords or two-factor-authentication.

Tools. A hardware / software device that accomplishes some cybersecurity function, such as a Firewall.

Strategy and Tactics. Strategy is the action plan that takes you where you want to go, like zero trust, and tactics are the individual steps that will get you there, like identity and authorization management systems.

Prehistory (prior to 1960)

600 BC	The Spartans used a device called a scytale to code plain text into encrypted messages. [120]
60 BC	The Romans used a simple substitution cipher where they encoded messages by shifting the letter by some agreed upon number.[120]
1553	Giovan Battista Bellaso invents the first encryption key; a shared secret phrase the recipient needs to decode the message.[120]
1824	The Prussian Army adopted a wargaming genre called Kriegsspiel (literally “wargame” in German). Blue game pieces represented the Prussian Army (the color of their uniforms). Red blocks represented the enemy forces. Network defenders adopted this model in Red Team / Blue Team / Purple Team operations in the 2000s.[69]
1874	William Stanley Jevons in his book, “The Principles of Science,” introduced the idea of asymmetric encryption by noticing that for any large number, you can’t easily know what two numbers multiplied together will produce it.[105]
1917	Edward Hebern (American) invented an electro-mechanical machine in which the key was embedded in a rotating disc.[120]
1918	Arthur Scherbius (German) invented the Enigma machine using more than one rotor.[120]
1945	Dr. Stanislaw Ulam, Dr. John von Neumann, and Dr. Nicholas Metropolis built the Monte Carlo Simulations while working to create the atomic bomb at Los Alamos during WWII.[49]

Phase 1 – The Mainframe (1960 - 1981)

1960s	Dr. Fernando Corbató introduced the idea of using passwords to keep users on the same mainframe out of each other’s files. Also, it provided a way to limit each user’s time (the initial max was four hours.)[1, 2]
1960s	John Draper and other phone phreakers, the hackers, became famous for using toy whistles found in Cap’n Crunch cereal boxes and other home made devices, that emitted a tone at 2600Hz, the exact sound that could seize a dial tone from an AT&T pay phone and allowed phone phreakers to make free phone calls.[73]

1960s	Robert Morris, while working at Bell Labs, invented storing password hashes to replace storing cleartext passwords on Unix systems. He based his system on preliminary work by Roger Needham.[105]
1967	Dr. Willis Ware published "The Ware Report" to the Defense Science Board for ARPA that led to the formal penetration testing efforts and to the development of the US Government's publication of the "Rainbow Series" of publications.[67]
1969	UCLA and the Stanford Research Institute established the internet connection. According to Andrew Blum, in the book "Tubes: A Journey to the Center of the Internet," "The internet took in its first breath."[76]
1970s	(Early) IBM invented a block cypher. Instead of using multiple letters as the enigma rotors did, the key is an entire block of text.[120]
1972	James P. Anderson, in a report to the Electronics System Division of the US Air Force, outlined a series of definitive steps that tiger teams (Penetration Test Teams) could take to test systems for their ability to be penetrated and compromised.[66, 111]
1973	The US adopted the Data Encryption Standard (DES).[120]
1974	The US Air Force conducted probably the penetration test of its Multics operating system.[66]
1976	Edward Luttwak published his book, "The Grand Strategy of the Roman Empire from the First Century AD to the Third," in which he coined the phrase "Defense-in-Depth" to describe his controversial theory about the Roman Army's defensive posture from the first to third century A.D.[3, 4]
1976	Whitfield Diffie and Martin Hellman published a research on what would be defined as the Diffie-Hellman key exchange, the beginnings of asymmetric encryption.[110]
1977	Wulf, Cohen, Corwin, Jones, Levin, Pierson, and Pollack introduced the idea of virtual machines (Virtual Sandboxes) for their Carnegie Mellon University Hydra system.[5]
1978	Gary Thuerk, a marketing manager, sent the first unsolicited bulk email (SPAM) to roughly 400 prospects via ARPANET, a forerunner to the modern internet, and reaped $13 million in sales for his company.[59]
1978	Ward Christensen and Randy Suess established the first dial-up bulletin board system in Chicago during a blizzard because they wanted a way to keep up with their computer club without having to gather together in person.[78]

1979 Unix V7 introduced the chroot system; changing the root directory of a process and its children to a new location in the filesystem. This was the beginning of process isolation: segregating file access for each process, the next step in virtual machines.[6]

1980 Leaders from the US Nuclear Regulatory Commission published their guidance on protecting nuclear power plants built before 1979. They advocate for a Defense-in-Depth model.[3, 102]

1980 James Anderson publishes "Computer Security Threat Monitoring and Surveillance," the first research on intrusion detection.[68]

Phase 2 – The PC (1981 - 1995)

1981 IBM unveiled the company's entrant into the nascent personal computer market, the IBM PC, and started the second phase of infosec history. Other companies, including Apple and Tandy Corp, were already making personal computers, but no other machine carried the revered IBM name.[75]

1983 The US Government published the first book in the series of Rainbow Books, “The Orange Book: DOD Trusted Computer System Evaluation Criteria.”[8]

1983 Steve Capps created the first fuzzer program by repurposing another tool called “The Monkey,” where a Macintosh computer could demo itself by playing back recorded actions, to create random mouse clicks and keyboard input in order to test the MacWrite and MacPaint applications. The term “fuzzer” did not come for another seven years but the technique has been widely used since by researchers trying to find software vulnerabilities.[61]

1984 Dr. Dorothy Denning, while working for SRI International, helped to develop the first model for intrusion detection, the Intrusion Detection Expert System (IDES), which provided the foundation for the IDS technology development that was soon to follow.[7]

1984 Eric Corley, AKA Emmanuel Goldstein – the shadowy leader of the resistance in George Orwell’s “1984,” founded “2600: The Hacker Quarterly,” an American magazine (sometimes called “the hacker’s bible”) that discussed issues around legal, ethical, and technical debates over hacking.[72]

1984 Security Dynamics Technologies was the first company to create FOB hardware with a one-time password (OTP) for authentication.[105 107]

1986 Dr. Dorothy Denning published her paper, "An Intrusion Detection Model," in the proceedings of the Seventh IEEE Symposium on Security and Privacy leading the way for the first commercial Intrusion Detection tools. Her paper is the basis for most of the work in IDS technology that followed.[9]

1986 The US Congress passed The Computer Fraud and Abuse Act (CFAA) as an amendment to the first federal computer fraud law to prohibit intentionally accessing a computer (hacking) without authorization with harsh penalty schemes.[70]

1986 The US Congress passed the Electronic Communications Privacy Act ("ECPA") to promote "the privacy expectations of citizens and the legitimate needs of law enforcement."[71]

1987 Bernd Fix discovered a method to neutralize the Vienna virus, becoming the first documented antivirus software ever written.[10]

1987 Omni magazine coined the word "cyberwar" and defined it in terms of giant robots and autonomous weapon.[74]

1988 Dr. Clifford Stoll publishes "STALKING THE WILY HACKER" that outlines the first ever public cyber espionage campaign sponsored by Russia using East German hacker mercenaries that targeted US governmental agencies. The next year, Stoll published his book "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage" that covered the same material with more detail.[47, 48]

1988 Jeff Mogul, Brian Reid, and Paul Vixie working for Digital Equipment Corp conducted the first research on firewall with the gatekeeper.dec.com gateway and "ScreeND."This was the first generation of firewall architectures.[11]

1988 Robert Tappan Morris, a first-year computer science graduate student at Cornell, created and launched the "Morris Worm" onto the internet; the first of its kind to cause as much damage as it did (10% of the existing internet affected). It also resulted in the first felony conviction in the US under the 1986 Computer Fraud and Abuse Act and prompted DARPA to fund the establishment of the CERT/CC at Carnegie Mellon University.[44, 45, 46]

1988 The Kerberos v4 protocol was first publicly described in a Usenex conference paper, a network security protocol that authenticates service requests between two or more trusted hosts across an untrusted network.[53]

1988 University of Wisconsin's Professor Barton Miller coined the phrase "fuzz test" in "An empirical study of the reliability of UNIX utilities," the technique has been widely used since by researchers trying to find software vulnerabilities.[62]

1989	(ISC)² founded as the International Information System Security Certification Consortium which eventually released the CISSP (Certified Information Systems Security Professional) standard approved by the ANSI Accreditation Services in 2004.[114] [115] [116]
1989	The developers from The Haystack project formed the commercial company, Haystack Labs, and released the last generation of the technology, Stalker, a host-based, pattern matching system that included robust search capabilities to manually and automatically query the audit data." [102]
1989	John Romkey created the first Internet of Things (IoT) device; a toaster that could be turned on and off over the Internet, at the '89 INTEROP conference.[30]
1989	Dave Presotto and Howard Trickey of AT&T Bell Laboratories pioneered the second generation of firewall architectures with their research in circuit relays, which are also known as circuit level firewalls. They also implemented the first working model of the third generation of firewall architectures, known as application layer firewalls. However, they neither published any papers describing this architecture nor released a product based upon their work.[11, 12]
1990	Third generation of firewall architectures was independently researched and developed by Gene Spafford of Purdue University, Bill Cheswick of AT&T Bell Laboratories, and Marcus Ranum describing application layer firewalls.[11, 12]
1990	The Chinese tell a group of North Korean hackers that they could use the Internet to steal secrets and attack the government’s enemies.[52]
1991	Marcus Ranum's firewall work received the most attention and took the form of bastion hosts running proxy services.[12]
1991	Dr. Fred Cohen published the first papers in 1991 and 1992 that used Defense-in-Depth to describe a common cybersecurity model in the network defender industry.[13, 14, 104]
1992	Digital Equipment Corp shipped DEC SEAL, the first commercial firewall and included proxies developed by Marcus Ranum.[11]
1993	Jon Arquilla and David Ronfeldt, working for the RAND Corporation, published “Cyberwar Is Coming!”, introducing the idea that cyber attacks could be used for traditional warfare.[43]

1993 Tim Howes, Steve Kille, and Wengyik Yeong develop the Lightweight directory access protocol (LDAP), a open source application protocol to manage authentication access to usernames, passwords, email addresses, printer connections, and other static data within directories. This protocol will be an important piece to Microsoft's Active Directory.[54]

1993 Jeff Moss (AKA Dark Tangent) organized the first DEFCON security conference that caters to the Hacker ethos.[88]

1994 William Cheswick and Steven Bellovin, published "Firewalls and Internet Security: Repelling the Wily Hacker," the first book on firewalls as a technology. They called it a circuit-level gateway and packet filtering technology.[103]

1994 Check Point Software released the first stateful inspection commercial firewall.[12]

1994 Amazon began work on an e-commerce service called Merchant.com to help third-party merchants like Target or Marks & Spencer build online shopping sites on top of Amazon's e-commerce engine. This eventually led to AWS.[15, 16]

1994 Vladimir Levin successfully hacked Citibank to the tune of $10 million that is likely the first significant cyber crime.[89]

1994 The Information System Security Certification Consortium (ISC)² administered the first CISSP exam. CISSP stands for The Certified Information Systems Security Professional and is arguably the most sought after certification credential by security professionals.[119]

Phase 3 – The Internet (1995 - 2006)

1995 The internet and the World Wide Web became a mainstream phenomena.[77]

1995 Citicorp hired Steve Katz to be the first Chief Information Security Officer.[90]

1995 ATT patented two-factor authentication.[105]

1995 Gartner's Jackie Fenn created the concept of a technology hype cycle: product announcement, rises through the "peak of inflated expectations," expectations diminish through the "trough of disillusionment," expectation rises through a much gentler "slope of enlightenment" and finally, reaches the "plateau of productivity." [112]

1995 Dan Farmer creates the first vulnerability scanner called SATAN (Security Administrator Tool for Analyzing Networks) "designed to scan a Unix host or set of Unix hosts on an IP network and report about well-known security vulnerabilities."[113]

1996 Aleph One published "Smashing The Stack For Fun And Profit,"the first published document about the practice of buffer overflow attacks against software.[37]

1996 The US Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to require the adoption of national standards for electronic health care transactions and code sets, as well as unique health identifiers for providers, health insurance plans and employers.[83]

1997 Deputy Secretary of Defense John Hamre, during a congressional hearing, said that the United States must prepare for an "electronic Pearl Harbor," a calamitous, surprise cyberattack designed not just to take out military command-and-control communications but to physically devastate American infrastructure.[74]

1997 This NSA Red Team conducted a no-notice Vulnerability Assessment/ Penetration Test (Code name: Eligible Receiver) of critical government networks to include the DoD. The report showed the network was so poorly protected the results were quickly classified.[100]

1997 Researchers break the Data Encryption Standard (DES).[120]

1998 Hactivist group "Cult of the Dead Cow" released the first version of Back Orifice, authored by Sir Dystic, at DEFCON 6 to demonstrate the lack of security in Microsoft's Windows 9x series of operating systems.[94]

1998 Attackers targeted a number of Department of Defense networks (Code Name: Solar Sunrise). Originally attributed to Iraq but it turned out to be two high school students from Cloverdale, California, who were arrested and pleaded guilty to the crime. Still, the attacks validated the findings to a red teaming exercise conducted earlier (Code Name: Eligible Receiver in 1997)[109]

1998 The Defense Information Systems Agency discovered Russian hacker activity against the Pentagon, National Aeronautics and Space Administration (NASA), and some affiliated academic and laboratory facilities (Code name: Moonlight Maze). The hackers stole unclassified information on contracts, research, military data, troop data, and maps of military installations.[100]

1998 Akamai builds the first Content Delivery Network (CDN); globally-distributed network of servers designed to place web content closer to its readers. It turns out that this is a decent resiliency tactic too.[117]

1998 Taher Elgamal— an engineer at Netscape — developed the original Secure Sockets Layer (SSL) protocol, which included keys and server authentication.[105]

1998 In anticipation of Y2K and other factors, U.S. President Clinton established the ISAC system, the information sharing and analysis center framework, when he signed Presidential Decision Directive-63 (PDD-63)[118]

1999 Kevin Ashton coined the term “the internet of things” at a Procter & Gamble conference.[31]

1999 The US Congress passed the Gramm-Leach-Bliley Act (GLBA) to protect consumers' personal financial information held by financial institutions.[86]

1999 Qiao Liang and Wang Xiangsui, two Chinese colonels, publish “Unrestricted Warfare: China’s Master Plan to Destroy America,” that proposes the strategy of what will become to be known as asymmetric warfare to level the playing field against the US military might.[95, 96]

2000 Poul-Henning Kamp introduced Jails that allowed administrators to partition a FreeBSD Unix computer system into several independent, smaller systems – called “jails” – with the ability to assign an IP address for each system and configuration; the next step in virtual machines.[6]

2000 Internet founding father Vint Cerf coined the phrase cyber hygiene when he testified to the United States Congress Joint Economic Committee. INfosec practitioners had been executing this best practice for at least a decade proper, but Vint Cerf gave it a name.[17]

2000 Microsoft released Windows Server 2000, the first release of Active Directory which became the de facto Identity and Access Management system for most organizations.[54]

2000	The Advanced Encryption Standard (AES) replaced DES as the standard by being faster and having the ability to use much longer keys.[120]
2001	17 software developers publish the “Agile Manifesto,” a rejection of the Waterfall model and an embracement of the idea of producing real, working code as a milestone of progress. This is the start of the Agile software development movement and the precursor to DevOps and DevSecOps.[64]
2001	The Payment Card Industry Security Standards Council established the Payment Card Industry Data Security Standard (PCI DSS), cybersecurity controls and business practices that any company that accepts credit card payments must implement.[84]
2002	Security Assertion Markup Language (SAML) V1.0 became an OASIS standard, an open source standard that allows identity providers to pass authorization credentials to service providers. OASIS is a non-profit standards body.[56]
2002	Bill Gates turns Microsoft on a dime to implement "Trustworthy Computing," shuts down Windows development for the first time ever to get a handle on the security issues the products were facing, and creates the Microsoft Security Development Lifecycle (SDL).[65]
2002	The US Congress passed the Federal Information Security Management Act that requires federal agencies to implement a program to provide security for their information and information systems.[81]
2002	The US Congress passed the Sarbanes-Oxley Act to protect investors and the public by increasing the accuracy and reliability of corporate disclosures and holds companies liable for bad Identity and Access Management.[55, 85]
2003	Amazon installs infrastructure-as-code internally (the beginnings of DevOps); a set of common infrastructure services everyone could access without reinventing the wheel every time. Business leaders realized that they could build the operating system for the internet from these services. This eventually led to AWS.[15, 16]
2003	Dave Wickers and Jeff Williams, working for Aspect Security, a software consultancy company, published an education piece in 2003 on the top software security coding issues of the day. That eventually turned into the OWASP Top 10, a reference document describing the most critical security concerns for web applications.[91]
2003	The US Department of Defense discovers the first Chinese computer cyber espionage operation codenamed “Titan Rain."[97]

2004	Google invents Site Reliability Engineering (SRE), the first foray into infrastructure as code (the beginnings of DevOps).[18]
2004	VoIP service provider BroadVoice introduced the idea of Bring Your Own Device (BYOD) to work.[29]
2005	Concur becomes the first company to offer a SaaS Cloud Platform.[19]
2005	Brad Fitzpatrick develops the first generation OpenID authentication protocol. This eventually becomes the authentication layer for OAuth.[57]
2005	Gartner security analysts Mark Nicolett and Amrit Williams coined the term SIEM (Security Event and Information Management) as an improvement to traditional log collection systems to offer long term storage, combined log analytics, with a focus on security events.[60]

Phase 4 – The Cloud (2006 - Present)

2006	Amazon becomes the first Company to offer an IaaS Cloud Platform (Amazon Elastic Compute or AWS).[15, 16]
2006	First managed identity services.[55]
2007	Palo Alto Networks launched the first next generation firewall, a firewall that not only does stateful inspection at layer 3, but more importantly, allows rules at the application layer, layer 7.[21]
2007	Russian launched DDOS attacks against Estonia.[74]
2008	According to Cisco Internet Business Solutions Group (IBSG), the Internet of Things (IoT) became real when more “things or objects” were connected to the Internet than people.[30]
2008	Russian Hackers (Turla, Snake, APT 28) penetrated the Pentagon’s classified networks. The Pentagon deployed the fix, code name Operation Buckshot Yankee later that day. This event led to the creation of what has become Cyber Command.[52]
2008	Dr. Gary McGraw published the first Building Security In Maturity Model (BSIMM) report; a survey of some 30+ companies that collated initiatives and activities around software security.[92]

2008	The Chinese People's Liberation Army (PLA) penetrated Lockheed Martin's networks and stole the plans related to the F-35, the world's most sophisticated, and certainly most expensive, fighter jet.[97]
2009	Intel is probably the first commercial company to approve a formal Bring Your Own Device (BYOD) policy when the company realized that many of its employees were bringing their own devices into work and connecting to the corporate network.[29]
2009	Pravir Chandra published the first SAMM (Software Assurance Maturity Model); a prescriptive security model that gives practitioners a way to measure how well they're doing against a set of prescribed best practices.[92]
2009	Robert Gates, President Obama's secretary of defense, concluded after the Russian (Turla, Snake, APT 28) penetration of the Pentagon's classified networks in 2008 to create the US Cyber Command to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners.[52, 101]
2010	Lockheed Martin's Hutchins, Cloppert, and Amin publish "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," the origination of the intrusion kill chain strategy.[22]
2010	John Kindervag, working for Forrester, published "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security." The idea of zero trust had been around for a number of years but this paper solidified the concept.[23]
2010	The Industrial Control Systems CERT starts tracking Industrial Control Systems vulnerabilities.[32]
2010	The US and Israeli governments launched "Olympic Games," the first public cyber attack (Stuxnet) to destroy another country's critical infrastructure; in this case, the Iranian uranium enrichment plant at Natanz. This might be the first public cyber attack to crossover from cyber espionage to cyber warfare.[50, 51, 52]
2010	First Identity as a Service in the cloud.[55]
2010	The Internet Engineering Task Force (IETF) released OAuth as an open-standard (RFC 5849) authorization protocol that describes how unrelated servers and services can safely delegate authenticated access to their assets without actually sharing credentials.[58]

2010	Google publicly announced it had been hacked by the Chinese government in what became to be known as Operation Aurora. Before, no commercial company would ever admit such a breach for fear of reputation damage. After, and aided by public disclosure laws, more and more companies follow the practice. The event also led to Google Site Reliability Engineers rebuilding the Google internal network from the ground up using Software Defined Perimeter and Zero Trust as their main strategies.[97]
2010	The Iranian Government announced the creation of a cybercorps; their answer to counter the US Cyber Command.[52]
2011	Gartner coined the term CASB (Cloud Access Service Broker) for security technology that protects SaaS applications.[24]
2011	Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, working for the US Department of Defense, published "The Diamond Model of Intrusion Analysis," written around the same time that the Lockheed Martin research team published their intrusion kill chain model. The authors designed the Diamond model specifically for intelligence analysts to track adversary groups across the intrusion kill chain.[40]
2011	The World Economic Forum coined the term Resilience "… the ability of systems and organizations to withstand cyber events …"[25]
2011	The US Office of Management and Budget (OMB) established The Federal Risk and Authorization Management Program (FedRAMP) to empower federal agencies to use modern cloud technologies, with an emphasis on security and protection of federal information.[82]
2011	The Chinese People's Liberation Army hacked RSA and stole their secret cryptographic keys responsible for the encryption function of their SecurID tokens product line that many organizations used for two factor authentication. It was the first public supply chain attack and led to the compromise of Lockheed Martin, Northrop Grumman, and L3. It was also the first time that a pure play commercial company (not a government contractor) noticed adversary lateral movement as a step in the hacking sequence; a step that had been captured by the Lockheed Martin's intrusion kill chain strategy a year before.[98]
2011	Responding to the US / Israeli operation Olympic Games, Iranian hackers began DDOSing roughly four dozen American financial institutions—including JPMorgan Chase, Bank of America, Capital One, PNC Bank, and the New York Stock Exchange.[52]
2011	Motorola added a fingerprint scanner to the ATRIX Android smartphone.[105]

2012	Iranian hackers cripple Saudi Aramco, the world's largest oil producer, destroying: 30,000 computers and 10,000 servers.[52]
2012	A number of commercial companies, like PayPal and Lenovo, formed the FIDO Alliance, which stands for Fast Identity Online, with the purpose of developing a passwordless authentication protocol. By 2013, Google, Yubico and NXP joined the Alliance and brought with them the idea of an open, second factor authentication protocol. By 2015, The Alliance announced support for contactless transport over Bluetooth and Near Field Communication (NFC).[108]
2013	Docker released an open source container management platform called dotCloud and established a partnership with Red Hat Linux. The idea of containers had been around for a while, but this started the momentum to make them standard practice.[20]
2013	Gartner's Anton Chuvakin coined the term Endpoint Threat Detection and Response (ETDR), now commonly referred to as EDR (Endpoint Detection and Response).[26]
2013	Mandiant published "APT1: Exposing One of China's Cyber Espionage Units," the first public document that outlined the Chinese government cyber attack campaigns across the intrusion kill chain. Also, the first time the general public starts to notice Cyber Threat Intelligence as something infosec professionals do.[38]
2013	MITRE established the ATT&CK Framework, an extension of the intrusion kill chain model that operationalized the Lockheed Martin strategy document with adversary tactics, techniques, and procedures.[41]
2013	General Valery Gerasimov, the Chief of the General Staff of the Russian Federation established the unofficial Gerasimov doctrine that seeks asymmetric targets (physical and virtual critical infrastructure including space) across the spectrum during war.[74]
2013	Gene Kim, Kevin Behr, and George Spafford published "The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win" introducing the idea of DevOps to the general business world.[93]
2013	Deep Panda (a Chinese hacking group) compromised OPM's database containing PII (Personal Identifiable Information) on US government clearance holders and might be the largest and most impactful cyber espionage campaign known to the public against any known country. The vast amounts of data collected plus the longevity of it (over 50 years since that's how long it will take for all individuals caught in the net to age out of government service) will be useful for many years to come.[99]

2013	Iranians breach the New York State's Bowman Avenue Dam's command-and-control system, an example of how nation states could control and damage the critical infrastructure of an enemy nation.[52]
2014	Amazon became the first Company to offer serverless functions (AWS Lambda).[27]
2014	The National Institute of Standards and Technology (NIST) published the "Framework for Improving Critical Infrastructure Cybersecurity" that became a cybersecurity best practice maturity model for the community around the ideas of Identify, Protect, Detect, Respond, and Recover.[42, 87]
2014	US intelligence agencies confirm that Russia has penetrated the US Electrical Grid in many locations using malware called "BlackEnergy" .[52]
2014	Iranians destroy the Sands Casino in Las Vegas.[52]
2014	North Korea hackers (Guardians of Peace) crippled Sony because of a movie released depicting the North Korean Supreme Leader (Kim Jong-un) in an unfavorable light. It marks the first time that a US President, President Obama, confirmed a cyber attribution on national television.[52]
2015	Google released Kubernetes 1.0; an open-source container orchestration system and gave it to The Cloud Native Computing Foundation (CNCF) to manage.[20]
2015	Security Orchestration as an idea emerged.[28]
2016	Six out of every ten companies had a Bring-Your-Own-Device (BYOD)-friendly policy in place.[29]
2016	The European Parliament adopted the General Data Protection Regulation (GDPR), a legal framework that requires businesses to protect the personal data and privacy of European Union (EU) citizens for transactions that occur within EU member states.[79]
2016	North Korean hackers steal $81 Million from the Bangladesh Central Bank. This marks the first public discovery of a new trend, nations states using government assets to conduct cyber crime for two reasons: APT Side Hustle to fund their nation state missions and State Sanctioned Organized Cyber Crime to bring revenue into the country.[52]
2017	Gartner coined the phrase Security Orchestration and Automation (SOAR); tools to orchestrate the security stack.[33]

2017	North Korean hackers launched a ransomware attack (code name: WannaCry) using the “Eternal Blue” exploit tool in the attack sequence that was stolen from the NSA by the Shadow Brokers hacktivist group and made public.[52]
2017	Russian GRU hackers, learning from the North Koreans, launched the NotPetya (Sandworm) campaign against Ukraine. Computers across the country abruptly stopped working. ATMs failed. Radiation monitors at the old Chernobyl nuclear plant couldn’t operate because the computers that controlled them went offline. The campaign targeted virtually every business in the country impacting 30 percent of the nation’s computers at one time and spread to other European countries as well.[74]
2018	Nir Zuk, the Palo Alto Networks founder and CTO, coined the phrase: XDR.[34]
2019	Gartner coined the phrase Secure Access Service Edge (SASE).[35]
2020	Rick Howard and Ryan Olson publish “Implementing Intrusion Kill Chain Strategies by Creating Defensive Campaign Adversary Playbooks,” the next extension to the Intrusion Kill Chain / Diamond / MITRE Attack framework models.[36]
2021	Darkside hackers take down the Colonial Pipeline in a ransomware attack causing some states to declare emergencies, temporary gas shortages caused by panicked motorists stocking up, and gas price hikes.[121]

References

1. “Man behind the First Computer Password: It’s Become a Nightmare,” by Danny Yadron, The Wall Street Journal, 21 May 2014.

2. “The Guy Who Invented Computer Passwords Thinks They’re a Nightmare,” by Adam Clark Estes, Gizmodo, 22 May 2014.

3. "The Next Board Problem: Automatic Enterprise Security Orchestration – a Radical Change in Direction," by Rick Howard, Palo Alto Networks, 2017.

4. “The Grand Strategy of the Roman Empire from the First Century AD to the Third,” by Edward Luttwak, Published by Johns Hopkins University Press, 1976.

5. “HYDRA -- the Kernel of a Multiprocessor Operating System,” by Wulf, Cohen, Corwin, Jones, Levin, Pierson, and Pollack, ARPA. June 1973.

6. “A Brief History of Containers: From the 1970s till Now,” by Rani Osnat, Aqua Security, 10 January 2020.

7. “The Evolution of Intrusion Detection Systems,” by Paul Innella, Tetrad Digital Integrity, LLC, Symantec, 16 November 2001.

8. “Rainbow Series.” nina.az, 30 October 2021.

9. "An Intrusion Detection Model," Dr. Dorothy Denning, Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131.

10. "Bernd Fix," Computer Hoper, 30 December 2019.

11. “Who Invented the Firewall?” by Kelly Jackson Higgins, Dark Reading, January 15, 2008.

12. “Evolution of the Firewall Industry.” by Cisco Systems, 28 September 2002.

13. “Models of Practical Defenses against Computer Viruses,” by Dr. Fred Cohen, Comput. Secur. 8 (1989): 149-160, 1989.

14. “Defense-in-depth against computer viruses,” by Dr. Fred Cohen, Comput. Secur. 11 (1992): 563-579.

15. “History of AWS,” Javatpoint, 2012.

16. “How AWS Came to Be,” by Ron Miller, TechCrunch, 2 July 2016.

17. "Joint Economic Committee,” United States Congress Joint Economic Committee," 23 February 2000

18. “Site Reliability Engineering: How Google Runs Production Systems,” by Betsy Beyer, Chris Jones, Jennifer Petoff, and Niall Richard Murphy, Published by O’Reilly Media, 16 April 2016.

19. “A SaaS History Lesson – the First SaaS Company’s Exceptional Journey,” by Tomasz Tunguz, Venture Capitalist at Redpoint, 28 April 2015.

20. “The History of Docker’s Climb in the Container Management Market,” by Stefani Muñoz, TechTarget, 2019.

21. “Nir Zuk’s Podcast on Network Security and Upcoming Technology,” by Ankur Shah, Neelima Rustagi, ZeroToExit Podcast,” 2021.

22. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” by Eric Hutchins, Michael Cloppert, Rohan Amin, Lockheed Martin Corporation, 2010.

23. "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security," by John Kindervag, Forrester, 2010.

24. “What is a CASB? Cloud Access Security Broker,” McAfee, 2019.

25. "Partnering for Cyber Resilience,” by The World Economic Forum, 2012.

26. “What Is Endpoint Detection and Response? A Definition of Endpoint Detection & Response,” by Nate Lord, Digital Guardian, 23 July 2019.

27. “What Is Serverless? Serverless Computing Explained,” by Josh Fruhlinger, InfoWorld, 15 July 2019.

28. “The Evolution of Security Operations, Automation and Orchestration,” by Jon Oltsik, CSO Online, 9 May 2018.

29. “Is BYOD (Bring Your Own Device) Dead?” by Adam Harkness, NetMotion Software, 21 October 2019.

30. “Internet of Things (IoT) History,” by Trevor Harwood, Postscapes, 12 November 2019.

31. “The IoT History and Future,” by Sandra Khvoynitskaya, 2019.

32. “IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things,” by David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Subodh Gajare, Published by Cisco Press, 13 June 2017.

33. “The Evolution of SOAR Platforms,” by Stan Engelbrecht, SecurityWeek.com, 27 July 2018.

34. “What Is XDR?,” Palo Alto Networks, 2015.

35:“What Is SASE?,” Palo Alto Networks, 2022.

36. "Implementing Intrusion Kill Chain Strategies by Creating Defensive Campaign Adversary Playbooks," by Rick Howard, Ryan Olson, and Deirdre Beard (Editor), The Cyber Defense Review, Fall 2020.

37. "Smashing The Stack For Fun And Profit," by Aleph One, Phrack 49, Volume Seven, Issue Forty-Nine File 14 of 16, 8 November 1996.

38. “APT1: Exposing One of China’s Cyber Espionage Units | Mandiant.” Mandiant.com, 2013.

39. "The Development of a Common Enumeration of Vulnerabilities and Exposures," by David Baker, Steven Christey, William Hill, and David Mann, MITRE, 1999.

40. "The Diamond Model of Intrusion Analysis,” by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, Center for Cyber Threat Intelligence and Threat Research, Hanover, MD, Technical Report ADA586960, 05 July 2011.

41. "MITRE ATT&CK: Design and Philosophy," by Blake Strom, Andy Applebaum, Doug Miller, Kathryn Nickels, Adam Pennington, and Cody Thomas, MITRE, March 2020.

42. “Framework for Improving Critical Infrastructure Cybersecurity,” by the National Institute of Standards and Technology (NIST), Version 1.0, 12 February 2014

43. “Cyberwar Is Coming!” by Jon Arquilla and David Ronfeldt, RAND Corporation, 1993.

44. “The Day Computer Security Turned Real: The Morris Worm Turns 30,” by Steven Vaughan-Nichols, Senior Contributing Editor, ZDNET, 2 November 2018.

45. “First Indictment under Computer Fraud Act,” Tony Long, WIRED, 26 July 2011.

46. “What Is a CERT, Anyway?” CERT NZ,” 2020.

47. “Stalking The Wily Hacker,” by Clifford Stoll, Communication Of The ACM, vol. 31. No. 5, May 1988.

48. “The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage,” by Clifford Stoll, Published by Gallery Books, 1989.

49. “The Beginning Of The Monte Carlo Method,” by N. Metropolis, Los Alamos Science Special Issue, Vol. 15, 1987, pp. 125-130, 1987.

50. “Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon,” by Kim Zetter, Published by Crown, 3 June 2014.

51. “Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power,” by David E. Sanger, Published by Crown Publishing Group, 1 January 2012.

52. “The Perfect Weapon: How the Cyber Arms Race Set the World Afire,” by David E. Sanger, Published by Crown, 19 June 2018.

53. “Kerberos and Windows Security: History,” by Robert Broeckelmann, Medium, 16 May 2018.

54. “History of LDAP,” by ldapwiki.com.

55:“The Evolution Of IAM (Identity Access Management,)” by SolutionsReview, Youtube, 3 September 2019.

56:“History of SAML,” by saml.xml.org, 2015.

57. “SAML2 vs JWT: Understanding OpenID Connect Part 1,” by Robert Broeckelmann, Medium, 25 March 2017.

58. “What is OAuth? How the open authorization framework works,” by Roger A. Grimes and Josh Fruhlinger, CSO, 20 September 2019.

59. “40 Years on from the First Spam Email, What Have We Learned? Here Are 5 Things You Should Know about Junk Mail,” by Rob Smith, World Economic Forum, 4 May 2018.

60. “The Evolution of SIEM,” by Christian Wiens, Security Boulevard, 13 October 2020.

61. “History: what is fuzzing?” fuzzing.info, 6 May 2012.

62. “An empirical study of the reliability of UNIX utilities,” Barton Miller, Louis Fredriksen, and Bryan So, Communications of the ACM, Volume 33, pp 32–44, 12 December 1990

63. “Celebrating 20 Years of Trustworthy Computing,” by Aanchal Gupta, Microsoft, 21 January 2022.

64. “The Winter Getaway That Turned the Software World Upside Down,” by Caroline Mimbs Nyce, The Atlantic, 8 December 2017.

65. “The Story behind the Microsoft Security Development Lifecycle,”by Rod Trent, ITPro Today, 7 March 2014.

66. “The History of Penetration Testing,” Infosec Resources, 4 September 2021.

67. “The Passing of a Pioneer,” CERIAS Blog, Purdue, 2013.

68. "Computer Security Threat Monitoring and Surveillance," by James Anderson, csrc.nist.gov, 26 February 1980.

69. “Kriegsspiel – How a 19th Century Table-Top War Game Changed History,” by MilitaryHistoryNow.com, 19 April 2019.

70. “Computer Fraud and Abuse Act (CFAA),” NACDL - National Association of Criminal Defense Lawyers, 2022.

71. “Electronic Communications Privacy Act (ECPA),” by EPIC (Electronic Privacy Information Center), 2016.

72. “2600: The Hacker Quarterly,” by Encyclopædia Britannica, 2022.

73. “Early Hackers Used Whistles from Cap’n Crunch Cereal Boxes,” by Anne Ewbank, Atlas Obscura, 18 May 2018.

74. "Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers," by Andy Greenberg, Published by Doubleday, 7 May 2019.

75 “How the IBM PC Won, Then Lost, the Personal Computer Market,” by James Cortada, IEEE Spectrum, 21 July 2021.

76. "Tubes: A Journey to the Center of the Internet,” by Andrew Blum, Published by Ecco, 1 January 2012.

77. “A Short History of the Internet,” by the National Science and Media Museum, 2020.

78. “The Lost Civilization of Dial-Up Bulletin Board Systems,” by Benj Edwards, The Atlantic, 4 November 2016.

79. “The Birth of GDPR: What Is It and What You Need to Know,” by Andrew Rossow, Forbes, 10 December, 2021.

80. “Collapse of the Soviet Union | Causes, Facts, Events, & Effects,” by Encyclopædia Britannica, 2022.

81. “Security and Privacy Laws, Regulations, and Compliance: The Complete Guide.” CSO staff. 2021, 3 September 2021.

82. “Program Basics,” by FedRAMP.gov, 2022.

83. “Security and Privacy Laws, Regulations, and Compliance: The Complete Guide,” CSO staff, CSO Online, 3 September 2021.

84. “Security and Privacy Laws, Regulations, and Compliance: The Complete Guide.” CSO Staff, CSO Online, 3 September 2021.

85. “Security and Privacy Laws, Regulations, and Compliance: The Complete Guide,” CSO Staff, CSO Online, 3 September 3 2021.

86. “Security and Privacy Laws, Regulations, and Compliance: The Complete Guide,” CSO Staff, CSO Online, 3 September 3 2021.

87. “History and Creation of the Framework,” by Nicole Keller, NIST, 8 February 2018.

88. “The History of Computing: DEF CON: A Brief History of the Worlds Largest Gathering of Hackers,” by Charles Edge, Thehistoryofcomputing.net, 2022

89. “25 Years Later: Looking Back at the First Great (Cyber) Bank Heist,” by Zia Hayat, Dark Reading, 2 January 2019.

90. “CISO Conversations: Steve Katz, the World’s First CISO,” by Kevin Townsend, Securityweek.com, 1 December 2021.

91. “The Start of OWASP – a True Story,” by Mark Curphey, Veracode, 26 May 2014.

92. “About the Building Security in Maturity Model,” BSIMM.” Bsimm, 2021.

93. “The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win,” by Gene Kim, Kevin Behr, and George Spafford, Published by IT Revolution Press, 10 January 2013.

94. “Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World,”by Joseph Menn, Published by PublicAffairs, 4 June 2019.

95. “Recognizing and Adapting To Unrestricted Warfare Practices by China,” by COL Bryan K. Luke, Air War College, 15 February 2012

96. “Unrestricted Warfare : China’s Master Plan to Destroy America,” by Qiao Liang and Wang Xiangsui, Published by Pan American Publishing Company, February 1999.

97. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," by Bryan Krekel, George Bakos, Christopher Barnett, Northrop Grumman Corporation Information Systems Sector, The US-China Economic and Security Review Commission, October 2009.

98. "The Full Story of the Stunning RSA Hack Can Finally Be Told," by Andy Greenberg, Wired, 20 May 2021.

99. "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," by Committee on Oversight and Government Reform US House of Representatives, 114th Congress, 7 September 2016.

100. "A Bunch of Hacks," by CSO Staff, CSO Online, April 2004.

101. "U.S. Cyber Command," by Command History, Cybercom.mil, 2020.

102. "An Approach For Using Probabilistic Risk Assessment In Risk-Informed Decisions On Plant-Specific Changes To The Licensing Basis: Regulatory Guide 1.174, Revision 3," by Anders Gilbertson, US Nuclear Regulatory Commission, January 2018.

103. "Firewalls and Internet Security: Repelling the Wily Hacker," by William Cheswick and Steven Bellovin, Published by Addison-Wesley Professional, 28 April 1994.

104. Dr. Fred Cohen, Rick Howard, Phone Conversation, 29 August 2016.

105. "A Developer's History of Authentication," by Workos.com, 5 September 2020.

106. "A Review of the Evolution of Multi-Factor Authentication (MFA) Technology," by Alexandra Daragiu, TypingDNA, 16 July 2019.

107. "Digital authentication: The past, present and uncertain future of the keys to online identity," BY COREY NACHREINER, GeekWire, 22 September 2018.

108. "History of FIDO Alliance - FIDO Alliance." FIDO Alliance, October 19, 2021.

109. "Solar Sunrise,"by The IT Law Wiki, 2022.

110."A Brief History of Encryption (and Cryptography)," by the Thales Group, October 2021.

111. "COMPUTER SECURITY TECHNOLOGY PLANNING STUDY," by James P. Anderson, Electronics System Division, Air Force Systems Command, USAF, October 1972.

112. "Mastering the Hype Cycle: How to Choose the Right Innovation at the Right Time," by Jackie Fenn and Mark Raskino, Published by Harvard Business Review Press, 16 September 2008.

113. "CERIAS - Center for Education and Research in Information Assurance and Security: Info About SATAN," Purdue.edu, 2022.

114. "CISSP ANSI Accreditation Services," by Ansica.org, 2016.

115. "(ISC)2 Security Transcends Technology," Archive.org, WayBackMachine, 2021.

116. "Inspire a Safe and Secure Cyber World: History Of (ISC)²," by (ISC)², 2022.

117. "Discontent and Disruption in the World of Content Delivery Networks," Jonathan Shieber, TechCrunch, June 2017.

118. "Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators," Federal Register, 5 August 1998.

119. "History of CISSP," by Theknowledgeacademy.com.

120. "A brief history of encryption (and cryptography)" by the Thales Group, 2021.

121. "Regulator Proposes $1 Million Fine for Colonial Pipeline One Year after Cyberattack," By Eduard Kovacs, Securityweek.com, 9 May 2022.

Identity and Authentication Timeline

1874

- William Stanley Jevons, in his book, “The Principles of Science,” introduced the idea of asymmetric encryption by noticing that for any large number, you can’t easily know what two numbers multiplied together will produce it.

1960s

- Fernando Corbató introduces the use of passwords.
- Robert Morris, while working at Bell Labs, invented storing password hashes to replace storing cleartext passwords on Unix systems. He based his system on preliminary work by Roger Needham.

1960s - 1970s:

- Computer administrators used Access Control Lists (ACLs) mechanisms to limit access.

Mid-1980s

- Security Dynamics Technologies was the first company to create FOB hardware with a one-time password (OTP) for authentication.

1988

- The Kerberos v4 protocol was first publicly described in a Usenex conference paper.

1993

- Tim Howes, Steve Kille, and Wengyik Yeong develop LDAP.

1995

- AT&T patented two-factor authentication in 1995.

Late 1990s

- Taher Elgamal — an engineer at Netscape — developed the original Secure Sockets Layer (SSL) protocol, which included keys and server authentication.

1999

- Microsoft introduced a product called Microsoft Passport that was soundly rejected by the internet for many reasons but mostly because it was proprietary.

2000

- Windows Server 2000 released, the first release of Microsoft Active Directory.

1999

- Microsoft introduced a product called Microsoft Passport that was soundly rejected by the internet for many reasons but mostly because it was proprietary.

2002

- Sarbanes Oxley: Held companies liable for bad access control.
- SAML V1.0 became an OASIS standard.

2005

- Brad Fitzpatrick develops the first generation OpenID authentication protocol.

2006

- First managed identity services.

2007

- The second-generation OpenID specification (OpenID v2.0).

2010

- First Identity as a Service in the cloud.
- OAuth was released as an open standard as RFC 5849, and quickly became widely adopted.

2011

- OpenID had become an also-ran, and, Wired declared that "The main reason no one uses OpenID is because Facebook Connect does the same thing and does it better. Everyone knows what Facebook is and it's much easier to understand that Facebook is handling your identity than some vague, unrecognized thing called OpenID." (Facebook Connect turned out to not be a world-beater either, but at least people knew what Facebook was.)
- Motorola added a fingerprint scanner to the ATRIX Android smartphone.

2012

- OAuth 2.0 released; widely criticized for multiple reasons but also widely used.
- A number of commercial companies, like PayPal and Lenovo, formed the FIDO Alliance, which stands for Fast Identity Online, with the purpose of developing a passwordless authentication protocol. By 2013, Google, Yubico and NXP joined the Alliance and brought with them the idea of an open, second factor authentication protocol. By 2015, The Alliance announced support for contactless transport over Bluetooth and Near Field Communication (NFC).

2014

- OpenID Connect was released, which reinvented OpenID as an authentication layer for OAuth.

SDP Timeline

1996

- A Microsoft employee developed the peer-to-peer tunneling protocol, or PPTP, the precursor to modern VPNs

2001

- James Yonan developed OpenVPN and used GPL (GNU General Public License) to publish it.

2004

- The Jericho Forum began talking about De-perimeterisation.

2007

- The US military incorporated some of those ideas into their Black Core initiative in 2007.
- Somewhere between 2007 then and 2010, the community started to refer to De-perimeterisation as Software Defined Perimeter or SDP.

2010

- Google got hit by a massive Chinese cyber espionage attack coined Operation Aurora, their Site reliability Engineers rolled out an internal version of SDP as part of a network redesign.
- John Kindervag releases his "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security," that formalizes the zero trust theory for the community.

13 November 2013

- Cloud Security Alliance Announces Software Defined Perimeter (SDP) Initiative
- Google launched a commercial offering of their internal SDP architecture called Beyond Core.

April 2014

- Cloud Security Alliance releases its "SDP Specification 1.0."

2017

- Evan Gilman and Doug Barth publish their Cybersecurity Canon Hall of Fame book, "Zero Trust Networks," in which they outline how they built their own SDP and zero trust networks.

August 2020

- NIST releases their Zero Trust Architecture document that outlines some of the early discussion of software defined perimeter.

10 March 2022

- Cloud Security Alliance Announces issues Expanded Specification for the Software-Defined Perim

OPM Timeline

1996

- USIS wins first contract to privatize the investigative branch of OPM.

2009

- OPM's Federal Investigative Services (FIS) contracted with three background investigative contractors: US Investigations Services (USIS), KeyPoint Government Solutions (KGS), formerly Kroll, and CACI International (CACI).

2011

- USIS became the subject of a whistle-blower lawsuit claiming that USIS charged OPM for finished thousands of background investigations when in fact they hadn't done them..

May 2012

- Members of the hactivist group Anonymous (AKA @k0detec) stole 37 USER ID / Password records from OPM.

July 2012

- US CERT discovers Command and control activity from OPM via malware called Hikit, associated with a Chinese cyber adversary group (the 2nd Bureau of the People's Liberation army - Unit 61398) commonly referred as Axiom.

April 2013

- Deep Panda hackers initially compromise USIS.

November 2013

- Deep Panda hackers, called X1 by the Congressional OPM data breach report, exfiltrated manuals and IT system architecture information.

December 2013

- Deep Panda hackers compromise KeyPoint.

2014

- The OPM IT team pushed their leadership to purchase Cylance's Protect, a higher-end product than the Cylance demo product they were using. OPM IT leadership rejected it because of office politics.

23 January 2014

- The U.S. Justice Department sues USIS in a 25-page complaint filed in United States District Court in Montgomery, Ala., claiming that, from 2008 to 2012, about 40 percent of the company's investigations were fraudulently submitted.

20 March 2014

- US-CERT notifies OPM of data exfiltration.
- OPM doesn't publicize the breach.
- OPM Investigators thought that the Deep Panda penetration was confined to a part of the network that didn't have any personnel data.
- OPM officials chose to allow the attackers to remain so they could monitor them and gain counterintelligence.
- OPM started planning for what they called the "big bang"—a system reset that would purge the attackers from the system

25 March 2014

- OPM CIO Donna Seymour briefed on the "big bang."

April 2014

- Deep Panda hackers (presumably) gained initial access to Anthem.

21 April 2014

- OPM contractor (SRA) discovers malware.

25 April 2014

- opmsecurity.org registered a command and control mechanism that implied that the discovered malware had been installed as far back as 2013.

7 May 2014

- Deep Panda hackers, dubbed X2 by the Congressional report, logged in as a KeyPoint contractor using OPM credentials and installed PlugX. This breach went undetected and the "big bang" didn't remove X2's access.

27 May 2014

- Big Bang Strategy shuts down infected systems but misses Keypoint install.
- Deep Panda hackersbegan loading keyoggers onto database administrators' workstations.

5 June 2014

- Deep Panda hackers install malware on a KeyPoint web server.

10 June 2014

- OPM CIO Donna Seymour testified before the Senate Homeland Security and Government Affairs Subcommittee on her strategic information technology plan; does not disclose the hacks

12 June 2014

- OPM installs an evaluation copy of Cylance Product

20 June 2014

- Deep Panda hackers conduct a remote (RDP) session with important and sensitive servers supporting the background process; not discovered until Spring 2015.

22 June 2014

- DHS releases incident report for first breach discovered on 20 March 2014.

23 June 2014

- Deep Panda hackers likely first had access to OPM's mainframe.

July - August 2014

- Deep Panda hackers exfiltrated the background investigation data from OPM's systems.
- Once established on the agency’s network, they used trial and error to find the credentials necessary to seed the jumpbox with their PlugX variant.

- During the long Fourth of July weekend, when staffing was sure to be light, the hackers began to run a series of commands meant to prepare data for exfiltration.
- Deep Panda hackers (X2) copied bundles of records onto drives from which they could be snatched, chopped them up into .zip or .rar files to avoid causing suspicious traffic spikes.

9 July 2014

- OPM acknowledges the March 2014 breach to the NYTs. No PII Lost (Just manuals and technical documents which is true).

21 July 2014

- OPM Director Katherine Archuleta downplayed the breach in an ABC interview: “We did not have a breach in security. There was no information that was lost. We were confident as we worked through this that we would be able to protect the data.”

29 July 2014

- Deep Panda hackers registered opmlearning.org to Tony Stark and used it as a C&C node.

August 2014

- USIS notified OPM of their own breach.

6 August 2014

- OPM issued a stop work order to USIS

16 August 2014

- KeyPoint malware installed on 5 June 2014 ceases to function.

25 August 2014

- Personal data of 25,000 government employees was likely compromised in the cyber-attack against USIS
- The Justice Department joined the whistleblower civil suit, accusing the company of submitting 665,000 background checks that were incomplete.

12 September 2014

- OPM declined to exercise its option to continue using USIS services.

October 2014

- Deep Panda hackers bridge from the OPM network to the Department of the Interior which holds additional OPM Personnel Records (4.2 million)

December 2014

- KeyPoint announced a breach of its own, 4.2 million records exfiltrated.
- Deep Panda hackers exfiltrated 80 million records from Anthem.

January 2015

- Anthem discovers Deep Panda hackers in their networks.

February 2015

- ThreatConnect's analysis of the Anthem hack discovered a suspicious domain registered to “Tony Stark”—the alter ego of Iron Man (opm-learning.org).
- Anthem discloses their breach to the public.

Spring 2015

- OPM discovers a Deep Panda remote session with important and sensitive servers that occurred on 20 June 2014.

3 March 2015

- Deep Panda hackers register idc-news-post.com and use it as another C2 node and data exfiltration.

9 March 2015

- OPM shuts down beaconing activity from opmseccurity.org (Steve Rogers).

March 2015

- Deep Panda's last recorded beaconing activity to opmsecurity.org.

26 March 2015

- Deep Panda hackers exfiltrate fingerprint data

1 April 2015

- Curtis Mejeur started work as one of OPM's senior IT strategists.

15 April 2015

- Brendan Saulsbury discovers command and control beaconing from OPM's network to opmsecurity.org with Cylance's Cylance V product.
- They realized that Deep Panda still had a foothold in their system
- OPM notifies US-CERT about suspicious network traffic related to opmsecurity.org.

16 April 2015

- Curtis Mejeur assigned the job to eradicate Deep Panda out of the OPM network.
- OPM staff requested Cylance's help fusing Cylance V to diagnose forensic images of OPM servers. Since this was a task more suited to Cylance Protect, they rolled out that tool in a free trial mode, installed on 2000 devices, and it "lit up like a Christmas tree" with widespread infections.

19 April 2015

- A Cylance technician, after discovery of a rare Deep Panda mistake (undeleted .rar file), told his CEO, Stuart McClure, “They are f*&ked btw.”

21 April 2015

- Investigators identified over 2,000 individual pieces of malware that were unrelated to the Deep Panda hacks (everything from routine adware to dormant viruses).
- Investigators discover that the Deep Panda hackers installed the PlugX variant on fewer than 10 OPM machines including including the jumpbox, the administrative server that’s used to log in to all the other servers.
- CyTech arrived at OPM for a long-scheduled appointment to demonstrate their CyFIR product. The breach was not public knowledge at this point, and OPM staff did not share any information about it with company founder Ben Cotton, who was there to lead the demo. CyFIR also detected the malware, and Cotton immediately agreed to help with the response. Realizing that the crisis was grave enough to demand immediate action, Cotton began providing software and services based on a handshake agreement.
- OPM racked up more than $800,000 in bills from CyTech—but no contract was executed and CyTech was not paid.

22 April 2015

- OPM CIO Donna Seymour testifies before the committee and discloses the "manual" breach.
- She made a series of false and misleading statements under oath regarding the agency's response.
- She testified that OPM purchased CyTech licenses, but OPM did not make any purchases from CyTech.
- She also testified that CyTech's CyFIR tool was installed in a quarantine environment for the demonstration, but this tool was running on a live environment at OPM when it identified malware on April 22, 2015.
- OPM IG first notified (accidental chance encounter in the hall); advises no need for a public announcement

23 April 2015

- OPM determines they have a major incident involving the exfiltration of personnel records which triggers a requirement to notify Congress.

24 April 2015

- As part of a grid modernization program in Washington, OPM's building was scheduled to have its power cut for several hours.
- OPM decided that, even though it would mostly be just a psychological triumph, they would dump the malware just minutes before the blackout. If Deep Panda was monitoring the network, they wouldn't realize their access had been cut until everything finished booting up at least 12 hours later.
- By the time power was restored on the 25th, the Deep Panda no longer had the means to roam OPM's network—or at least that's what everyone hoped.
- OPM orders global Quarantine.

26 April 2015

- Cylance engineers identify command and control session from important and sensitive servers on June 2014

30 April 2015

- OPM Notifies Congress.

20 May 2015

- OPM notices another large scale exfiltration which triggers another requirement to notify Congress.

27 May 2015

- OPM notifies Congress.

June 2015

- Tony Scott, US federal CIO, orders a 30 day sprint to improve basic hygiene throughout the government. “Don’t waste a good crisis,”

4 June 2015

- OPM briefs the media about 4.2 million records stolen.

16 June 2015

- OPM Director Katherine Archuleta repeatedly told the House Oversight and Government Reform Committee that she couldn’t say if any non-personnel information was lost in the 2014 hack.

19 June 2015

- FireEye attributes Deep Panda (first noticed by Crowdstrike) as the adversary campaign that conducted attacks against OPM, at least the hackers used some of the same tactics.

24 June 2015

- OPM CIO Donna Seymour testifies before the committee and minimizes the importance of the 2014 manuals breach.

29 June 2015

- The American Federation of Government Employees (AFGE - Union for KeyPoint employees) files a class action lawsuit alleging that "OPM violated our constitutional right to informational privacy by recklessly disregarding its Inspector General’s warnings over many years about its IT security deficiencies."
- A judge threw the suit out in 2017 because the Privacy Act, the law that the suit was based on, used the word "disclosed" in relation to data and that didn't apply in cases where data was stolen but not publicly revealed.

30 June 2015

- OPM finally decides to buy Cylance Protect a day before the trial period was set to elapse (The were in trial mode all this time) . Cylance didn’tactually receive payment for months.
- Cylance reports that on the 10,250 devices they are deployed on, they found nearly one piece of malware for every five devices.

9 July 2015

- OPM issues a press release confirming 21.5 million records compromised.

10 July 2015

- OPM Director Katherine Archuleta resigns

23 September 2015

- OPM updates fingerprint record loss estimate from 1.1 million fingerprints to 5.6 million.

22 February 2016

- OPM CIO Donna Seymour resigns.

Red team, blue team timeline

From the Roman Catholic Church's "Office of the Devil's Advocate" to the Kriegsspiel of the Prussian General Staff to the secretive AMAN organization, Israel's Directorate of Military Intelligence, the roots of red teaming run deep.

Early 19th century:
The Prussian Army adopted a wargaming genre called Kriegsspiel (literally “wargame” in German) to train its officers. One group of officers developed a battle plan, and another group assumed the role of the opposition, trying to thwart it. Blue game pieces stood in for the home team—the Prussian Army—since most Prussian soldiers wore blue uniforms. Red blocks represented the enemy forces—the red team—and the name has stuck ever since.

World War II:
British Field Marshal Bernard Montgomery relied upon junior officers to study German Field Marshal Irwin Rommel in Africa and Europe, then assesses the Allies' plans.

Early 1970s:
The US Navy established the SSBN Security Program to identify potential vulnerabilities that the Soviet Union might exploit .

1972:
Scientific philosopher Karl Popper wrote, “In science we need to form parties, as it were, for and against any theory that is being subjected to serious scrutiny.”

1982:
President Ronald Reagan signed a National Security Decision Directive to create a permanent "Red Team" to challenge US verification capabilities, assumptions, and policies in order to anticipate how, in what ways, and for what purposes, the Soviets might try to avoid compliance with the provisions of arms control agreements.

1984:
President Ronald Reagan signed a National Security Decision Directive to create a Red Team review panel to consider and anticipate possible Soviet noncompliance, concealment, and deception activity.

1990:

The presidential commission on the bombing of Pan Am 103 directed the FAA to develop "measures to improve testing of security systems." This was the birth of the Red Team.

1998:
Secretary Rumsfeld chaired the Ballistic Missile Threat Committee that examined the same data available to the intelligence community but identified alternative paths adversaries might take and came to different conclusions about the threat.

1999:
The US Army established a Red Franchise organization within its Training and Doctrine Command (TRADOC) to guide Army training, concept and force development, experimentation, and transformation.

12 Sep 2001:
Around midnight, then-Director of Central Intelligence George Tenet decided to form a group of contrarian thinkers to challenge conventional wisdom in the intelligence community and mitigate the threat of additional surprises through “alternative analysis.”

2003:
Red teams in the military got a boost after a 2003 Defense Science Review Board recommended increasing their use to help guard against the shortcomings that led up to 11 September 2001.

2004:
Largely in response to the 2003 Defense Science Review Board recommendations, the Army stood up its service-level red team, the Army Directed Studies Office (ADSO).

2006:
The first class graduated from the Red Team University course at Fort Leavenworth's University of Foreign Military and Cultural Studies as the war in Iraq entered its fourth year.

2012:
Then-CIA Director Gen. David Petraeus directed the Red Cell to “take on our most difficult challenges” and “shock us.”

Intelligence Timeline

1988

- The first CERT: In the aftermath of the Morris Worm—the first destructive Internet worm— DARPA (Defense Advanced Research Projects Agency, a science and technology organization of the US Department of Defense) sponsored Carnegie Mellon University to establish the first CERT/CC (Computer Emergency Response Team/Coordination Center).

1990

- CERTs: FIRST was founded to bring together incident response and security teams from every country across the world to ensure a safe internet for all.

1993

- CERTs: The Air Force established the AFCERT (Air Force Computer Emergency Response Team). The other services followed suit soon thereafter.

1996

- The first ISAO: The FBI founded the InfraGard National Members Alliance, or InfraGard National, to facilitate information sharing between law enforcement and the private sector. ISAOs would not be an official thing until 2015.

1993

- CERTs: The military CERTS contributed to the eventual stand-up of the Joint Task Force - Computer Network Defense (JTF-CND).

22 May 1998

- The first ISACs: U.S. President Clinton established the ISAC system, the information sharing and analysis center framework, when he signed Presidential Decision Directive-63 (PDD-63)

2000

- CERTs: The United States Computer Emergency Response Team (US-CERT) initially formed. It eventually became the Computer Emergency Readiness Team.

Early 2000s

- Traffic Light Protocol: The National Infrastructure Security Coordination Centre (NISCC), an inter-departmental center of the UK government (now Center for the Protection of National Infrastructure | CPNI), developed The Traffic Light Protocol (TLP), a method for labeling and handling shared sensitive information.

2002

- DHS: US Congress established the Department of Homeland Security (DHS) combining 22 different federal departments and agencies into a unified, integrated Cabinet agency.
- DHS: DHS Assigned the responsibility for “responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world.”

2004

- Fusion Centers: In response to 9/11, the U.S. Congress passes the Intelligence Reform and Terrorism Prevention Act to provide regional situational awareness and analysis (including cyber) at both the state level and major metropolitan level in the U.S.

2009

- NCCIC: The National Cybersecurity and Communications Integration Center (NCCIC) created as a unified operations center combining the U.S. Computer Emergency Readiness Team (US-CERT), the National Coordinating Center for Telecommunications (NCC), and the Industrial Control Systems CERT.

2010

- Kill Chain: Lockheed Martin’s Hutchins , Cloppert , and Amin publish “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" , the origination of the intrusion kill chain strategy.

2011

- Kill Chain: Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, working for the US Department of Defense, published "The Diamond Model of Intrusion Analysis”, written around the same time that the Lockheed Martin research team published their intrusion kill chain model. The authors designed the Diamond model specifically for intelligence analysts to track adversary groups across the intrusion kill chain.

2013

- Kill Chain: MITRE established the ATT&CK® Framework , an extension of the intrusion kill chain model that operationalized the Lockheed Martin strategy document with adversary tactics, techniques, and procedures.

2015

- The first ISAOs: U.S. President Obama, with Executive Order 13691, established the Information Sharing and Analysis Organization (ISAO) framework that made it legal to share information about cybersecurity incidents without fear
- ISAOs: Congress passes the Cybersecurity Information Sharing Act (CISA), the federal law that provides various protections to non-federal entities that share cyber-threat indicators or defensive measures with each other or with the Federal Government. CISA removes barriers that were impeding robust cyber information sharing in the U.S

2018

- US sharing adversary Playbook intelligence: The U.S. Justice Department indicts members of two specific units of the Main Intelligence Directorate of the Russian General Staff—known by the acronym GRU—that are called Unit 26165 and Unit 74455,

the first time a U.S. Government agency shared tactics, techniques, and procedures across the intrusion kill chain of an adversary playbook to the public.

August 2021

- JCDC: The Cybersecurity and Infrastructure Security Agency (CISA) established the Joint Cyber Defense Collaborative (JCDC), a group of public and private sectors as well as federal and SLTT (State, Local, Tribal, and Territorial Government entities) to strengthen the nation's cyber defenses through innovative collaboration, advanced preparation, and information sharing and fusion.

February 2022

- Shields Up: Two days after Russia began its military invasion of Ukraine, CISA released its first Shields Up warning for US-based organizations, stating: "Every organization—large and small—must be prepared to respond to disruptive cyber activity."

March 2022

- US sharing adversary Playbook intelligence: The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE) release a joint Cybersecurity Advisory (CSA) to provide information on multiple intrusion campaigns conducted by state-sponsored Russian cyber actors from 2011 to 2018 that targeted U.S. and international Energy Sector organizations using the MITRE ATT&CK® framework.

May 2022

- US sharing adversary Playbook intelligence: The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) release a joint Cybersecurity Advisory (CSA) to warn organizations that Russian state-sponsored cyber actors have gained network access through exploitation of default MFA protocols and a known vulnerability using the MITRE ATT&CK® framework.

Equifax Hack Timeline

2017

10 March

Mandiant says the first evidence of hacker “interaction” occurred on March 10th, considerably earlier than May 29thas Equifax originally stated.[4] [7]

Between May 13th and late July

Intruders

- Accessed sensitive information “stored in databases in an Equifax legacy environment”. [7]
- Compromised two systems that support Equifax’s online dispute application.[7]
- Set up “about 30 web shells”that were accessed from around 35 “distinct public IP addresses”. [7]

According to Mandiant, the attackers methods and tools do not match any “threat actor group” it tracks, and does not “overlap with those seen in previous investigations by the firm”. [7]

29 July

The in-house security team discovered and blocked the assault, and then took the website offline the following day after observing additional questionable activity. A followup investigation determined that hackers gained access to Equifax’s archives through a known security flaw in its database framework.[5]

2 August

Equifax hired Mandiant, an independent cybersecurity firm, to investigate the breach. The inquiry concluded that the hack may have involved the theft of personal data including credit card, social security and, in some cases, drivers’ license numbers, birth dates, and addresses of about 143 million U.S. consumers – roughly 60 percent of American adults.[5]

7 September

Equifax publicly acknowledged the breach and took steps to provide consumers with information and assistance to find out if their personal data had been compromised. [5]

- Creating a website specifically for consumers to find out if they had been impacted, to learn more information about the hack, what they might be able to do about it, and what they can do to protect themselves from potential future cyberattacks.
- Offering free credit file monitoring and identity theft protection to U.S. consumers whether they were affected by the attack or not.
- Establishing a call center to answer consumer questions concerning the breach and to encourage consumers to sign up for the company's monitoring and theft protection service

8 September

Equifax shares plunge 13.7% in first day of trading after breach announced.[4]

10 September

Customers who signed up post data breach to Equifaxs' credit monitoring program learn that in the Equifax terms of service, they are barred from participating in any class-action lawsuits that may arise from the incident.[6]

11 September

Sen. Orrin Hatch, R-Utah, who chairs the Senate Committee on Finance, and Sen. Ron Wyden, D-Oregon, the panel's ranking minority member, ask the credit-reporting giant for a timeline of the breach, along with details of Equifax's efforts to quantify the scope of the intrusion and limit consumer harm.[4]

12 September

Equifax CEO apologizes in USA TODAY op-ed.[4]

Equifax announced both its chief information officer and chief security officer would retire, effective immediately.[5]

13 September

BBC News: Equifax had 'admin' as login and password in Argentina.[5]

15 September

Equifax announces its chief information officer, Susan Mauldin, and chief security officer, David Webb are retiring "effective immediately."[4]

21 September

The company is so inept, it's been directing people to a white hat phishing site specifically intended to test the company's security response.[6]

26 September

Equifax announces its CEO, Richard Smith, retires. Paulino do Rego Barros, Jr., a seven-year veteran of the company, is appointed interim Chief Executive Officer.[4]

Its chief executive office stepped down on September 26, but is scheduled appearance to testify before Congress in early October.[5]

2 October

Equifax releases information from a report by forensic computer security company Mandiant which identified an additional 2.5 million people whose information was stolen. [4]

3 October

Former Equifax CEO Richard Smith testifies before the House Digital Commerce and Consumer Protection subcommittee in which Smith says "mistakes were made." [4]

12 October

Equifax Inc. took part of its website offline Thursday after code on the site redirected users to a malicious URL urging them to download malware.[6]

2018

14 March

Jun Ying, who was to become the company's next chief information officer, was indicted for using confidential information to exercise his vested Equifax stock options and then sell the shares before the company publicly reported a breach. [6]

2019

12 May

Equifax revealed in its earnings release that the incident has cost about $1.4 billion plus legal fees.[6]

RSA Security Hack Timeline

2011

3 March

Establishing the beachhead: RSA analysts eventually traced the origin of the breach to a single malicious file that they believed had landed on an RSA employee's PC. A staffer in Australia had received an email with the subject line "2011 Recruitment plan" and an Excel spreadsheet attached to it. He'd opened it. Inside the file was a script that exploited a zero-day vulnerability—a secret, unpatched security flaw—in Adobe Flash, planting a common piece of malicious software called Poison Ivy on the victim's machine.[1]

8 March

First Indication something was amiss. The admin had noticed that one user had accessed a server from a PC that the user didn't typically work on, and that the permissions setting on the account seemed unusual.[1]

16 March

RSA's executives debated how to go public. One person in legal suggested they didn't actually need to tell their customers, Sam Curry remembers Coviello slammed a fist on the table: They would not only admit to the breach, he insisted, but get on the phone with every single customer to discuss how those companies could protect themselves. As the recovery effort got under way, one executive suggested they call it Project Phoenix. Coviello immediately nixed the name. "Bullshit," he remembers saying. "We're not rising from the ashes. We're going to call this project Apollo 13. We're going to land the ship without injury." [1]

17 March

RSA (EMC) files form 8-K, a report of unscheduled material events or corporate changes at a company that could be of importance to the shareholders or the Securities and Exchange Commission (SEC).[2]

18 March

Coviello published an open letter to RSA's customers on the company's website. "Recently, our security systems identified an extremely sophisticated cyberattack in progress," the letter read. "While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a

current two-factor authentication implementation as part of a broader attack," the letter continued—somewhat downplaying the crisis. [1]

25 May

Breach goes public. A post appeared on the influential tech blogger Robert X. Cringely's website, titled "InsecureID: No More Secrets?" [1]

27 May

Reuters revealed thatLockheed Martin had been hacked using the stolen tokens. [1]

June

In another open letter to customers, RSA's Art Coviello admitted, "We were able to confirm that information taken from RSA in March had been used as an element of an attempted broader attack on Lockheed Martin, a major US government defense contractor." [1]

In the second quarter earnings call, EMC reported that their internal incident response cost was $66 million.[3]

2013

February

The New York Times and the security firm Mandiant attribute the attacks to a Chinese state hacker group that named APT1, People's Liberation Army Unit 61398. Among its dozens of targets over the previous five years: the governments of the United States, Canada, South Korea, Taiwan, Vietnam; and the United Nations—and RSA.[1]

Encryption Timeline

This is a summary of “A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY)” by the Thales Group supplemented by other bits and pieces.

600 BC

- The Spartans used a device called a scytale to code plain text into encrypted messages.

60 BC

- The Romans used a simple substitution cipher where they encoded messages by shifting the letter by some agreed upon number

1553

- Giovan Battista Bellaso invents the first encryption key; a shared secret phrase the recipient needs to decode the message

1917

- Edward Hebern (American) invented an electro-mechanical machine in which the key was embedded in a rotating disc.

1918

- Arthur Scherbius (German) invented the Enigma machine using more than one rotor.

Early 1970s

- IBM invented a block cypher. Instead of using multiple letters as the enigma rotors did, the key is an entire block of text.

1976

- Whitfield Diffie and Martin Hellman published research on what would be defined as the Diffie-Hellman key exchange, the beginnings of asymmetric encryption.

1977

- Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) create the first working algorithm of the Diffie-Hellman key exchange.

1986-1987

- Neil Koblitz and Victor Miller invent elliptic curve cryptography to use much smaller keys (160) compared to RSA Algorithm (1024).

1997

- Researchers break the Data Encryption Standard (DES).

2000

- The Advanced Encryption Standard (AES) replaced DES as the standard by being faster and having the ability to use much longer keys.

Colonial Pipeline Timeline

April 2019

First evidence of Darkside tools being tested on the Internet.

November 2020

First instances of the Darkside service being used.

29 April 2021

- Darkside Hackers gain entry into the networks of Colonial Pipeline through a virtual private network account.

6 May 2021

- Darkside Hackers execute ransomware campaign by stealing 100 gigabytes of data before locking computers with ransomware and demanding payment.

7 May 2021

- Colonial Pipeline notifies The FBI of a network disruption.
- Colonial Pipeline shutdown their IT systems and temporarily paused production on a majority of their pipelines.
- Colonial Pipeline paid nearly $5 million to Russian hackers.

8 May 2021

- Colonial Pipeline issues statement on attack stating they have been victims of ransomware and have engaged a third-party cybersecurity firm and alerted law enforcement.
- Colonial Pipeline, unnamed U.S. companies and several U.S. government organizations (including the White House, the FBI, CISA and NSA) shut off key servers operated by the hackers. The steps stopped the flow of stolen Colonial Pipeline data from the United States to alleged hacker locations in Russia.
- Elliptic, a computer security company specializing in cryptocurrency, said that it had identified the Bitcoin wallet used by DarkSide to collect the Colonial Pipeline ransom payment.

9 May 2021

- Colonial Pipeline issued a second statement giving an update of their investigation into the attack and the status of their pipeline operations.
- Joe Biden, the U.S. president, declared a state of emergency and removed restrictions concerning fuel transportation by road.

10 May 2021

- Georgia Governor Brian Kemp declared a state of emergency and temporarily waived collection of the state's taxes on diesel and gasoline.
- President Biden said that the hackers operate out of Russia.
- The FBI confirmed that DarkSide ransomware is responsible for the compromise of the Colonial Pipeline networks.
- Colonial Pipeline opens Line 4 (which runs from Greensboro, N.C., to Woodbine, Md.) under manual control for a limited period of time while existing inventory is available.

11 May 2021

- The CSIA and FBI issued a cybersecurity advisory that described DarkSide ransomware and associated risk mitigation strategies.
- Colonial Pipeline described alternative fuel shipping strategies that are now in place amid the effort to safely restore the pipeline.

12 May 2021

- Colonial Pipeline managed to resume pipeline service (5:00 p.m. ET) though it will take a few days for the supply chain to return to normal performance.
- Panic Buying: More than 1,000 fuel stations have run out of gasoline amid "panic buying" in the Southeastern United States.

14 May 2021

- DarkSide announced that it is shutting down because of unspecified "pressure" from the United States.

15 May 2021

- The pipeline operations were fully restarted
- The DarkSide RaaS operation was shut down.

18 May 2021

- Despite the authorities best efforts, 10,600 gas stations were still out of fuel.

7 June 2021:

- The U.S. government recovered a "majority" of the millions of dollars paid in ransom to hackers behind the Colonial Pipeline cyberattack.

21 Jul 2021

- A new group called BlackMatter emerged seeking access to big game ransomware targets with annual revenues above $100 million in the US, Canada, Australia, and the UK. CrowdStrike reverse-engineered the DarkSide and BlackMatter Windows variants and saw sufficient overlaps to believe that BlackMatter is simply DarkSide in a new guise.

9 May 2022:

- The Department of Transportation is seeking to levy nearly $1 million in fines against Colonial Pipeline for a series of safety violations. The violations allegedly contributed to the pipeline's decision to temporarily shut down gas operations in the wake of the May 2021 DarkSide ransomware attack

Chaos Engineering Timeline

2006

- Google's DiRT (Disaster Recovery Testing) program was founded by site reliability engineers (SREs) to intentionally instigate failures in critical technology systems and business processes in order to expose unaccounted for risks.

2008

- Netflix made a very public display of moving from the datacenter to the cloud.
- In August, they reacted to a major database corruption event in the datacenter which left Netflix unable to ship DVDs for three days.
- Christmas Eve. AWS suffered a rolling outage of elastic load balancers (ELBs) across regions. Since Netflix's control plane ran on AWS, customers were not able to choose videos and start streaming them.

2010

- The Netflix Engineering Tools team created Chaos Monkey in response to Netflix's move from physical infrastructure to cloud infrastructure provided by Amazon Web Services, and the need to be sure that a loss of an Amazon instance wouldn't affect the Netflix streaming experience.

2011

- The Simian Army added additional failure injection modes on top of Chaos Monkey that would allow testing of a more complete suite of failure states, and thus build resilience to those as well.

2012

- Netflix shared the source code for Chaos Monkey on Github.

2013

- Capital One starts Chaos Engineering with something called "Blind Resiliency Testing."

2014

- Netflix decided they would create a new role: the Chaos Engineer.
- In October, Netflix announced Failure Injection Testing (FIT), a new tool that built on the concepts of the Simian Army, but gave developers more granular control over the "blast radius" of their failure injection.

2015:

- Netflix established a Chaos Engineering Team
- Casey Rosenthal created a community of practice and organized "Chaos Community Day" in the Autumn held in Uber's office in San Francisco: Netflix, Google, Amazon, Microsoft, Facebook, DropBox, WalmartLabs, Yahoo!, LinkedIn, Uber, UCSC, Visa, AT&T, NewRelic, HashiCorp, PagerDuty, and Basho.

2017

- Linked-In began its Chaos Engineering program with Project Waterbear.

2018

- Gremlin launches Chaos Conf, the first large-scale conference dedicated to Chaos Engineering. In just two years, the number of attendees would grow by nearly 10x and include experts from software, retail, finance, delivery, and many other industries.
- Slack experiments with it's Disasterpiece Theater with more than twenty exercises

2020

- AWS adds Chaos Engineering to the reliability pillar of the AWS Well-Architected Framework (WAF).
- AWS announces Fault Injection Simulator (FIS), a fully managed service for natively running chaos experiments on AWS services.

2021

- Gremlin publishes the first ever State of Chaos Engineering report. The report shows how the practice of Chaos Engineering has grown among organizations, key benefits of Chaos Engineering, how often top performing teams run chaos experiments, and more.