Recent High-Profile Cyberattack Examples

Thousands of cyberattacks are perpetrated against enterprise networks every day. Unfortunately, many more of these attacks succeed than are typically reported in the mass media. For organizations that are the victims of such attacks, the financial and reputational damage can be devastating. Some high-profile past breaches that continue to serve as cautionary examples many years later include:

- **Target.** In late 2013, Target discovered that credit card data and debit card data from 40 million of its customers, and the personal information of an additional 70 million of its customers, had been stolen over a period of about 19 days, from November 27 to December 15, 2013. The attackers were able to infiltrate Target's point-of-sale (POS) systems by installing malware (believed to be a variant of the ZeuS financial botnet) on an HVAC (heating, ventilation, and air conditioning) contractor's computer systems to harvest credentials for an online portal used by Target's vendors. Target's 2016 annual report disclosed that the total cost of the breach was US$292 million.

- **Home Depot.** In September 2014, Home Depot suffered a data breach that went unnoticed for about five months. As with the Target data breach, the attackers used a vendor's credentials and exploited a *zero-day threat*, based on a Windows vulnerability, to gain access to Home Depot's network. Memory scraping malware was then installed on more than 7,500 self-service POS terminals to collect 56 million customer credit card numbers throughout the United States and Canada. Home Depot's 2016 annual report disclosed that the total cost of the breach was US$298 million.

- **Anthem.** In February 2015, Anthem disclosed that its servers had been breached and *personally identifiable information* (PII) including names, Social Security numbers, birthdates, addresses, and income information for about 80 million customers had been stolen. The breach occurred on December 10, 2014, when attackers compromised an Anthem database by using a database administrator's credentials. The breach wasn't found until January 27, 2015, when the database administrator discovered a questionable query being run with his credentials. The total cost of the breach is expected to reach US$31 billion.

Several other recent examples of attacks and breaches include:

- **Marriott.** In November 2018, Marriott reported a data breach potentially involving the credit card information, passport numbers, and other personal data of up to 500 million hotel guests of more than 6,700 properties in its Starwood hotel brands (W Hotels, St. Regis, Sheraton, Westin, Element, Aloft, The Luxury Collection, Le Méridien, and Four Points) over a four-year period from 2014 to 2018. The sensitive nature of the personal data – which included mailing addresses, phone numbers, email addresses, dates of birth, gender, reservation dates, and arrival and departure dates/times – opened the door to a broad range of potential criminal activities beyond credit card fraud and identity theft.

- **Quest Diagnostics.** In May 2019, Quest Diagnostics was notified by one of its billing collections service providers, American Medical Collection Agency (AMCA), that an unauthorized user had potentially accessed more than 12 million patient records including individual patient records, financial data, Social Security numbers, and other medical information.
- **City of Baltimore.** The U.S. city of Baltimore, Maryland, was hit by a ransomware attack in May 2019, demanding payment of $72,000 in bitcoin. Although the city appropriately refused to pay the ransom, they have budgeted $18.2 million to remediate the damage associated with the attack. Baltimore is just one example: 82 U.S. cities and municipalities were hit by ransomware attacks in 2019.
- **Capital One.** In July 2019, Capital One announced a data breach affecting more than 100 million individual customers in the U.S. and Canada, which resulted from an individual exploiting a configuration vulnerability. Although the breach did not compromise credit card numbers or account login credentials, it exposed PII and other sensitive information including names, addresses, phone numbers, email addresses, dates of birth, some Social Security numbers, self-reported incomes, credit scores, credit limits and balances, payment history, and transaction data.
- **Gekko Group.** In November 2019, France-based Gekko Group, a subsidiary of Accor Hotels, suffered a data breach in a database containing over 1 terabyte of data. The breach potentially exposed the customer information of Gekko Group brands (600,000 hotels worldwide), their clients, and connected external websites and platforms (such as Booking.com), including PII, hotel and transport reservations, and credit card information.
- **SolarWinds.** In December 2020, the cybersecurity firm FireEye and the U.S. Treasury Department both reported attacks involving malware in a software update to their SolarWinds Orion Network Management System perpetrated by the APT29 (Cozy Bear/Russian SVR) threat group. This attack is one of the most damaging supply chain attacks in history, potentially impacting more than 300,000 SolarWinds customers, including the U.S. federal government and 425 of the Fortune 500 companies.
- **Colonial Pipeline.** In May 2021, the Colonial Pipeline Company – which operates one of the largest fuel pipelines in the U.S. – was hit by the DarkSide threat actor group with a ransomware-as-a-service (RaaS) attack. Although the company acted quickly to shut down its network systems and paid the $4.4 million ransom, operations were not fully restored for six days, which caused major fuel shortages and other supply chain issues along the U.S. eastern seaboard. Additionally, the personal information – including the health insurance, Social Security, driver's license, and military identification numbers – of nearly 6,000 individuals was compromised.
- **JBS S.A.** In May 2021, Brazil-based JBS S.A. – the largest producer of beef, chicken, and pork worldwide – was hit by a ransomware attack attributed to the REvil threat actor group. Although the company paid the $11 million ransom, its U.S. and Australia beef processing operations were shut down for a week.
- **Government of Ukraine.** In January 2022, several Ukrainian government websites including the ministry of foreign affairs and the education ministry were hacked by suspected Russian attackers. Threatening messages were left on the websites during a period of heightened tensions between the governments of Ukraine and Russia.

Key Terms

A *zero-day threat* is the window of vulnerability that exists from the time a new (unknown) threat is released until security vendors release a signature file or security patch for the threat.

Personally identifiable information (PII) is defined by the U.S. National Institute of Standards and Technology (NIST) as “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity … and (2) any other information that is linked or linkable to an individual….” Examples of PII include:

- **Name** (such as full name, maiden name, mother’s maiden name, or alias)
- **Personal identification number** (such as Social Security number, passport number, driver’s license number, financial account number, or credit card number)
- **Address information** (such as street address or email address)
- **Telephone numbers** (such as mobile, business, and personal numbers)
- **Personal characteristics** (such as photographs, X-rays, fingerprints, and biometric data)
- **Information about personally owned property** (such as vehicle registration number and title information)
- **Information that is linked or linkable to any of the above** (such as birthdate, birthplace, religion, and employment, medical, education, and financial records)

Important lessons to be learned from these attacks include:

- A “low and slow” cyberattack can go undetected for weeks, months, or even years.
- An attacker doesn’t necessarily need to run a sophisticated exploit against a hardened system to infiltrate a target organization. Often, an attacker will target an auxiliary system or other vulnerable endpoint, then pivot the attack toward the primary target.
- Unpatched vulnerabilities are a commonly exploited attack vector.
- The direct and indirect financial costs of a breach can be devastating for both the targeted organization and individuals whose personal and financial information is stolen or compromised.