World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

The crowdstrike incident: Analysis and unveiling the intricacies of modern cybersecurity breaches

Iqra Naseer *

Cognizant Technology Solutions Doha Qatar.

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(01), 728–733

Publication history: Received on 23 August 2024; revised on 05 October 2024; accepted on 07 October 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.1.0473

Abstract

The CrowdStrike incident is also helpful in evaluating the understanding of who is defending from cyber-attacks and what methods are being used. This pen works on the deep understanding of how this attack was performed, how the adversary detailed it step by step, what TTPs were used, and what an APT is at all. Deconstructing the CrowdStrike incident, this research shows how intruders implant themselves in the enterprise network and how this intrusion can be repelled or at least made less impactful towards preemptive security measures, real time threat intelligence, and effective response actions. This study also looks into how machine learning and AI based tools respond to and prevent cyber-attacks. Conclusions indicate progress and attacks in cyberspace, and the need for new approaches in protection of systems from such incidents.

Keywords: CrowdStrike Incident; Cybersecurity breaches; Advanced persistent threats (APT); Threat intelligence; Vulnerability exploitation; Data breaches

1. Introduction

CrowdStrike is a well-known cybersecurity technology company that works in endpoint security, threat intelligence, and incident response[1]. CrowdStrike is one of the fastest growing cyber security organizations since its establishment in 2011, and the CrowdStrike Falcon platform for endpoint detection and response (EDR) is currently a leading product. The company provides an artificial intelligence, machine learning and behavioral analytics approach to detect and respond to advanced cyber threats in real time. The news helped further cement CrowdStrike's reputation as one of the go-to companies for investigating and responding to major cybersecurity incidents, due largely in part to its work uncovering the 2016 hack on the Democratic National Committee (DNC). It came after a published report blamed Russian intelligence-affiliated hacking groups — known as APTs, or Advanced Persistent Threats. CrowdStrike, because of their capability to do attribution this attack and then reverse that malicious act led them to be widely known. Aside from isolated events, the company empowers enterprises to protect against myriad cyber threats like ransomware, identity threat detection and malware -- even protect against nation-state espionage. Its services are utilized by governments, Fortune 500 and global organizations[2]. An examination of cybersecurity breaches has been more key in a digital age where hackers can launch sophisticated attacks that results in businesses, governments, and other organizations grinding to a halt or services suspended as well as sensitive data exposed. In an organization, a cybersecurity breach could also mean a huge financial lose, reputational damage or even worst legal consequences. Moreover, traditional defense mechanisms fail under increasingly crafted and sophisticated cyber attacks proving the significance to move forward with more innovative and advanced security technologies, demanding continuous research in this area. Researchers and cybersecurity professionals can learn which new attack vectors, threat actor tactics, techniques and procedures (TTPs) or vulnerabilities not previously identified in their environment to watch for after studying incidents such as the CrowdStrike breach or other significant cyber intrusions. With this knowledge,

* Corresponding author: Iqra Naseer

organizations can enhance their security systems, take proper decisions on preventive action against potential threats and also develop better strategies for responding to threats. It also assists in making everyone understand why and what it is necessary to implement the changes in security activities and gives implications on the progression of daily threats that organizations experience[3]. The importance of examining these breaches is … also associated with the notion of safeguarding national security considering how cyber attacks can be government-sponsored or have consequences for key infrastructures. Given that cyber warfare is becoming a crucial component of international politics, comprehension of the complexity of cyber attacks is imperative in fashioning efficient defense systems against all attacks on both private establishments and government institutions. The positive impact of the aforementioned purpose on the activities of the organization consists in the presentation of the CrowdStrike incident and the potential consequences of modern unscrupulous attacks on related organizations and borderlines. Drawing on this case, target enumerates core weaknesses and attacking strategies that are prone to exploitation by the adversaries seeking to accomplish modern cybersecurity, defense, counter-measures, target[4]. To facilitate an optimized evaluation of this paper, it has been structured into various components. In the first segment, introduction, the reader gets to know why cybersecurity breaches are a major concern today as well as the company CrowdStrike and other companies' efforts in dealing with such. The second section presents a case study on blanket v Crowdstrike and proceeds to the research questions regarding the Analysis of the ideologies and techniques used in the assault. Section three extends the discussion of such breaches on the security of the cybersecurity measures adopted by such organizations, whereas the last section seeks to wind up the activities related to the construction of this paper and outlines ways of improving cyber warfare strategy. In summary, each section follows from the logically preceding one in order to systematically justify the relevance of analysis of complaints concerning cybersecurity breaches about the current state of affairs in the digital sphere[5].

2. Background on CrowdStrike Incident

Table 1 Aspect, Details, Timeline, and Key Players Involved in the CrowdStrike Incident across Multiple Dimensions

Aspect	Details	Timeline	Key Players Involved
Incident Overview	Data breach of the DNC by Russian-backed hacking groups, stealing sensitive emails and documents.	April 2016 – July 2016	Adversaries: APT28 (Fancy Bear), APT29 (Cozy Bear)
Discovery of Breach	DNC hired CrowdStrike to investigate suspicious activity, who confirmed the breach by Russian APTs.	April - May 2016	DNC (Democratic National Committee), CrowdStrike (cybersecurity firm)
Breach Publicly Disclosed	CrowdStrike publicly announced the breach, attributing it to Russian intelligence groups.	June 2016	Russian intelligence agencies (GRU, FSB), WikiLeaks (published stolen emails)
Government Response	FBI and other agencies launched investigations; U.S. imposed sanctions on Russia.	Post-July 2016	U.S. intelligence community, FBI, U.S. Congress

The CrowdStrike incident describes the company's inquiry of the major hacks of the Democratic National Committee (DNC) in 2016. CrowdStrike was under contract for investigating abnormal behavior on DNC's system against which hackers had gone out onto the system and accessed emails and other confidential information. This breach sent law enforcement officials on fishing expeditions as thousands of emails were turned in to be made public towards the controversial campaigns for the elections in America. They measured one of the indications in that APT that the Russian sponsored groups are attacking, that it was two groups namely Fancy Bear APT28 and Cozy Bear APT29. The people in these clusters were associated with the Russian General Staff and the FSB. Last page of DNC cyber security documents including Cyber threat intelligence alignment DNC: The fire mute of key incidents 2016: Timeline of events. As early as 2016, constructive affairs of the DNC observed unexplainable events on the networks[6]. By these times since beginning 2016 or thereabouts DNC secured CrowdStrike to investigate the hack. Management of CrowdStrike received feedback from the hacked organisation validated that indeed a breach occurred. The intrusion was made public in the month of June 2016 as the perpetrators of the said attacks were attributed to the Russian.Following the disclosure, stolen DNC emails were released through platforms like WikiLeaks in July 2016, causing widespread media coverage and political fallout. The key adversaries in this incident were the Russian hacking groups Fancy Bear and Cozy Bear. Their attacks were part of a larger effort to influence the U.S. election by targeting political entities. The impacted organization was primarily the DNC, but the breach also affected other individuals and entities associated with the election campaign.

The U.S. intelligence community later confirmed CrowdStrike's findings, asserting that the breach was part of a Russian effort to interfere in the 2016 election[7]. The breach triggered significant public and governmental reactions. The U.S. government imposed sanctions on Russia, and several investigations, including by the FBI and the Mueller investigation, were launched to examine the incident's broader implications. The breach raised awareness of the growing threat of cyberattacks against democratic institutions worldwide.

3. Methodology

The methodology for researching the incident includes in-depth review of the mechanisms behind the attack, which tools and techniques the attacker employs, and what response strategies CrowdStrike utilizes. Basic data sources used for this kind of analysis include publicly published reports and technical documentation. The core of understanding the attack comes from CrowdStrike's internal reports, blog posts, and whitepapers describing the actions of APT28 (Fancy Bear) and APT29 (Cozy Bear). Secondary sources include government reports, through official channels from agencies such as the FBI or the Department of Homeland Security, to support CrowdStrike's findings[8]. These reports provide insightful information regarding the incident nature of the attack and possible political implications. Besides official reports, third-party cybersecurity analyses from companies FireEye and Symantec were consulted to corroborate CrowdStrike's methods, timelines, and attributions. The New York Times, Washington Post, among other more credible media sources, provided more information relative to how public and political reaction was panicking over the hack. Advanced Persistent Threats and state-sponsored cyberattacks' academic literature has been framed in the research work along with theoretical bodies for deepened analysis. Several analytical tools have been applied to unravel the CrowdStrike hack. First, the attack vector analysis conducted based on spear-phishing and network vulnerability exploits has been done to analyze how the hackers entered the network of the DNC. Second, behavioral analytics have been looked into by analyzing how CrowdStrike utilizes machine learning and artificial intelligence in detecting anomalous behavior within the network in real-time. This assessment demonstrates how AI-based technologies are increasingly becoming standard in detecting advanced intrusions. The other category of analysis included threat attribution models with a focus on backtracking the attack to Russian state-sponsored groups APT28 and APT29. In this case, traces exist in the form of malware signatures, IP tracing, and behavior patterns known by a certain group of attackers. In addition, a study of other related high-profile breaches was done to analyze common vulnerabilities and patterns of a cyber-attack and further solidify the study of the CrowdStrike case. This research study suffers from a number of limitations. The first limitation of this study is that it is based on secondary sources in the form of reports available in the public domain and media reports[9]. This significantly hampers the scope to gain potentially more detailed, classified information that could have arisen as a result of internal investigations, which consequently reduces the scope of the technical analysis depth. Much of the process involved in attribution, widely accepted, is inherently a complex process, with inherent error potential. Frequently, attackers utilize sophisticated obfuscation that may mislead the investigators in the area of cybersecurity. Further, the tools and technologies used are also those that should be relevant for the year during which the attack happened. Cybersecurity is an ever-evolving area, and since the incident, methodologies and tools have kept changing both in terms of attacking and defending systems. Therefore, some analysis would not be as it is currently representing the current state of matters regarding cybersecurity practices, hence an ongoing research and real-time data would be needed to keep up with the proper present state of understanding cybersecurity challenges[10].

4. Analysis of the Breach

Critical insights on the technical vulnerabilities breached through the Democratic National Committee (DNC) hacking reveal in the CrowdStrike investigation. The first critical vulnerability is that the attackers exploited outdated or not appropriately secured email servers. Likely, they utilized spear-phishing emails to unlock compromised credentials in key DNC personnel and members to gain initial access to the system. Once inside the network, attackers relied on weak multi-factor authentication and poor password hygiene to gain elevated privileges and move laterally. One of the primary attack vectors for adversaries was spear-phishing-a technique that enables attackers to send a fraudulent email to a specific user or users of a particular organization to extract credentials. Malicious links or attachments in emails were the entry points used for installing malware in the target machine. Compromise of individual user accounts gave access to the DNC network, from where sensitive information was extracted. Further lateral movement across the network was carried out, sensitive emails and documents on critical servers were obtained. Through the intrusion, the attackers deployed diverse, advanced TTPs. After they had gained access into the network, they used credential dumping tools to gain passwords with elevated privileges. They then installed malware, which included RATs within the system, which maintained persistent access in the system and was able to avoid getting noticed as it allowed the attackers to decrypt large chunks of data undetected. TTPs such as those similar to APTs allow hackers to go unnoticed for months within a network[11]. This breach of the DNC bears a strong resemblance to other state-backed hacks that

have been linked to the cyberattacks against Sony Pictures in 2014 as well as the WannaCry ransomware attack in 2017. These incidents incorporated phishing attacks and malware to infiltrate systems, which then exfiltrated or destroyed sensitive information. Such attacks, like the DNC breach, use persistent access techniques that enable an attacker to take advantage of exploitation opportunities for a long time; however, what was different about the DNC breach was its political significance-it directly affected the U.S. election-herein lies the new dawn of state sponsored cyberattacks on democratic institutions. Cybersecurity Breaches have rapidly increased in recent years as attackers use the latest technologies to execute attacks. Figure 1 shows some of the top Cybersecurity Breaches:

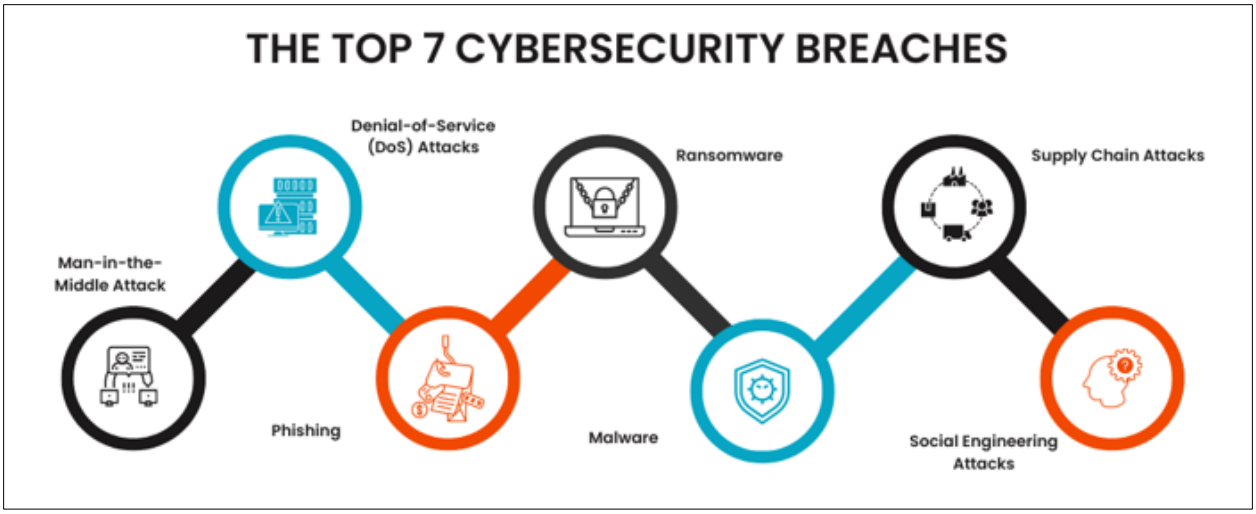

Figure 1 Different Types of Cyber Security Breaches

5. Impact and Emerging Trends in Cybersecurity Breaches

The CrowdStrike incident influenced modern cybersecurity strategies, most particularly in regard to how organizations approach threat detection and response. The state-sponsored actors' breach of the Democratic National Committee highlighted a need for more sophisticated methods of detection and much better security measures. Organizations began focusing more on proactive defense strategies, away from the traditional perimeter-based protection to continuous monitoring of the internal systems. This incident further established the focus on MFA, regular patching, and strict password hygiene, among others, which would reduce vulnerabilities[12]. The change in cybersecurity policies after the incident was to move towards real-time detection and response of threats. Using behavioural analytics and machine learning capabilities of CrowdStrike in identifying anomalous activity on the DNC network became the model of modern-day cybersecurity. As can be recognized, there is a significant utilization of AI-driven monitoring tools that are implemented to identify abnormal patterns in user behaviors within an organization and flag threats before their normal eventualities become effective. There was increased adoption of incident response protocols by organizations focused on early containment, mitigation, and post-breach analysis. Of course, it also gave testament to the need for threat intelligence to defend against APTs. Their TTPs will be dissected for the incorporation of an intelligence framework that forms predictive intent and prevents attacks from occurring. In doing so, it galvanizes a more dynamic and responsive cybersecurity strategy: such organizations can't just sit back and wait to be breached but rather are proactive in preventing it. Cybersecurity breaches related to CrowdStrike have definitely been rather sophisticated since the incident. There has been a heightened strategic targeting of critical infrastructure and high-profile organizations by state-sponsored cyberattacks and supply chain attacks[13]. In this context, AI and machine learning have expanded significantly in the scope of cybersecurity design. This is so because those technologies can identify sophisticated threats that evade traditional security controls and respond to them accordingly. Notably, the attack surface increased with reliance on ERP and CRM systems. With companies relying increasingly on such systems, attackers have been taking advantage of those weaknesses to hack in and siphon off highly valuable data, and there is a growing call for very tight cybersecurity tailored for these platforms. Figure 2 represents the risk analyses, security protocols, plans for responding to incidents, tracking, and staff training in cybersecurity strategy essentials:

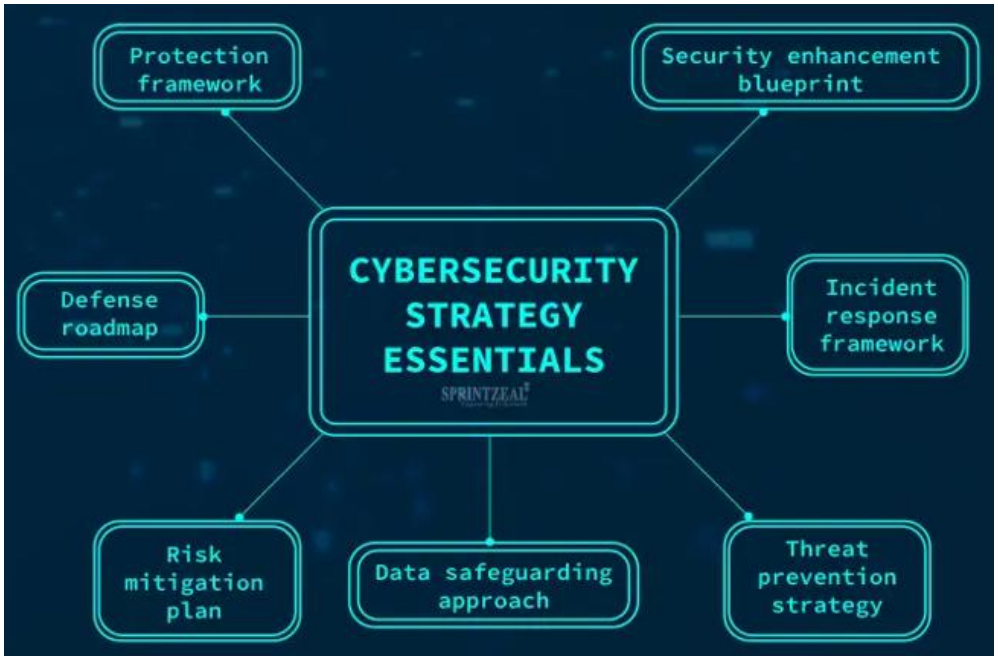

Figure 2 The Essentials in Cybersecurity Strategy

5.1. Lessons Learned from the Incident

The CrowdStrike incident is important for organizations with the intent of improving their cybersecurity posture to draw critical lessons on how to do it. First, there is the appreciation that there is an urgent need for organizations to move from a reactive security posture toward a proactive security posture. Of course, the DNC breach underlined the case for continuous monitoring of networks by well-equipped state-of-the-art tools in the form of AI and machine learning. This would eliminate the chance of long intrusions because anomalies would appear early. In this regard, the organizations must give first priority to ensuring multi-factor authentication, regular patching, and robust access controls where credential theft and lateral movement of networks could be reduced[14]. Regular employee training about phishing and social engineering attacks is essential to prevent initial compromise. In expectation of similar threats, companies should invest in threat intelligence platforms, which track adversaries' TTPs and therefore give businesses the anticipation of new attack vectors and improvements in incident response strategy. Companies should also continue to perform penetration testing and vulnerability assessments in a way that will identify weaknesses before they are exploited. Only through the application of these practices will organizations be able to build the necessary defenses in cybersecurity - ones that will be able and capable of resisting even the most sophisticated cyber threats[15].

6. Conclusion

In conclusion, Incident like CrowdStrike drew attention to vulnerabilities through sophisticated state-sponsored cyber attacks which need real-time threat detection, stronger authentication mechanisms, and proactive cybersecurity. Key takeaways are, the AI and threat intelligence play a critical role in modern defense. Future research may focus more on improving automated detection systems, getting an understanding of emerging attack vectors, and security for ERP/CRM systems. Complex breaches must be controlled by organizations applying a proactive, intelligence-led approach with constant assessment and evolution of defense strategies to stay ahead of emerging cyber threats.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] J. Ahmad *et al.*, "Machine learning and blockchain technologies for cybersecurity in connected vehicles," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery,* vol. 14, no. 1, p. e1515, 2024.

[2] N. G. Camacho, "The Role of AI in Cybersecurity: Addressing Threats in the Digital Age," *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023,* vol. 3, no. 1, pp. 143-154, 2024.

[3] N. Leonov, M. Buinevich, and A. Chechulin, "Top-20 Weakest from Cybersecurity Elements of the Industry Production and Technology Platform 4.0 Information Systems," in *2024 International Russian Smart Industry Conference (SmartIndustryCon)*, 2024: IEEE, pp. 668-675.

[4] R. K. Ray, F. R. Chowdhury, and M. R. Hasan, "Blockchain Applications in Retail Cybersecurity: Enhancing Supply Chain Integrity, Secure Transactions, and Data Protection," *Journal of Business and Management Studies,* vol. 6, no. 1, pp. 206-214, 2024.

[5] P. O. Shoetan, O. O. Amoo, E. S. Okafor, and O. L. Olorunfemi, "Synthesizing AI'S impact on cybersecurity in telecommunications: a conceptual framework," *Computer Science & IT Research Journal,* vol. 5, no. 3, pp. 594-605, 2024.

[6] E. Tariq *et al.*, "How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks," *International Journal of Data and Network Science,* vol. 8, no. 1, pp. 69-76, 2024.

[7] N. Choucri, S. Madnick, and J. Ferwerda, "Institutions for cyber security: International responses and global imperatives," *Information Technology for Development,* vol. 20, no. 2, pp. 96-121, 2014.

[8] R. D. Edelman, *Rethinking Cyber Warfare: The International Relations of Digital Disruption*. Oxford University Press, 2024.

[9] L. Ghafoor and M. Khan, "A Threat Detection Model of Cyber-security through Artificial Intelligence."

[10] H. Luiijf, K. Besseling, M. Spoelstra, and P. De Graaf, "Ten national cyber security strategies: A comparison," in *Critical Information Infrastructure Security: 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8-9, 2011, Revised Selected Papers 6*, 2013: Springer, pp. 1-17.

[11] G. N. Reddy and G. Reddy, "A study of cyber security challenges and its emerging trends on latest technologies," *arXiv preprint arXiv:1402.1842,* 2014.

[12] D. Schatz, R. Bashroush, and J. Wall, "Towards a more representative definition of cyber security," *Journal of Digital Forensics, Security and Law,* vol. 12, no. 2, p. 8, 2017.

[13] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE communications surveys & tutorials,* vol. 14, no. 4, pp. 998-1010, 2012.

[14] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access,* vol. 8, pp. 151019-151064, 2020.

[15] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems,* vol. 99, pp. 45-56, 2018.