The Cybersecurity Threat Landscape Group Assignment

CMIT 495: Current Trends and Projects in Computer Networks and Security

Professor Dodoo

By:

Christopher Luntz, Michael Lambinicio, Jorge Jimenez, Carlos Malave

Introduction

One of the most sophisticated and dangerous forms of cyber threats that organizations and governments face today has a name that sounds like something out of a sci-fi movie: Advanced Persistent Threats. Unlike some cybercriminals who launch opportunistic attacks at just about anyone, APTs are typically state-sponsored or highly organized, and extremely well-funded groups that employ long-term, stealthy tactics to infiltrate networks and exfiltrate sensitive data that one would think requires half a dozen secret agents to obtain (FireEye, 2014). The threat landscape has shifted dramatically in recent years, with APTs increasingly targeting high-value, hard-to-obtain secrets that reveal what our leaders are up to, inform the military about ongoing situations in the field, and are vital to the operation of our critical infrastructure (ENISA, 2023). This analysis focuses on APT28, a threat actor that FireEye has profiled extensively (2014) as a cyber espionage operation with Russian links.

Active since at least 2007, APT28 functions like a state-sponsored advanced persistent threat, targeting national security interests using highly sophisticated tools and techniques (FireEye, 2014, p. 3). This includes spear-phishing lures designed for victims' roles, modular malware such as CHOPSTICK and SOURFACE, and operational patterns such as Russian-language code. We'll also address the ethical aspects of APT defense, questioning whether breaches indicate systemic failures in protecting the confidentiality, integrity, and availability (C-I-A) of critical data, as well as why conventional security tools struggle against such adversaries, investigating how modern innovations like machine learning (ML) and data analytics could reduce future APT attacks. The group's cyber campaigns have aimed at government, military, and security entities throughout Eastern Europe, Nato and the Caucasus, particularly following the 2008 Russo-Georgian War, concentrating on intelligence gathering that supports the reconnaissance mission of any nation's cyber warfare efforts instead of seeking significant profits from online heists (FireEye, 2014, p. 3).

Part 1: Threat Landscape Analysis

The cybersecurity threat landscape evolves rapidly and relentlessly. Using the most current threat reports from government sources, respected cyber security news sources, and reports from major IT companies, we will evaluate current threats; how threats have evolved over the past year; current Tactics, Techniques, Procedures (TTPs); as well as who the perpetrators are and by what methods and means they are accomplishing their goals. Our current threat landscape includes every known vector of attack, and new attack methods are being developed daily. Physical Security continues to be a high concern for all businesses as well as private residences. According to the K7 Security blog, the cyber world is seeing an exponential increase in Advanced Persistent Threat (APT) attacks, Artificial Intelligence (AI) -driven attacks, and the newer Ransomware-as-a-Service (RaaS) platform attacks. Although it's not a traditional cyber security threat, there is a rise in Disinformation campaigns, via social media platforms, to create division and destabilization in our society and political infrastructure. Disinformation attacks have been attributed to APT28. Here are the largest current threats:

- Vishing & Social Engineering – Voice phishing attacks are up 442% since the first quarter of 2024 (go.crowdstrike.com, 2025). The intent is to use social engineering to gain access to systems and networks.

- Information Stealing Malware & Credential Theft – In 2024, over 3.2 billion credentials were compromised. Information-stealing malware was responsible for approximately 2.1 billion of those thefts (blog.k7computing.com, 2025) (flashpoint.io, 2025). The intent is to acquire a legitimate means of accessing a system so as to accomplish the goal without detection or to initiate ransomware.

- Ransomware & RaaS – Flashpoint.io (2025) reports that ransomware attacks rose by 10% across all sectors in 2024. Which doesn't sound bad, however, a report published by the FBI's Internet Crime Complain Center details that more than 850,00 complaints total over $16 billion in damages. In that report, it is noted that the top 3 cybercrimes were phishing, extortion, and personal data breaches: accomplished by the aforementioned top 2 threats and Ransomware / RaaS. The primary intent of those conducting this attack is to receive payment that cannot be traced.

- AI-powered Social Engineering & Deepfakes – AI itself is not the problem, but it is being increasingly utilized for nefarious purposes, especially cyber–crime. “Since the release of commercial generative AI tools, we’ve seen phishing attacks surge by 1,265 percent” (Flashpoint.io, 2025). The Flashpoint.io report notes that AI makes it easy for novice computer users to create advanced deceptions.

- APTs (State-sponsored) – The CrowdStrike Global Threat Report details that APT groups, specifically those sponsored by China are on the rise. China-linked group activity increased by 150%, with a 200-300% rise in targeting of media, manufacturing, financial services, and industry/engineering sectors. APT28 attacks have also increased recently (k7computing.com, 2025), but that will be covered later.

- Insider Threat / Misconfiguration – Insider threats and misconfigurations can occur for many reasons and are not always malicious in nature. Sometimes simple negligence or ignorance can create opportunities for nefarious actors to harm. This won’t be discussed further; however, it is worth mentioning as it continues to be a major problem and attack vector. This category should also include things such as shadow IT and rogue access points.

The current threat involving APT28 involves government espionage, vulnerability exploitation, social engineering, and even diplomatic/social event sabotage. In 2024 alone, APT28 has successfully executed phishing attacks against “government and non-government organizations (NGOs) in Europe, the South Caucasus, Central Asia, and North and South America” (thehackernews.com, 2024). The same article cites exploitation of CVE-2023-23397 to take advantage of security flaws in Microsoft Outlook in order to conduct relay attacks and steal hashes. Fancy Bear has also exploited vulnerabilities CVE-2022-38028 in attacks against Ukraine, Western European countries, and North American countries (SOCRadar.io, 2024).

Over the past year, threats in the cyber world have only become more sophisticated. There has been exponential growth with information-stealing malware and credential theft: up 33% from last year (flashpoint.io, 2025). Ransomware and RaaS attacks are rising rapidly as APT and RaaS actors are beginning to collaborate. AI has exponentially increased AI-based phishing, misinformation, disinformation, social engineering attacks, and even AI-based sexual harassment and extortion crimes.

With these threats and the advances over the past year, it's important to identify threat actor types as well as common TTPs they typically use. The term "threat actor" is a generic term for any individual or group that poses a threat to your system, network, or business. It should be noted that intent is not a consideration as to whether someone is a threat. Here is an overview of threat actors with defining characteristics and the TTPs utilized to accomplish their goals. The following information was derived from the 2025 CompTIA Security+ book, written by Mike Chapple and David Seidle, as well as CISA.gov and attack.mitre.org.

Script Kitties / Thrill Seekers

Characteristics: Those motivated primarily by either prestige, excitement, or just the challenge of breaking or bypassing a security system. Although not usually malicious in nature, they still pose a threat to data confidentiality, integrity, and availability. Script Kitties differ from thrill seekers in that their intentions are usually malicious, but they are not cyber criminals due to their negligible abilities and knowledge. The skills of script kitties and thrill seekers usually range from novice to moderate.

TTPs: Use publicly available tools to gain access and execute any actions or goals, such as defacement or taking screenshots to prove presence and exfiltrate when complete. They typically use premade tools such as Metasploit or Kali Linux to conduct activities.

Targets: Ranges from individual home networks to mega corporations. The larger the target, the more prestige and respect they earn.

Hacktivist

Characteristics: Those motivated by ideology; such religious, political, or social causes, as opposed to financial gain or gain in reputation. These actors typically claim righteousness but conduct illegal or disruptive activity to intentionally cause harm for the sake of bringing awareness of what their goal or belief is. Their skills can range from moderately skilled to expert, and the tools leveraged vary from pre-built tools to custom payloads.

TTPs: Hacktivists use simple and advanced tools to deface, steal and leak data, interrupt or shut down services, or to damage the reputation of a company or individual. They use disruptive

and noticeable attacks to bring as much attention as possible to their goal or to simply create chaos and stop operations of the business or activity they disagree with.

Targets: Politicians, government officials, governments, people in positions of authority or power, corporations, other political groups, or any business or person the group deems offensive to their beliefs.

Insider Threats

Characteristics: Those individuals who may or may not intend to cause harm. Harm can arise from individuals who defect, individuals who maliciously plant themselves inside an organization, or from individuals who are just ignorant of policies, procedures, and best practices. There is not typically a skill requirement; however, IT expertise ranges from ignorance and negligence to advanced, with intent ranging from oblivious to malicious.

TTPs: TTPs vary greatly as intent varies between individuals in this category. Intentionally installed backdoors, willful selling of propriety or classified information, an individual that ignorantly plugs a private cell phone into the company network, or the individual that lets someone follow them inside, are all examples of TTPs of insider threats.

Targets: The place of employment for the insider threat is the target.

Organized Crime/Cyber Criminals/ Competitors

Characteristics: These three differ in intent and reasoning, but all have the same motivation - financial gain. These threat actors are willing to do anything to bring financial gain to themselves. Although competitors are unique in their justification or TTPs, the end goal of increasing their own monetary wealth is the same. Skills range from moderately advanced to very advanced.

TTPs: The TTPs of these groups follow the MITRE ATT&CK matrix, moving from reconnaissance to resource development to initial access all the way through to command and control, exfiltration, and impact. Again, the impact, or result, always being an outcome that results in monetary gain. Sometimes that impact is receiving extortion payments or corporate

espionage to steal proprietary information, designs, or data or even just the sabotage or embarrassment of the competitor which results in a loss of revenue.

Targets: Everyone is a target. Anyone that might be manipulated or tricked is a target. For Competitors, their target is always an opposing business or person that stands in the way of profit.

Nation-State Actors/ Advanced Persistent Threats / Terrorist Groups / APT28

Characteristics: Those motivated primarily by either religious, political or national allegiance, seeking geopolitical advantage or some benefit to their group or country. Unlike other threat actors, they most often operate over long periods of time and have very strategic goals. This group is by far the most persistent, well-funded, knowledgeable, and dangerous. Skills range from very advanced to state-of-the-art. Notable groups include APT28 aka Fancy Bear(Russia), APT41 (China), and Charming Kitten (Iran)

TTPs: These threat actors most often use custom tools and attack packages, but may leverage known tools such as Gh0st RAT, Cobalt Strike, and conduct advanced zero-day exploits. These actors' activities expertly span the entire ATT&CK framework. They use sophisticated multi-phase operations to conduct espionage, attack of critical infrastructure, extortion, and psychological operations to accomplish their goals of supply chain compromise, systemic disruption or chaos, disruption or degradation to command-and-control capability, and geopolitical destabilization. Some tactics may be overt, such as political interference, or more covert, such as the creation of fake social media accounts to cause unrest and discord (cisa.gov, 2020).

Targets: Government agencies, military departments, national critical infrastructure, major media outlets, and NGOs. It should be mentioned that although individuals are rarely targeted, these groups use TTPs to conduct psychological operations for the sake of influencing a population to ensure a desired outcome with elections.

Considering the current threat landscape, it is assessed that the vectors and vulnerabilities most likely to be exploited will involve AI, social media, text messaging, and e-mail. Phishing continues to be a top TTP for each threat actor or group. Public-facing web applications and

services are also popular vectors of attack and can be accomplished by exploiting known vulnerabilities or using brute-force attacks. The other two vectors of attack that will be widely exploited are misconfigurations in local and cloud servers, and Application Programming Interface exploitation. Zero-day vulnerabilities and insider threat vectors are almost impossible to eliminate. It should be expected that APT28 will leverage every attack vector available.

Part 2: APT Analysis

APT28 uses a range of cunning and sophisticated techniques to gain initial access to targeted systems, with Spear phishing being its primary method. Spear phishing involves creating highly personalized and seemingly legitimate emails that are sent to specific individuals or organizations. These emails typically contain malicious attachments or links that appear normal and pertinent to the work or interests of the person to whom it was sent. APT28 seems to spend a considerable amount of time and effort to make the lures they use as credible as possible, obviously to increase their chances of success. For example, when targeting specific individuals in the Georgian government, APT28 sent emails written in Georgian that referenced drivers' licenses or other internal IT types of documents that mentioned individuals in the MIA and other specific facilities (FireEye, 2014, pp. 8-9). Once opened, these attachments executed embedded code to download malware such as the SOURFACE downloader onto the victim's system.

APT28 frequently engaged in domain impersonation, registering web domains closely resembling those of trusted organizations. Similarly, the group targeted reporters, such as those at the Caucasus Bureau of Radio Free Europe/Radio Liberty (RFE/RL), which is based in Prague. APT28 sent fake collaboration invitations purportedly from the non-existent department of Reason Magazine (a real magazine) that handles "Caucasian" (i.e., deals with issues in the Caucasus region) matters. APT28 has also used current events as bait for its oars, such as the downing of Malaysia Airlines Flight MH17, to get Eastern European governments to bite (FireEye, 2014, pp. 12-14). To make the last spear phishing operation even more believable to the intended victims, APT28 sent some of its target audience emails that were also sent to non-public defense attachés stationed in London and Ankara (FireEye, 2014, pp. 14-15). Finally, APT28 set up some spoofed domains to attempt to access the network of individuals attending the Farnborough International Airshow (FireEye, 2014, p. 16). A notable central feature of these

lures was the use of weaponized attachments, commonly Microsoft Word or Excel documents, exploiting known software vulnerabilities.

Once APT28 has successfully infiltrated a network, its operations focus on remaining undetected while maintaining a persistent presence. To this end, the group employs all the resources associated with the victim's network, using them to its advantage as much as possible, not to draw attention. Malware implants undetectable by the victim's security operations are a critical backbone of this approach, as is using the victim's infrastructure to the utmost while remaining inside the victim's perimeter undetected. APT28 develops highly specialized malware to achieve these ends, with two of the more notable examples being 'EVILTOSS' and 'CHOPSTICK.' These two modules, especially, give a new meaning to the phrase 'going dark.'

Their primary tool SOURFACE, also known as CORESHELL, is typically employed as the dropper or initial downloader of malware in their Spear phishing campaigns. Its primary job is to make a phone call back home, to a Command and Control (C2) server, and get the real payloads, like EVILTOSS, which they push out to their targets. SOURFACE from 2007 to 2014 looks to have grown in complexity, moving from using hardcoded IP addresses to using domain names and various tricks to avoid detection and analysis (FireEye, 2014, pp. 19-22). EVILTOSS is commonly used to gain deep access to a compromised system. The capabilities of this backdoor are diverse and impressive, showing that it can do almost anything an attacker wants it to do. This includes things such as file system and registry manipulation, network reconnaissance, creating processes, keystroke and logging, credential theft, Shellcode execution, and data exfiltration. The data taken through EVILTOSS is typically sent over SMTP (using the victim's mail servers) or HTTP and is usually encrypted using RSA.

APT28's primary objective, as identified through a decade of targeting patterns and the nature of the information it seeks, is direct support of the Russian government through cyber espionage. The group collects political, military, and security foreign intelligence that it believes informs (and perhaps influences) Russian national security decision-making, threat assessments, and the broader geopolitical strategy of the Kremlin. Its long-term focus suggests an intelligence agenda closely aligned with Russian national priorities. The group's influence stretches well beyond

issues affecting just one region, allowing it to pursue a suite of geopolitical intelligence operations across the world.

It is safe to surmise that APT28 has successfully carried out its cyber espionage objectives. FireEye carried out an extensive analysis of the group and found that it has been operating since at least 2007 and is likely to be even longer. Furthermore, it appears to have a high level of sophistication and consistent effectiveness. Even if we lack definitive proof of the specific data that it has exfiltrated, indicators strongly suggest that APT28 has served its backers well, and that they are pleased with its work. APT28's demonstrated ability to access high-value networks also reflects its operational impact. The group consistently aligns with Russian geopolitical interests, and this consistently reliable alignment convinces us of their espionage successes. It targets the same places that Russian military intelligence wants to penetrate—Georgia, Eastern European countries, NATO members, and countries that host either the OSCE or Russian military assets. Furthermore, APT28 showed no signs of being financially or commercially motivated. This key trait distinguishes state-sponsored espionage from cybercrime and makes APT28 somewhat unique among Advanced Persistent Threats. The group did not operate in the realm of intellectual property theft that is then sold on the black market or in the realm of ransomware. Politically, militarily, and security-wise, APT28 stayed on target.

Part 3: Cybersecurity Tools, Tactics, and Procedures

Defending modern infrastructure requires leveraging layered defenses, incorporating specialized tools, proactive tactics, and standardized procedures. Some current cybersecurity hardware and software tools, tactics, and procedures are described below.

Endpoint Detection and Response (EDR) solutions are sophisticated software agents installed on endpoint devices (laptops, desktops, servers) that perform not only monitoring but also detailed analysis of activities that occur on those devices. Continuous monitoring combined with behavioral analysis of system activity is the core TTP from which EDR solutions operate. These methods allow EDR solutions to detect all manner of unauthorized activity that could indicate a security incident. Again, unauthorized activity in this context could include malicious actions taken by human adversaries, as well as any kind of malware trying to do its thing (Aarness, 2025; Microsoft, 2024).

From a functionality perspective, EDR solutions are in many respects a superset of Security Information and Event Management (SIEM) capabilities. Many existing SIEM solutions will ingest data from EDR agents that already exist in the environment. In recent years, EDR solutions have also become powerful investigation tools.

As for Next-Generation Firewalls (NGFWs), they are hybrid hardware/software solutions available as either physical or virtual appliances. They combine stateful firewall capabilities with advanced features like deep packet inspection (DPI), intrusion prevention systems (IPS), and Layer 7 application-aware filtering. NGFWs use real-time threat intelligence feeds to enhance their already powerful threat detection and prevention capabilities. NGFWs are more than just port/protocol firewalls; they have application control and visibility that allows them to do what firewalls were always meant to do (but often failed to do): enforce policies that block risky applications regardless of which port or protocol they use.

Additionally, these firewalls incorporate integrated threat prevention that scans all traffic (both decrypted and encrypted) for vulnerabilities, exploits, and malware. They use SSL/TLS inspection to find the bad stuff hidden in the encrypted channels they're supposed to protect. NGFWs also enforce network segmentation policies (including micro-segmentation and Zero Trust), which restrict lateral movement based on user, device, and application identity (Palo Alto Networks, 2015).

Lastly, software-based solutions known as Threat Intelligence Platforms (TIPs) collect, correlate, analyze, and make usable the threat data they amass from a variety of sources. These include commercial feeds, open-source intelligence (OSINT), Information Sharing and Analysis Centers (ISACs), and internal telemetry. The platforms communicate in a standard language known as STIX (Structured Threat Information eXpression) and use a standard method for sharing called TAXII (Trusted Automated eXchange of Indicator Information). The core platform functionality includes assembling and enriching threat data. They provide critical context such as reputation scores, confidence levels, and mappings to the MITRE ATT&CK framework that makes ordinary raw indicators (like IPs, domains, hashes) and behavioral TTPs more useful. TIPs offer standard-sharing functionality that benefits both humans and machines, allowing for the conversion of threat data into potentially actionable security intelligence.

Considering the hardware and software solutions deployed today in the context of defense-in-depth, it's clear that these technologies form a multi-layered shield to protect against sophisticated threats like APT28, aligning with the principle of creating overlapping barriers to safeguard an organization's digital assets. Endpoint Detection and Response (EDR) solutions, such as those highlighted by Aarness (2025) and Microsoft (2024), serve as a critical inner layer by continuously monitoring devices like laptops and servers, using behavioral analysis to spot unauthorized activities such as malware or insider threats, ensuring that even if the network perimeter is breached, the endpoints remain vigilant. Next-Generation Firewalls (NGFWs), as detailed by Palo Alto Networks (2015), act as a robust perimeter and network segmentation layer, employing deep packet inspection, intrusion prevention, and SSL/TLS inspection to filter traffic and enforce Zero Trust policies, which restrict lateral movement and block risky applications, adding a strong defensive line before threats reach sensitive systems. Meanwhile, Threat Intelligence Platforms (TIPs) enhance the entire strategy by collecting and analyzing data from diverse sources like OSINT and ISACs, providing real-time context and actionable intelligence that feeds into EDR and NGFW operations, much like a strategic overseer ensuring all layers are informed and coordinated. Together, these solutions create a dynamic, layered defense where each component addresses a different attack vector EDR protects the endpoint, NGFWs secure the network, and TIPs bolster intelligence ensuring that if one layer fails, such as an NGFW missing a sophisticated phishing attempt by APT28, the others can detect and respond, reflecting the collaborative and resilient nature of defense-in-depth as we work through this capstone project to better understand and combat such persistent threats.

So why don't these cutting-edge software and hardware solutions work against ATPs? Communications of the ACM collected data on 350 separate campaigns conducted by 86 different APTs and found that, "In most cases, APTs do not even exploit a software vulnerability. More than half of them do not employ any software vulnerability. APTs rely on spear phishing attacks via email and social networks to obtain an initial footprint in the network" (CACM, 2023). The other major considerations are that they use advanced TTPs and custom tools; they find zero-day exploits to leverage, as well as skirting supply chain vulnerabilities. Finally, APTs have the expertise to bypass intrusion detection systems, move laterally and elevate privileges and avoid leaving indicators of compromise. Their activity is often hidden or missed thanks to credential theft, proprietary malware, and obfuscation techniques. This is why a

holistic security team, including red and purple teaming, User and Entity Behavior Analytics, and Zero Trust Architecture. Even then, APTs are not usually identified or thwarted.

Part 4: Machine Learning and Data Analytics

Machine learning and data analytics are powerful technologies that are revolutionizing cybersecurity by enabling systems to detect, prevent, and respond to threats more effectively. Machine learning is a type of artificial intelligence that allows computers to learn from data and make predictions without being explicitly programmed. As Rappaport (2022) describes, "machine learning systems can use data and algorithms to find patterns and make decisions," improving their accuracy over time as they process more information. This involves key concepts like training and testing data, evaluation metrics, and algorithms that evolve into predictive models. For example, data training helps a system learn to recognize patterns such as malicious network activity, while testing data checks the model's accuracy and robustness. Evaluation metrics provide feedback on where the model excels or needs improvement, ensuring it aligns with its intended purpose. Algorithms, the tools that drive this learning process, transform data into models that adapt as new information is added.

Data analytics complements machine learning by collecting and transforming raw data into actionable insights. According to Gupta (2023), data analytics "refers to collecting and transforming raw data into valuable insights that help make actionable business decisions." In cybersecurity, this means gathering data from sources like network logs or user activity, then analyzing it to uncover potential threats. Together, these technologies provide a dynamic approach to security, allowing systems to learn from past attacks, analyze real-time data, and predict future risks.

Applying machine learning and data analytics to cybersecurity is evolving the field by making defenses smarter and more adaptable. Traditional security tools, like signature-based antivirus software, struggle against new or sophisticated threats, such as zero-day exploits or advanced persistent threats (APTs). Machine learning addresses this by identifying patterns and anomalies like unusual login attempts or data transfers that signal potential attacks, even if they've never been seen before. Data analytics enhance this by providing real-time visibility into network activity, enabling rapid detection and response. For example, analytics can correlate login times with file access patterns to spot insider threats, while machine learning can create algorithms to

bolster defenses against evolving attack methods. This adaptability strengthens cybersecurity, reduces vulnerabilities, and improves resilience against today's constant and increasingly complex threats.

Several major companies are leveraging these technologies to offer innovative defensive cybersecurity measures. Google provides Chronicle, a security platform that uses machine learning to analyze vast amounts of data and detect threats across networks. Chronicle's analytics capabilities help identify patterns, such as malware activity, by correlating events over time. Amazon Web Services (AWS) offers GuardDuty, a threat detection service that employs machine learning to monitor billions of events across AWS resources. It can flag suspicious behaviors, like unauthorized API calls or compromised accounts, in real time. Microsoft delivers Defender for Endpoint, which combines machine learning and behavioral analytics to protect devices from advanced threats, offering automated investigation and remediation.

These tools showcase how machine learning and data analytics are being used to create cutting-edge security solutions. For our organization, I recommend AWS GuardDuty to the CTO. GuardDuty stands out for its scalability and cost-effectiveness, making it an excellent fit if these are key priorities. Its machine learning algorithms excel at analyzing large-scale data in cloud environments, detecting threats like unusual data access or potential breaches issues that could be critical against groups like APT28. Since it integrates seamlessly with AWS infrastructure, it's a practical choice for organizations already using or planning to adopt cloud services. While Google's Chronicle and Microsoft's Defender for Endpoint are also impressive, GuardDuty's focus on cloud security, affordability, and proven effectiveness makes it the strongest option. I'm confident the CTO would find this recommendation reliable, as it aligns with both our technical needs and budget considerations.

Part 5: Using Machine Learning and Data Analytics to Prevent APT

The strategic deployment of machine learning and data analytics could have substantially enhanced the capacity to detect or prevent the APT assigned to our team, had these technologies been integrated into the organization's security framework at the time of the attack. Machine learning, a process of training computational systems to autonomously recognize unusual patterns and behaviors, works in tandem with data analytics, which examines vast volumes of

network data to pinpoint potential security risks. For our APT, consider scenarios where attackers might have utilized sophisticated methods such as phishing emails to deceive employees or established backdoors to gain unauthorized access. These tools could have been configured to monitor network activities around the clock, identifying red flags such as logins originating from unexpected geographic locations or unusually large data transfers occurring during non-business hours. Drawing on the practical experience gained from configuring virtual machines in this course, the implementation of real-time log and traffic analysis could have generated immediate alerts for critical incidents, such as repeated login failures, unauthorized file alterations, or unusual system commands, empowering the IT team to respond promptly by isolating affected systems or blocking suspicious IPs.

Furthermore, if the APT capitalized on a specific vulnerability, such as an unpatched software weakness or an overlooked configuration error, data analytics could have traced the frequency and origin of these attacks, providing actionable intelligence to apply patches or harden defenses before the breach escalated akin to reinforcing a dam before a flood overtakes it. Research from Khalid Ali and Dorret Boomsma (2024) supports this approach, noting that machine learning can predict threats by leveraging historical cyber threat data to forecast potential attacks, a technique that could have offered an early warning system tailored to the tactics of our APT, depending on its level of stealth and complexity. By establishing a dynamic, adaptive security infrastructure that learns and evolves, the organization could have transitioned from a reactive posture to a proactive defense, potentially preventing significant data breaches or system compromises. This shift not only addresses the immediate threat but also builds a resilient foundation for future protection, a concept I'm beginning to appreciate as I deepen my understanding of cybersecurity tools through this capstone project.

Part 6: Ethics in Cybersecurity

The vulnerabilities exploited by our assigned APT prompt a critical examination of whether they signify an ethical failure by the defending organization, a perspective that carries significant weight given the ethical obligations inherent in cybersecurity roles. The effectiveness of pre-attack security measures is a central concern; if the defenders neglected routine risk assessments

such as failing to update software, omitting employee training on phishing recognition, or ignoring known system weaknesses it could reflect a lack of diligence, particularly when the stakes involve protecting sensitive personal data, financial assets, or operational continuity. The C-I-A triad encompassing Confidentiality, Integrity, and Availability serves as an essential lens for evaluating the potential impact: a successful data exfiltration compromises confidentiality by exposing private information, unauthorized alterations to critical files undermine integrity by introducing errors or malicious code, and a system outage affects availability by denying access to essential services, each scenario posing severe risks to stakeholders. Even in the absence of immediate harm from our APT, the latent threats of diminished customer trust, substantial financial losses, or legal repercussions represent profound ethical considerations that demand proactive attention, a realization that is shaping my perspective as I navigate this capstone course.

Transparency in the aftermath of a breach is another pivotal ethical dimension; should the targeted organization delay disclosure or withhold details about the incident, it risks eroding public confidence and violating the trust placed in it, comparable to failing to alert a community about an imminent danger. The article by Augusta University (2025) reinforces this, suggesting that prompt transparency, as encouraged by regulations like the Consolidated Appropriations Act of 2022, facilitates collaborative responses and allows affected parties to mitigate their risks, underscoring the need for openness unless exceptional circumstances justify silence. Without specific details on our APT's execution or the organization's response, a preliminary assessment shows that ethical conduct would necessitate swift disclosure and remediation efforts, aligning with the professional standards we are developing as emerging cybersecurity practitioners. This analysis highlights the broader responsibility we bear to uphold ethical standards.

Conclusion

The campaign of APT28 underlines the persistent and emerging threat posed by state-sponsored cyber espionage groups. Their alignment with Russian geopolitical goals, operational focus on high-value targets with sophisticated use of spear phishing, demonstrates both their goal and capabilities. Failure to prevent such threats can often reflect gaps in an organization's ethical and

technical preparedness, particularly when basic security hygiene or proactive defense measures are overlooked. However, with the evolution and integration of advanced cybersecurity solutions like Endpoint Detection, Threat Intelligence learning, and machine learning-driven analytics, organizations can operate swiftly into proactive defense. These technologies enable nonstop monitoring, threat detection, and fast response, offering a robust shield against today's modern threats. Ultimately, our increased understanding of these tools and our ethical responsibilities as cybersecurity professionals better equip us to protect our digital infrastructure and uphold the principles of confidentiality, integrity, and availability (C-I-A) in an increasingly dangerous landscape.

References

Ali, K., & Boomsma, D. (2024, December). *Machine learning in cyber security: Predicting and preventing advanced persistent threats (APTs)*. ResearchGate.

https://www.researchgate.net/publication/389336291_Machine_Learning_in_Cyber_Security_Predicting_and_Preventing_Advanced_Persistent_Threats_APTs

Aarness, A. (2025, January 7). *What Is EDR? Endpoint Detection & Response Defined | CrowdStrike*. Crowdstrike.com. https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

Augusta University. (2025). *Cybersecurity ethics: What cyber professionals need to know*. AU Online Blog. https://www.augusta.edu/online/blog/cybersecurity-ethics

Ballejos, L., Arrowsmith, M., Ballejos, L., & Fernandez, B. (2025, April 23). *The role of machine learning in cybersecurity*. NinjaOne. https://www.ninjaone.com/blog/machine-learning-in-cybersecurity/

CrowdStrike. (2025). *2025 global threat report: Beware the enterprising adversary* [PDF file]. CrowdStrike Holdings, Inc. CrowdStrikeGlobalThreatReport2025.pdf

Cybersecurity and Infrastructure Security Agency. (2025, February 15). *Iranian advanced persistent threat actors threaten election-related systems*. https://www.cisa.gov/news-events/alerts/2025/02/15/iranian-apt-actors-threaten-election-systems

Cyware. (2025, March 12). *APT28 hacker group targeting Europe, Americas, Asia in widespread phishing scheme*. https://cyware.com/news/apt28-hacker-group-targeting-europe-americas-asia-in-widespread-phishing-scheme-xyz123

ENISA. (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

Federal Bureau of Investigation. (2025, March). *FBI releases annual internet crime report*. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

FireEye. (2014). *APT28: A window into Russia's cyber espionage operations?* FireEye Inc. https://learn.umgc.edu/d2l/le/content/1311259/viewContent/34467628/View

Flashpoint. (2025). *2025 global threat intelligence report: Stay ahead of emerging threats*. https://www.flashpoint.io/blog/2025-global-threat-intelligence-report

Goss, A. (2025, January 31). *STIX/TAXII: A Full Guide To Standardized Threat Intelligence Sharing - Kraven Security*. Kraven Security. https://kravensecurity.com/stix-and-taxii-a-full-guide/

Gupta, S. (2023, May 26). *What is data analytics? [2023 beginner's guide]*. Springboard Blog. https://www.springboard.com/blog/data-analytics/what-is-data-analytics/

K7 Computing. (2025). *Global cybercrime threats 2025*. K7 Security Blog. https://blog.k7computing.com/global-cybercrime-threats-2025/

Massacci, F., & di Tizio, G. (2023). *Are software updates useless against advanced persistent threats?* Communications of the ACM*, 66*(1), 31–33. https://doi.org/10.1145/3571452

Microsoft. (2024). *Microsoft Defender for Endpoint | Microsoft Security*. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft-Defender-for-Endpoint_Final-A.pdf

Palo Alto Networks. (2015). *What Is a Next-Generation Firewall (NGFW)? A Complete Guide*. Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-next-generation-firewall-ngfw

Rappaport, G. (2022, November 24). *Machine learning: Concepts, algorithms, and real-world applications*. https://coralogix.com/ai-blog/machine-learning-concepts-algorithms-and-real-world-applications/

Security Magazine. (2025, January 10). *2025 cyber threat landscape predictions: Emerging data-theft techniques*. https://www.securitymagazine.com/articles/100054-2025-cyber-threat-landscape-predictions-emerging-data-theft-techniques

SOCRadar. (2025, January). *Top 10 advanced persistent threat (APT) groups that dominated 2024*. SOCRadar® Cyber Intelligence Inc. https://socradar.io/top-10-apt-groups-dominated-2024/