Spring 3-17-2022

Zero Trust and Advanced Persistent Threats: Who Will Win the War?

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Todd Whittaker
Franklin University, todd.whittaker@franklin.edu

Recommended Citation

Karabacak, B., & Whittaker, T. (2022, March). Zero trust and advanced persistent threats: Who will win the war?. Proceedings of the 17th International Conference on Cyber Warfare and Security, USA, 17(1), 92-101. https://doi.org/10.34190/iccws.17.1.10

Zero Trust and Advanced Persistent Threats: Who Will Win the War?

Bilge Karabacak and Todd Whittaker
Franklin University, OH, US
bilge.karabacak@franklin.edu
todd.whittaker@franklin.edu

Abstract: Advanced Persistent Threats (APTs) are state-sponsored actors who break into computer networks for political or industrial espionage. Because of the nature of cyberspace and ever-changing sophisticated attack techniques, it is challenging to prevent and detect APT attacks. 2020 United States Federal Government data breach once again showed how difficult to protect networks from targeted attacks. Among many other solutions and techniques, zero trust is a promising security architecture that might effectively prevent the intrusion attempts of APT actors. In the zero trust model, no process insider or outside the network is trusted by default. Zero trust is also called perimeterless security to indicate that it changes the focus from network devices to assets. All processes are required to verify themselves to access the resources. In this paper, we focused on APT prevention. We sought an answer to the question: "could the 2020 United States Federal Government data breach have been prevented if the attacked networks used zero trust architecture?" To answer this question, we used MITRE's ATT&CK® framework to extract how the APT29 threat group techniques could be mitigated to prevent initial access to federal networks. Secondly, we listed basic constructs of the zero trust model using NIST Special Publication 800-207 and several other academic and industry resources. Finally, we analyzed how zero trust can prevent malicious APT activities. We found that zero trust has a strong potential of preventing APT attacks or mitigating them significantly. We also suggested that vulnerability scanning, application developer guidance, and training should not be neglected in zero trust implementations as they are not explicitly or strongly mentioned in NIST SP 800-207 and are among the mostly referred controls in academic and industry publications.

Keywords: Zero Trust, Zero Trust Architecture, ZTA, NIST SP 800-207, MITRE ATT&CK, Advanced Persistent Threats, APT, APT29, SolarWinds Orion Breach

1. Introduction

On December 13, 2020, Cybersecurity and Infrastructure Security Agency (CISA), the federal body responsible for managing the cybersecurity of critical sectors in the US, released an emergency directive (CISA, 2020). The directive was the announcement of the worst cyber-espionage incident ever suffered by the US because of the long duration and the sensitivity and high profile of the targets (Wikipedia, 2021a). If printed, the amount of data stolen would form a stack far taller than the Washington Monument (Bajak, 2020). It was probably one of the most organized cyber-espionage campaigns and the biggest cyber-raid against the US in years. The breach has been named in various names, including SolarWinds Orion Breach, SolarWinds Orion Software Supply Chain Breach, or 2020 United States Federal Government Data Breach.

Many federal organizations in the US were affected by this security incident, such as eleven Departments, including State, Defense, Treasury, Energy, Homeland Security, and Justice. US federal government was not the only victim. There are other Governments, Fortune 500 companies, International Organizations. For example, the British government, NATO, European parliament, and Microsoft were among the victims (Harding and Sabbagh, 2020). SolarWinds announced that it sent an advisory to about 33,000 of its customers around the globe who might have been affected, and roughly 18,000 customers had installed the compromised product (Cimpanu, 2020).

In this modern trojan horse story, cyber attackers turned SolarWinds Orion software into a trojan horse by injecting malicious code. To do that, they penetrated Solarwind's update server by obtaining the easy-to-guess password of the server and injected malware into Orion's update packages. SolarWinds was not the only exploited product; the attackers also exploited software or credentials from Microsoft and VMware.

Attackers started their malicious activities in September 2019. They spent roughly six months on reconnaissance and resource development before initiating the attack. During this time, they created their proof-of-concepts codes, developed a command-and-control system that would allow them to connect victim networks, send commands, and download data. They sneaked their code to the SolarWinds update server as early as March 2020; this is also considered the start day of penetrating federal networks in the US. It has been

passed roughly nine months between the initial access of the attackers and the announcement of the breach by CISA. Eventually, the malicious activities span a timeline of fifteen months.

The cybersecurity advisory released by the United States holds "Russian Foreign Intelligence Service (SVR) actors" responsible for compromising SolarWinds Orion software update packages (NSA, CISA and FBI, 2021). The advisory specifically mentioned the names of three APT groups: APT29, Cozy Bear, and the Dukes.

When it comes to the information on the activities of these threat groups, the MITRE ATT&CK webpage helps security researchers and companies a lot. “MITRE ATT&CK is a knowledge base of cyber adversary behavior and taxonomy for adversarial actions across their lifecycle” (MITRE, 2021b). The tactics and techniques used by the APT29 group have been listed and analyzed on the MITRE ATT&CK webpage. Among the information listed for APT29, there are tools used by the group, procedures -specific implementations of techniques-, associated groups. ATT&CK framework shows Cozy Bear and The Dukes as associated groups with APT29. According to MITRE ATT&CK, APT29 uses more than 80 attack techniques spread into ten different tactics across the adversarial lifecycle. MITRE ATT&CK knowledge base is a community-supported and free-to-use threat intelligence database that can help detect malicious activities and attribute them to the threat groups.

Detection of cyber threats is essential in network defense; prevention is the first step, though. Cyber defenders, including the industry, non-profit organizations, government agencies, and academia, have been working on new services, software, models, tools, and architectures to prevent the attacks at their earliest phases. Zero trust network architecture is a coordinated cybersecurity and system management strategy that combines many existing cybersecurity solutions and paradigms with a different security mindset (NSA, 2021). Zero trust is not a siloed or isolated security application; instead, it is a model that changes the approaches to the trust concept in networks. In the zero trust model, the trust is removed from the network and systems; so that no process (user, computer, device) is trusted by default regardless of its network location and ownership (Rose *et al.*, 2020). Zero trust is also called perimeterless security to indicate the fact that it changes the focus from network devices to data and enterprise resources, and all processes are required to verify themselves to access the resources (Wikipedia, 2021b). Zero trust has been adapted by some enterprises, introduced by security vendors in their services and product portfolio, proposed by academia, and recently formalized by the US government by NIST Special Publication 800-207. Zero trust architecture can be very effective in preventing APT attacks and reducing the impact of sophisticated attacks considerably.

In this article, we reviewed the literature and MITRE ATT&CK database to answer the following questions:

1. Could the 2020 United States Federal Government Data Breach caused by SolarWinds Orion and other vendor vulnerabilities have been prevented if the attacked networks used zero trust architecture?
2. If not, what other controls would have been required to prevent the breach in federal networks?

The article's goal is to provide insights into the effectiveness of Zero Trust Architecture (ZTA) to prevent APT attacks. For that purpose, we reviewed four techniques and five sub-techniques used by the APT29 group to gain initial access to networks (MITRE, 2021a). We also reviewed NIST Special Publication 800-207 and academic resources to extract the main constructs of ZTA. Finally, we discussed the effectiveness of ZTA constructs in preventing the techniques and sub-techniques of the APT29 group and answered two research questions above.

The paper has four sections. The first section is the introduction. The second section is reserved for the literature review. The third section is the part of the article where we answer the research questions. The fourth section is dedicated to future studies and conclusions.

2. Literature Review

This section is grouped into three subsections. The first subsection is dedicated to the methods and tools to prevent APTs. The second subsection is reserved for the MITRE ATT&CK summary. The third subsection gives coverage to the literature about ZTA.

2.1 APT Prevention

As research questions imply, APT detection is not within the scope of this article. Therefore, the literature review on APT is limited to prevention.

It would not be wrong to say that most academic papers about APTs discuss detection methods instead of prevention methods. Vulnerabilities are inevitable. State-sponsored cyber actors are targeted groups and have been using sophisticated techniques. As an expected consequence of these facts, APT groups frequently compromise networks and systems (Karabacak and Tatar, 2014). As a matter of fact, successful APT attacks are assumed to be successful no matter when. The incapability of prevention methods by nature might be the root reason behind the high proportion of APT detection papers (Tatar, Karabacak and Gheorghe, 2016). Cole also assumes the prevention failure in his book and says, "Prevention is ideal, but detection is a must" (Cole, 2013). Cole emphasizes the importance of both prevention and detection in fighting against APTs. According to Cole, companies usually forget about prevention and focus on detection.

On the other hand, the reverse is also true when looking at the long time spans of incidents; companies invest in prevention and show minimal effort on detection (Cole, 2013). The recent breach statistics confirm that millions of records have been stolen from organizations unnoticed for months, even years. Cole emphasizes the importance of augmentation of traditional prevention technologies with additional technologies. The author lists three traditional prevention technologies: firewall, Intrusion Prevention System (IPS), and Data Loss Prevention (DLP). For the augmentation of the firewall, he proposes adding internal firewalls from different vendors in addition to perimeter firewalls and using host-based firewalls. IPS augmentation steps are minimizing false positives and tuning to detect the indicators of APTs. DLPs can be augmented by tying with a Digital Rights Management solution. Finally, Cole indicates that these foundational technologies will not be sufficient to stop APTs.

Moon et al. propose a multi-layer defense system to prevent and detect APTs (Moon *et al.*, 2014). The defense system collects and analyzes log information from endpoints and processes the information with the help of eight components. The authors share two cases for the prevention: infection through USB and spear phishing. The proposed defense system might effectively prevent some specific cyberattacks; however, it cannot be applied to all circumstances. Mohamed et al. stress two crucial social aspects to prevent APT attacks: security awareness and information security policies (Mohamed, Jantan and Abiodun, 2018). They propose an enhancement to the MITRE ATT&CK Mitigations for a specific incident caused by malware infection. They propose automatic termination of the connection between the victim and attacker. Their proposed solution is not comprehensive and mature in mitigating a diverse set of APT tactics and techniques. Messaoud et al. provide a list of technologies to protect against APT actors. Those technologies are sandboxing, honeypots, SIEM, and user behavior analytics (Messaoud *et al.*, 2016). They map these technologies with different attack phases of APT actors in their lifecycle using a matrix. According to the proposed matrix, all these technologies are effective in preventing APT attacks; however, they don't share insights into the possible limitations of these four technologies in preventing APT attacks. Adelaiye et al. review the literature and highlights 12 APT mitigation techniques proposed by 25 researchers (Adelaiye, Ajibola and Faki, 2019). Authors emphasize traffic/data analysis, pattern recognition, and anomaly detection as promising APT mitigation methods. The emphasized methods are all detective controls. There are some prevention methods among the 12 highlighted techniques, which are whitelists, blacklists, IDS, awareness, deception, risk assessment, and multi-layer security. Liu proposes a network security architecture for APT detection and prevention (Liu, 2014). The author focuses on the detection part and proposes a centralized analysis and control module. For the prevention part, they suggest using a firewall and IPS. Jeun et al. categorize the preventive countermeasures for APTs into two; technical and managerial countermeasures. Security tools -firewall, IPS, antivirus-, using authentic software, DLP, encryption, and network separation are listed as technical; risk management, security education, and access control are listed as managerial countermeasures (Jeun, Lee and Won, 2012). Zulkefli et al. propose Multi-Level Security – Access Control framework to prevent APT in BYOD environment (Zulkefli, Singh and Malim, 2015). The proposed model has six layers; outside, mobile component, authentication, authorization, accounting, and security policies. The proposed solutions emphasize the importance of user awareness and robust policy infrastructure for effective prevention.

In addition to recommendations and solutions proposed by academia, security vendors continuously improve their product portfolio that help prevent APT attacks directly or indirectly. Firewall, antivirus, IPS, web application firewall, web & email protection, and sandboxing are among the most common products to prevent APT attacks (Hudson, 2014).

2.2 MITRE ATT&CK

MITRE ATT&CK is a publicly available threat intelligence database that groups the techniques used by cyber actors into 14 tactics sorted by the lifecycle of an attack (MITRE, 2021b). It is based on real-world observations. ATT&CK framework categorizes adversarial behavior into two broad classes; Enterprise and Mobile. There are customized ATT&CK matrices that fall into these two classes. When this article has been prepared, there are 11 matrices for enterprise networks and two matrices for mobile. There is also one matrix for industrial control systems. In addition to ATT&CK matrices that include all documented tactics and techniques for enterprise networks and mobile platforms, MITRE ATT&CK Navigator shows specific techniques used by a threat group. For this article, the authors reviewed six initial access techniques of the APT29 threat group after switching to the MITRE ATT&CK Navigator of the group. Tactics and techniques are the building stones of the framework. Techniques are listed under tactics; there are 188 Techniques, 379 Sub-techniques grouped under 14 tactics. "Techniques represent "how" an adversary achieves a tactical goal by performing an action. Tactics represent the "why" of an ATT&CK technique or sub-technique; they are the reason for performing an action. Sub-techniques are a more specific description of the adversarial behavior used to achieve a goal. They describe behavior at a lower level than a technique (MITRE, 2021b)." ATT&CK website shares other cyberthreat information such as threat groups and tools used by threat groups. The latest version of the ATT&CK (v10) provides detailed information about 129 threat groups and 637 pieces of software used in cyber-attacks.

There are many use cases that ATT&CK can be utilized. For example, it can be used

1. by defense teams to detect cyber threats
2. to model threats and perform comparable and structural threat intelligence
3. by red teams to emulate cyber threats
4. by security architects and engineers to assess the current security posture and redesign the security architecture.

As an example of the fourth use case, the MITRE organization shares the details of a behavioral-based threat model based on MITRE ATT&CK to perform validation of security products (Strom *et al.*, 2017). Several academic studies propose original security methods and models using the ATT&CK framework—the proposed methods and models by academia map to one of four use cases listed above. For example, Outkin et al. present a game-theoretic method that uses the MITRE ATTA&CK APT3 threat data to model attacker-defender interaction and enhance the defender strategies (Outkin *et al.*, 2021). Manocha et al. propose a security assessment rating framework using ATTA&CK (Manocha *et al.*, 2021). Pell et al. study a dynamic threat modeling for 5G networks using ATTA&CK (Pell *et al.*, 2021). Choi et al. show how ATT&CK can be used to generate random attack sequences against ICS datasets (Choi, Yun and Min, 2021). Georgiadou et al. evaluate organizational/individual security culture and security vulnerabilities together and map them to adversaries using ATT&CK to develop a cybersecurity culture framework (Georgiadou, Mouzakitis and Askounis, 2021). Xiong et al. propose a new threat modeling language for enterprise security based on the ATT&CK enterprise matrix (Xiong *et al.*, 2021).

The flexibility and open nature of ATT&CK attract the attention of enterprises and security vendors. Enterprises use the database to improve their security capabilities. Security product vendors actively use ATT&CK to enhance their product features and libraries and map their functionalities to the adversary techniques.

2.3 Zero Trust Architecture (ZTA)

"Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated" (Rose *et al.*, 2020). In the zero trust model, no process insider or outside the network is trusted by default. Zero trust is also called perimeterless security to indicate that it changes the focus from networks, network devices, and perimeters to data and enterprise resources; all entities must verify themselves to access the resources. Some vendors develop zero-trust platforms, whereas some use zero-trust principles to improve their existing security solutions. Colortokens is one of the vendors that developed a zero-trust platform, and they explain how their platform helps stop APT threats (Nayak, 2021). A number of vendors have been preparing guidance documents to provide general information about ZTA and how their products adapt to the architecture (Chowdhury, 2019; Banach, 2021; Checkpoint, 2021; Colortokens, 2021; Splunk, 2021; VMware, 2022).

There are not so many academic studies that analyze the effectiveness and capabilities of ZTA in preventing APT attacks. Alevizos et al. claim that authenticated and authorized endpoints can be considered weak points in networks adopting ZTA so that APTs can perform malicious activities through these endpoints. They suggest using blockchain to verify the integrity of endpoints in a ZTA (Alevizos, Ta and Hashem Eiza, 2021). Horne and Nair claim that ZTA is a realistic security model to battle modern threats, including APTs (Horne and Nair, 2021). Although it is not an academic work, Van Driel provides an overview of how zero trust frustrates APT actors in his blog post (Van Driel, 2015).

Academic studies on ZTA have proposed solutions for specific cybersecurity and technology cases that do not directly touch APT prevention. Collier and Sarkis compare zero trust concepts and current supply chain concepts (Collier and Sarkis, 2021). They discuss the application of zero trust for more secure supply chains. Zaheer et al. propose eZTrust for microservices, a network-independent perimeterization approach using zero trust concepts (Zaheer *et al.*, 2019). One of the use cases for eZTrust is to deploy contingency policies that block the traffic to vulnerable applications. Tao et al. propose a method to perform security controls on big data (Tao, Lei and Ruxiang, 2018). They base their method on zero trust; the first phase of their three-phased approach is user context recognition based on zero trust. Chen et al. propose a security protection framework for power mobile Internet services using zero trust (Chen *et al.*, 2021). Mehraj and Banday propose a zero-trust strategy for the cloud environment (Mehraj and Banday, 2020). The strategy is in the conceptual design phase and is based on choosing trustworthy entities in the cloud environment. De Silva et al. propose a mathematical model for a zero-aware smart home system based on continuous authentication and context-aware access control; both are based on zero trust (da Silva, Macedo and dos Santos, 2021). Vanickis et al. propose a risk-based access control framework for zero trust networks and define the policy languages -such as firewall access control policies- to support the framework (Vanickis *et al.*, 2018).

Trust itself is a vulnerability, and zero trust is a systemic approach to patch this vulnerability (Campbell, 2020). Zero trust might be very efficient in preventing today's sophisticated cyber attackers when implemented adequately by organizations. Academia collaboratively and continuously researches zero trust and proposes conceptual or technical solutions for various cases and systems, including cloud environments, smart homes, supply chains, big data, microservices, and power mobile internet services. Industry adapts itself very well to ZTA; they develop new services and products and share white papers with their partners and customers.

2.4 The Gap in the Literature

There are quite a few academic studies that bring the ZTA and APT concepts together. One of those studies proposes a ZTA and blockchain-based solution that focuses on preventing APTs (Alevizos, Ta and Hashem Eiza, 2021). To the best of our knowledge, there are no studies that research the effectiveness of ZTA in preventing APT attacks.

3. The Analysis of the Effectiveness of Zero Trust in Preventing APTs

In the next section, we analyze the effectiveness of ZTA in preventing APT actors. First, we use MITRE ATT&CK to extract and review the initial access techniques and sub-techniques of the APT29 group. Second, we use the literature and NIST SP 800-207 to extract the main building blocks of zero trust. Third, we analyze the effectiveness of ZTA in preventing the APT29 techniques.

We have several delimitations and limitations. First, we delimit our review to the 2020 United States Federal Government Breach. In this regard, we review the attack techniques of the APT29 group, as that group was one of the main actors of the government breach (NSA, CISA and FBI, 2021). The amount of information about APT actors is limited. MITRE ATT&CK provides the most comprehensive information about the techniques and tools used by APT actors. We used MITRE ATT&CK as the only source of information for APT29 techniques. APT29 group might be using more techniques than provided by the ATT&CK framework. In our reviews, we are limited by the information provided in the ATT&CK. We also assumed that no further tactics in the attack lifecycle would be successful without initial access to the networks.

This section has three sub-sections. In the first subsection, we share our review of four techniques and five sub-techniques of the APT29 group to gain "initial access" to networks. In the second subsection, we summarize the principles and building blocks of zero trust architecture. In the third subsection, we evaluate the effectiveness of zero trust in preventing APT techniques.

3.1 APT Analysis

We limited our scope to the initial access tactic of APT29 because our focus is the prevention at the very beginning of the threat lifecycle. If defenders succeed in thwarting APT actors at the initial access step, APTs will not be able to step up to the forthcoming tactics. Specifically, 11 tactics in ATT&CK Enterprise Matrix that come after the initial access are actions of the APT actors who completed the initial access. The two tactics before the initial access are reconnaissance and resource development. The preventive countermeasures associated with these tactics are within the scope of cyber deterrence and cyber diplomacy.

There are tools and methods, including zero trust, that can effectively prevent APT techniques associated with the tactics after the initial access. However, our focus is to analyze the effectiveness of zero trust in preventing APT activities without any network compromises.

Figure-1 shows the four techniques and five sub-techniques used by APT29 in initial access. Figure-1 is taken from the ATT&CK Navigator page of APT29. The shaded techniques are the ones used by APT29.

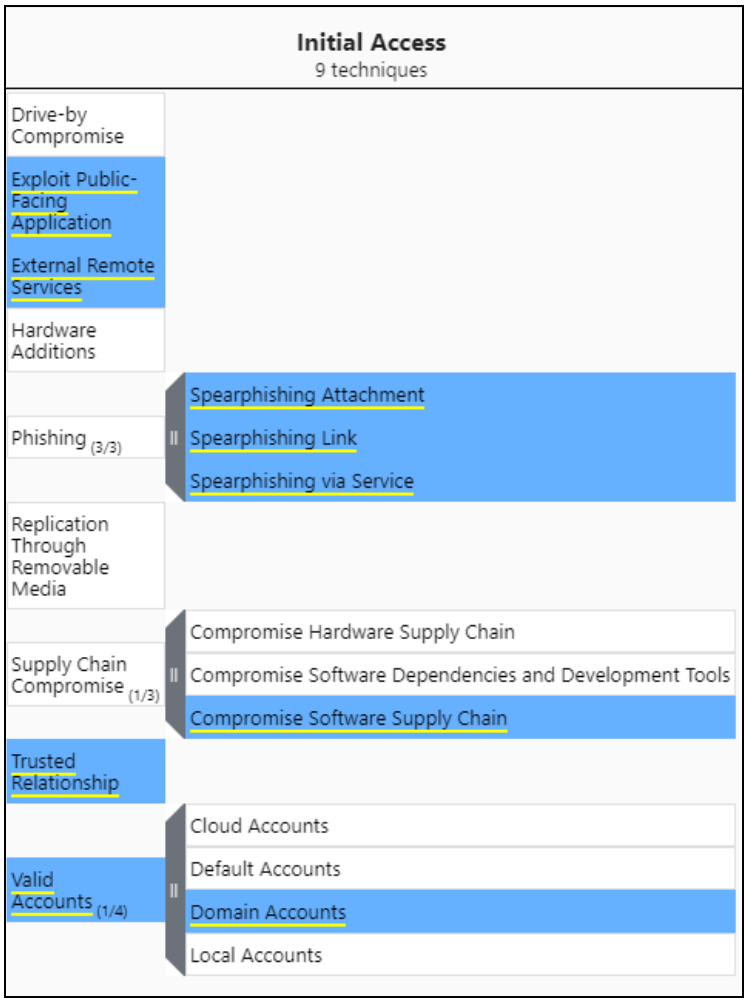

Figure 1: Initial access techniques and sub-techniques of APT29

Respective countermeasures for these techniques are listed in Table-1. The countermeasures are extracted from the ATT&CK webpage as well. The description of techniques and mitigations is not given in this article because of the space constraints.

Table 1: Mitigations for APT29 techniques and sub-techniques

Technique/Sub-technique	Mitigation
T1190: Exploit Public-Facing Application	1. Application Isolation and Sandboxing (1)

	2. Exploit Protection (2) 3. Network Segmentation (3) 4. Privileged Account Management (4) 5. Update Software (5) 6. Vulnerability Scanning (6)
T1133: External Remote Services	1. Disable or Remove Feature or Program (7) 2. Limit Access to Resource Over Network (8) 3. Multi-factor Authentication (9) 4. Network Segmentation (3)
T1199: Trusted Relationship	1. Network Segmentation (3) 2. User Account Control (10)
T1078: Valid Accounts	1. Application Developer Guidance (11) 2. Password Policies (12) 3. Privileged Account Management (4) 4. User Training (13)
T1078.002: Domain Accounts	1. Multi-factor Authentication (9) 2. Privileged Account Management (4) 3. User Training (13)
T1566.001: Spearphishing Attachment	1. Antivirus/antimalware (14) 2. Network Intrusion Prevention (15) 3. Restrict Web-based Content (16) 4. Software Configuration (17) 5. User Training (13)
T1566.002: Spearphishing Link	6. Restrict Web-based Content (16) 7. Software Configuration (17) 8. User Training (13)
T1566.003: Spearphishing via Service	1. Antivirus/antimalware (14) 2. Restrict Web-based Content (16) 3. User Training (13)
T1195.002: Compromise Software Supply Chain	1. Update Software (5) 2. Vulnerability Scanning (6)

After removing the duplicated mitigations from Table-1, we are left with 17 unique controls to compare with Zero Trust. Note that numbers that uniquely identify controls are put next to each control in the second column of Table-2.

3.2 Zero Trust Architecture

ZTA is not a straightforward solution; instead, it combines different kinds of technologies, methods, and procedures. It involves people, processes, and technology. Successful implementation of ZTA requires a total commitment from leadership (Chowdhury, 2019; NSA, 2021). It should also be aligned with business objectives (Chowdhury, 2019). Every organization can adapt to ZTA differently depending on different organizational and technological factors. In this section, we extracted seventeen components of ZTA by reviewing various academic and industry resources (Modderkolk, 2018; Chowdhury, 2019; Rivas, 2019; Embrey, 2020; Rose *et al.*, 2020; Uttecht, 2020; Alevizos, Ta and Hashem Eiza, 2021; Banach, 2021; Buck *et al.*, 2021; Checkpoint, 2021; Colortokens, 2021; Garbis and Chapman, 2021; Sanders *et al.*, 2021; Splunk, 2021; Xiaojian *et al.*, 2021; VMware, 2022):

1. Centralized authentication of users, devices, and applications (accompanied by SSO and MFA)
2. Encryption
3. Continuous monitoring
4. Network segmentation
5. Application segmentation
6. Network access control
7. System access control
8. Traffic filtering
9. Application execution control

10. Operational and forensic analysis (Includes vulnerability scanning (Uttecht, 2020))
11. Policy enforcement
12. Configuration management
13. Data discovery, tracking, and analysis (Asset inventory)
14. User account management
15. Least privilege principle
16. Guidance and training of application developers
17. Training and awareness

ZTA uses the existing technologies; the differentiation of ZTA is how it brings these technologies together to create a zero-trust mindset in organizations. Below is the list of fundamental tenets of zero trust as shared in NIST SP 800-207. The above list of countermeasures might not help readers understand how ZTA is designed and deployed. The implementation context for the seventeen items above is explained thoroughly in NIST SP 800-207.

3.3 Comparative Analysis of ATT&CK Mitigations and ZTA Components

This section compares two numbered lists of countermeasures in Sections 3.1 and 3.2. The first list was the mitigations suggested by MITRE ATT&CK to prevent APT29 initial access attempts. The second list was the list of components of ZTA, composed after reviewing NIST SP 800-207 and several academic articles and industry whitepapers. The controls in the two lists are matched in Table-2.

Table 2: Comparison of ATT&CK mitigations and ZTA components

Mitigation suggested by MITRE ATT&CK (See Table-1)	**Corresponding component of ZTA as suggested by NIST SP 800-27, academia and/or industry (See the list in the previous page)**
Application Isolation and Sandboxing (1)	Application segmentation (5)
Exploit Protection (2)	Traffic filtering (8)
Network Segmentation (3)	Network segmentation (4)
Privileged Account Management (4)	Least privilege principle (15)
Update Software (5)	Operational and forensic analysis (10) Configuration management (12)
Vulnerability Scanning (6)	Operational and forensic analysis (10)
Disable or Remove Feature or Program (7)	Application execution control (9)
Limit Access to Resource Over Network (8)	Network access control (6) System access control (7)
Multi-factor Authentication (9)	Centralized authentication of users, devices, and applications (accompanied by SSO and MFA) (1)
User Account Control (10)	User account management (14) Least privilege principle (15)
Application Developer Guidance (11)	Guidance and training of application developers (16)
Password Policies (12)	Policy enforcement (11)
User Training (13)	Training and awareness (17)
Antivirus/antimalware (14)	Application execution control (9)
Network Intrusion Prevention (15)	Network access control (6)
Restrict Web-based Content (16)	Least privilege principle (15)
Software Configuration (17)	Configuration management (12)

All of the mitigations suggested by MITRE ATT&CK to prevent APT29 initial access have been matched by technologies, methods, and procedures recommended for zero trust implementations by NIST SP 800-207, academia, or industry.

NIST's SP 800-207 can be considered one of the principal resources in defining ZTA. It provides comprehensive guidance for organizations that plan to switch to ZTA. However, Vulnerability Scanning, Application Developer Guidance, and User Training have not been explicitly or strongly mentioned in NIST SP 800-207. Authors

suggest that the future revision of NIST SP 800-207 should include these controls; even if they are not at the core of zero trust, they are essential preventative controls.

Three ZTA components in the list don't match any mitigations suggested by MITRE ATT&CK to prevent the APT29 threat actor. These components are (1) encryption, (2) continuous monitoring, and (3) data discovery, tracking, and analysis (Asset inventory). It is an anticipated situation; because the authors reviewed a number of academic and industry papers to extract ZTA components. It has been expected that the set of extracted components will be more extensive than the set of mitigations suggested by MITRE ATT&CK.

4. Conclusion

Information security controls can be classified as preventive and detective controls; some are preventive and detective, such as antivirus software. Prevention is ideal; however, detection is a must. As a matter of fact, one hundred percent prevention is impossible, making absolute security an impossible task. Eventually, this reality makes detection a mandatory process for organizations.

The two tactics of MITRE ATT&CK that come before "Initial Access" are "Reconnaissance" and "Resource Development". Cyber deterrence and cyber diplomacy might be effective in preventing Reconnaissance and Resource Development. Both tactics are difficult to mitigate by organizations, though, because the prevention methods for these tactics are implemented in a domain that is predominantly out of direct control of organizations. Moreover, these prevention methods might not be as effective as the prevention methods of Initial Access and subsequent tactics after the Initial Access. The detection of reconnaissance and resource development can be accomplished by cyber threat intelligence services. It is an effective method frequently used by organizations. Initial Access is the first tactic after Reconnaissance and Resource Development that an organization has direct control on the mitigation steps to prevent the techniques under this tactic. Effective prevention of Initial Access techniques is key to keeping the networks secure. In the SolarWinds breach, after attackers succeeded in the initial attack, they progressed successfully in the subsequent tactics such as Execution, Persistence, and Privilege Escalation.

Zero Trust Architecture is a promising approach to prevent Advanced Persistent Threats. There is a significant overlap between MITRE ATT&CK controls to prevent Initial Access and ZTA components and principles extracted from a diverse set of academic and industry papers. Merely focusing on detecting APTs has proven insufficient, and prevention should be considered at a higher priority than it has been in the past. ZTA is a structured way of accomplishing that goal.

ZTA can prevent the APT actors at the Initial Access and, therefore, improve the security significantly. In this regard, the 2020 United States Federal Government Data Breach caused by SolarWinds Orion and other vendor vulnerabilities could have been prevented if the attacked networks had used ZTA; in the worst case, the harm caused by the attacks might be far less compared to the actual case.

References

Adelaiye, O., Ajibola, A. and Faki, S. (2019) 'Evaluating Advanced Persistent Threats Mitigation Effects: A Review', p. 14.

Alevizos, L., Ta, V.T. and Hashem Eiza, M. (2021) 'Augmenting zero trust architecture to endpoints using blockchain: A STATE-OF-THE-ART review', *Security and Privacy* [Preprint]. doi:10.1002/spy2.191.

Bajak, F. (2020) 'Hack may have exposed deep US secrets; damage yet unknown', *AP News*. Available at: https://apnews.com/article/technology-hacking-coronavirus-pandemic-russia-350ae2fb2e513772a4dc4b7360b8175c (Accessed: 18 November 2021).

Banach, Z. (2021) 'Vulnerability scanning with PAM in zero trust environments'. Available at: https://www.netsparker.com/blog/docs-and-faqs/vulnerability-scanning-privileged-access-management-zero-trust-environments/ (Accessed: 6 January 2022).

Buck, C. *et al.* (2021) 'Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust', *Computers & Security*, 110, p. 102436. doi:10.1016/j.cose.2021.102436.

Campbell, M. (2020) 'Beyond Zero Trust: Trust Is a Vulnerability', *Computer*, 53(10), pp. 110–113. doi:10.1109/MC.2020.3011081.

Checkpoint (2021) 'The Ultimate Guide to Zero Trust Security'. Available at: https://pages.checkpoint.com/the-ultimate-guide-to-zero-trust.html (Accessed: 19 November 2021).

Chen, L. *et al.* (2021) 'Research on the Security Protection Framework of Power Mobile Internet Services Based on Zero Trust', in *2021 6th International Conference on Smart Grid and Electrical Automation (ICSGEA)*. *2021 6th International Conference on Smart Grid and Electrical Automation (ICSGEA)*, Kunming, China: IEEE, pp. 65–68. doi:10.1109/ICSGEA53208.2021.00021.

Choi, S., Yun, J.-H. and Min, B.-G. (2021) 'Probabilistic Attack Sequence Generation and Execution Based on MITRE ATT&CK for ICS Datasets', in *Cyber Security Experimentation and Test Workshop*. *CSET '21: Cyber Security Experimentation and Test Workshop*, Virtual CA USA: ACM, pp. 41–48. doi:10.1145/3474718.3474722.

Chowdhury, D.D. (2019) 'An Essential Guide to Zero Trust Security', p. 32.

Cimpanu, C. (2020) 'SEC filings: SolarWinds says 18,000 customers were impacted by recent hack', *ZDNet*. Available at: https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/ (Accessed: 18 November 2021).

CISA (2020) 'CISA Issues Emergency Directive to Mitigate the Compromise of Solarwinds Orion Network Management Products'. Available at: https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network (Accessed: 18 November 2021).

Cole, E. (2013) *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Syngress.

Collier, Z.A. and Sarkis, J. (2021) 'The zero trust supply chain: Managing supply chain risk in the absence of trust', *International Journal of Production Research*, 59(11), pp. 3430–3445. doi:10.1080/00207543.2021.1884311.

Colortokens (2021) 'The Definitive Guide to Zero-Trust Security'. Available at: https://colortokens.com/ebook/definitive-guide-zero-trust-security/ (Accessed: 19 November 2021).

Embrey, B. (2020) 'The top three factors driving zero trust adoption', *Computer Fraud & Security*, 2020(9), pp. 13–15. doi:10.1016/S1361-3723(20)30097-X.

Garbis, J. and Chapman, J.W. (2021) *Zero Trust Security: An Enterprise Guide*. Berkeley, CA: Apress. doi:10.1007/978-1-4842-6702-8.

Georgiadou, A., Mouzakitis, S. and Askounis, D. (2021) 'Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework', *Sensors*, 21(9), p. 3267. doi:10.3390/s21093267.

Harding, L. and Sabbagh, D. (2020) 'Suspected Russian hackers spied on US federal agencies', *The Guardian*. Available at: https://www.theguardian.com/world/2020/dec/14/suspected-russian-hackers-spied-on-us-federal-agencies (Accessed: 18 November 2021).

Horne, D. and Nair, S. (2021) 'Introducing Zero Trust by Design: Principles and Practice Beyond the Zero Trust Hype', p. 11.

Hudson, B. (2014) 'Advanced Persistent Threats: Detection, Protection and Prevention'. Sophos.

Jeun, I., Lee, Y. and Won, D. (2012) 'A Practical Study on Advanced Persistent Threats', in *Computer Applications for Security, Control and System Engineering*. *SecTech 2012*, Korea: Springer, pp. 144–152.

Karabacak, B. and Tatar, U. (2014) 'Strategies to Counter Cyberattacks: Cyber threats and Critical Infrastructure Protection', in Edwards, M. (ed.) *NATO Science for Peace and Security Series - E: Human and Societal Dynamics*, pp. 63–73.

Liu, X. (2014) 'Research on Prevention Solution of Advanced Persistent Threat', in. *2014 2nd International Conference on Software Engineering, Knowledge Engineering and Information Engineering (SEKEIE 2014))*, Singapore. doi:10.2991/sekeie-14.2014.33.

Manocha, H. *et al.* (2021) 'Security Assessment Rating Framework for Enterprises using MITRE ATT&CK® Matrix', p. 11.

Mehraj, S. and Banday, M.T. (2020) 'Establishing a Zero Trust Strategy in Cloud Computing Environment', in *2020 International Conference on Computer Communication and Informatics (ICCCI)*. *2020 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India: IEEE, pp. 1–6. doi:10.1109/ICCCI48352.2020.9104214.

Messaoud, B.I.D. *et al.* (2016) 'Advanced Persistent Threat: New analysis driven by life cycle phases and their challenges', in *2016 International Conference on Advanced Communication Systems and Information Security (ACOSIS)*. *2016 International Conference on Advanced Communication Systems and Information Security (ACOSIS)*, Marrakesh, Morocco: IEEE, pp. 1–6. doi:10.1109/ACOSIS.2016.7843932.

MITRE (2021a) 'APT29 Attack Navigator'. Available at: https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0016%2FG0016-enterprise-layer.json.

MITRE (2021b) 'Frequently Asked Questions'. Available at: https://attack.mitre.org/resources/faq/ (Accessed: 18 November 2021).

Modderkolk, M. (2018) *Zero Trust Maturity Matters*. Master's Thesis. Utrecht University.

Mohamed, N.A., Jantan, A. and Abiodun, O.I. (2018) 'An Improved Behaviour Specification to Stop Advanced Persistent Threat on Governments and Organizations Network', *Hong Kong*, p. 6.

Moon, D. *et al.* (2014) 'MLDS: Multi-Layer Defense System for Preventing Advanced Persistent Threats', *Symmetry*, 6(4), pp. 997–1010. doi:10.3390/sym6040997.

Nayak, S. (2021) 'What Are Advanced Persistent Threats (APTs) and How Can You Contain Them?' Available at: https://colortokens.com/blog/advanced-persistent-threats-apt/ (Accessed: 19 November 2021).

NSA (2021) 'Embracing a Zero Trust Security Model'.

NSA, CISA and FBI (2021) 'Russian SVR Targets U.S. and Allied Networks'.

Outkin, A.V. *et al.* (2021) 'Defender Policy Evaluation and Resource Allocation Using MITRE ATT&CK Evaluations Data', *arXiv:2107.04075 [cs]* [Preprint]. Available at: http://arxiv.org/abs/2107.04075 (Accessed: 19 November 2021).

Pell, R. *et al.* (2021) 'Towards Dynamic Threat Modelling in 5G Core Networks Based on MITRE ATT&CK', *arXiv:2108.11206 [cs]* [Preprint]. Available at: http://arxiv.org/abs/2108.11206 (Accessed: 19 November 2021).

Rivas, G. (2019) 'Zero Trust Model: An Effective Approach to Protecting Your Digital Environment', 14 January. Available at: https://www.gb-advisors.com/the-zero-trust-model/ (Accessed: 6 January 2022).

Rose, S. *et al.* (2020) *Zero Trust Architecture*. National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-207.

Sanders, G. *et al.* (2021) 'Integrating Zero Trust and DevSecOps'.

da Silva, G.R., Macedo, D.F. and dos Santos, A.L. (2021) 'Zero Trust Access Control with Context-Aware and Behavior-Based Continuous Authentication for Smart Homes', in *Anais do XXI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2021)*. *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, Brasil: Sociedade Brasileira de Computação - SBC, pp. 43–56. doi:10.5753/sbseg.2021.17305.

Splunk (2021) 'The Essential Guide to Zero Trust'. Available at: https://www.splunk.com/en_us/form/the-essential-guide-to-zero-trust.html (Accessed: 19 November 2021).

Strom, B. *et al.* (2017) 'Finding Cyber Threats with ATT&CK-Based Analytics', (16), p. 53.

Tao, Y., Lei, Z. and Ruxiang, P. (2018) 'Fine-grained Big Data Security Method Based on Zero Trust Model', in *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*. Singapore: IEEE, pp. 1040–1045.

Tatar, U., Karabacak, B. and Gheorghe, A. (2016) 'An Assessment Model to Improve National Cyber Security Governance', in Zlateva, D.T. and Greiman, V.A. (eds) *11th International Conference on Cyber Warfare and Security*. ACPI Limited, pp. 312–319.

Uttecht, K.D. (2020) *Zero Trust (ZT) Concepts for Federal Government Architectures*. Technical Report 1253. Lexington: Lincoln Laboratory.

Van Driel, R. (2015) 'Zero Trust and APT'. Available at: https://www.linkedin.com/pulse/zero-trust-apt-ruud-van-driel-cissp/). (Accessed: 19 November 2021).

Vanickis, R. *et al.* (2018) 'Access Control Policy Enforcement for Zero-Trust-Networking', in *2018 29th Irish Signals and Systems Conference (ISSC)*. *2018 29th Irish Signals and Systems Conference (ISSC)*, Belfast: IEEE, pp. 1–6. doi:10.1109/ISSC.2018.8585365.

VMware (2022) 'Implement Zero Trust Security'. Available at: https://www.vmware.com/solutions/zero-trust-security.html (Accessed: 6 January 2022).

Wikipedia (2021a) '2020 United States federal government data breach'. Available at: https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach (Accessed: 18 November 2021).

Wikipedia (2021b) 'Zero trust security model'. Available at: https://en.wikipedia.org/wiki/Zero_trust_security_model.

Xiaojian, Z. *et al.* (2021) 'Power IoT security protection architecture based on zero trust framework', in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*. *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, Zhuhai, China: IEEE, pp. 166–170. doi:10.1109/CSP51677.2021.9357607.

Xiong, W. *et al.* (2021) 'Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix', *Software and Systems Modeling* [Preprint]. doi:10.1007/s10270-021-00898-7.

Zaheer, Z. *et al.* (2019) 'eZTrust: Network-Independent Zero-Trust Perimeterization for Microservices', in *Proceedings of the 2019 ACM Symposium on SDN Research*. *SOSR '19: Symposium on SDN Research*, San Jose CA USA: ACM, pp. 49–61. doi:10.1145/3314148.3314349.

Zulkefli, Z., Singh, M.M. and Malim, N.H.A.H. (2015) 'Advanced Persistent Threat Mitigation Using Multi Level Security – Access Control Framework', in *Computational Science and Its Applications – ICCSA 2015*. *The 15th International Conference on Computational Science and Its Applications*, Canada: Springer, pp. 90–105.