Abstract – This document provides a comprehensive analysis of publication which details the evolving tactics, techniques, and procedures (TTPs) employed by cyber actors to gain initial access to cloud-based systems. The analysis will cover various aspects including the identification and exploitation of vulnerabilities, different cloud exploitation techniques, deployment of custom malware.

The analysis provides a distilled exploration, highlighting the key points and actionable intelligence that can be leveraged by cybersecurity professionals, IT personnel, and specialists across various industries to enhance their defensive strategies against state-sponsored cyber threats. By understanding the actor's adapted tactics for initial cloud access, stakeholders can better anticipate and mitigate potential risks to their cloud-hosted infrastructure, thereby strengthening their overall security posture.

I. Introduction

The document titled "cyber actors adapt tactics for initial cloud access" released by the National Security Agency (NSA) warns of use of cyber actors have adapted their tactics to gain initial access to cloud services, as opposed to exploiting on-premise network vulnerabilities.

This shift is in response to organizations modernizing their systems and moving to cloud-based infrastructure. The high-profile cyber campaigns like the SolarWinds supply chain compromise are now expanding to sectors such as aviation, education, law enforcement, local and state councils, government financial departments, and military organizations.

The stark reality is that to breach cloud-hosted networks, these actors need only to authenticate with the cloud provider, and if they succeed, the defenses are breached. The document highlights a particularly disconcerting aspect of cloud environments: the reduced network exposure compared to on-premises systems paradoxically makes initial access a more significant linchpin.

Over the past year, the TTPs observed have been alarmingly simple yet effective, with the cyber actors exploiting service and dormant accounts through brute force attacks. The document offers a cold comfort implies a race against time to fortify their defenses against these TTPs to prevent initial access.

II. Key findings

- **Adaptation to Cloud Services**: Cyber actors have shifted their focus from exploiting on-premises network vulnerabilities to directly targeting cloud services. This change is a response to the modernization of systems and the migration of organizational infrastructure to the cloud.
- **Authentication as a Key Step**: To compromise cloud-hosted networks, cyber actors must first successfully authenticate with the cloud provider. Preventing this initial access is crucial for stopping from compromising the target.
- **Expansion of Targeting**: Cyber actors have broadened their targeting to include sectors such as aviation, education, law enforcement, local and state councils, government financial departments, and military organizations. This expansion indicates a strategic diversification of targets for intelligence gathering.
- **Use of Service and Dormant Accounts**: it highlights that cyber actors have been observed using brute force attacks to access service and dormant accounts over the last 12 months. This tactic allows to gain initial access to cloud environments.
- **Sophistication of cyber actors**: The cyber actors can execute global supply chain compromises, such as the 2020 SolarWinds incident.
- **Defense through Cybersecurity Fundamentals**: The advisory emphasizes that a strong baseline of cybersecurity fundamentals can defend against cyber actors. For organizations that have transitioned to cloud infrastructure, protecting against TTPs for initial access is presented as a first line of defense.

III. Adaptation to Cloud Services

The adaptation of attacks to target cloud services marks a significant evolution in the landscape of cyber espionage and cyber warfare. This shift is not merely a change in target but represents a deeper strategic adaptation to the changing technological environment and the increasing reliance of governments and corporations on cloud infrastructure. The move towards cloud services by organizations is driven by the benefits of scalability, cost-efficiency, and the ability to rapidly deploy and update services. However, this transition also presents new vulnerabilities and challenges for cybersecurity.

A. Strategic Shift to Cloud

As organizations have modernized their systems and migrated to cloud-based infrastructure, actors have adapted their tactics, techniques, and procedures (TTPs) to this new environment. This adaptation is driven by the realization that cloud services, by centralizing vast amounts of data and resources, present a lucrative target for espionage and intelligence gathering. The cloud's architecture, while offering

numerous advantages to organizations, also necessitates a reevaluation of security strategies to address unique vulnerabilities.

B. Tactics, Techniques, and Procedures (TTPs)

The adaptation of actors to cloud services involves a range of sophisticated TTPs designed to exploit the specific characteristics of cloud environments. One of the primary methods of gaining initial access to cloud-hosted networks involves authenticating to the cloud provider. This can be achieved through various means, including brute forcing and password spraying to access services and dormant accounts. These accounts, often used to run and manage applications without direct human oversight, are particularly vulnerable as they may not be protected by multi-factor authentication (MFA) and may possess high levels of privilege.

Furthermore, actors have been observed using system-issued tokens for authentication, bypassing the need for passwords. They have also exploited the process of enrolling new devices to the cloud, bypassing MFA through techniques such as "MFA bombing" or "MFA fatigue." Additionally, the use of residential proxies to obscure their internet presence and make malicious activity harder to detect represents another layer of sophistication in their operations.

C. Implications and Mitigations

The adaptation of actors to target cloud services has significant implications for cybersecurity. It underscores the need for organizations to implement robust security measures tailored to the cloud environment. This includes enforcing strong password policies, implementing MFA, managing and monitoring service and dormant accounts, and configuring device enrollment policies to prevent unauthorized access. Additionally, adjusting the validity time of system-issued tokens and employing network-level defenses to detect and mitigate the use of residential proxies are critical steps in defending against these threats.

IV. TTPs DETAILS:

- **Credential Access / T1110 Brute Forcing**: actors utilize password spraying and brute forcing as initial infection vectors. This approach involves attempting multiple passwords against different accounts (password spraying) or numerous password attempts on a single account (brute forcing) to gain unauthorized access.
- **Initial Access / T1078.004 Valid Accounts**: **Cloud Accounts**: The actors gains access to cloud services by using compromised credentials. This includes targeting both system accounts (used for automated tasks and services) and dormant accounts (inactive accounts that still remain on the system).
- **Credential Access / T1528 Steal Application Access Token**: Actors exploit stolen access tokens to log into accounts without needing the passwords. Access tokens are digital keys that allow access to user accounts, and obtaining these can bypass traditional login mechanisms.
- **Credential Access / T1621 Multi-Factor Authentication Request Generation**: Known as 'MFA bombing' or 'MFA fatigue,' this technique involves actors repeatedly sending MFA requests to a victim's device. The goal is to overwhelm or fatigue the victim into accepting the request, thus granting the attacker access.
- **Command and Control / T1090.002 Proxy**: **External Proxy**: To maintain covert operations and blend in with normal traffic, actors use open proxies located in residential IP ranges. This makes malicious connections harder to distinguish from legitimate user activity in access logs.
- **Persistence / T1098.005 Account Manipulation**: Device Registration: After gaining access to accounts, actors attempt to register their own devices on the cloud tenant. Successful device registration can provide persistent access to the cloud environment.

A. Access via Service and Dormant Accounts

One of the key strategies employed by actors involves targeting service and dormant accounts within cloud environments. Service accounts are used to run and manage applications and services without direct human interaction. These accounts are particularly vulnerable because they often cannot be protected with multi-factor authentication (MFA) and may have highly privileged access depending on their role in managing applications and services. By gaining access to these accounts, threat actors can obtain privileged initial access to a network, which they can use as a launchpad for further operations

The document also highlights that campaigns have targeted dormant accounts—accounts belonging to users who are no longer active within the victim organization but have not been removed from the system. These accounts can be exploited by attackers to regain access to a network, especially following incident response measures such as enforced password resets. actors have been observed logging into these inactive accounts and following password reset instructions, allowing them to maintain access even after incident response teams have attempted to evict them

B. Cloud-Based Token Authentication

Another TTP mentioned in the document is the use of cloud-based token authentication. Actors have been observed using system-issued access tokens to authenticate victims' accounts without needing a password. This technique bypasses traditional credential-based authentication methods and can be particularly effective if the validity period of these tokens is long or if the tokens are not properly secured and managed

C. Brute Forcing and Password Spraying

The document also describes the use of brute forcing (T1110) and password spraying by actors as initial infection vectors. These techniques involve attempting to access accounts by trying many passwords or using common passwords against many accounts, respectively. Such methods are often successful due to the use of weak or reused passwords across different accounts

D. The Role of Access Tokens

Access tokens are an integral part of modern authentication systems, especially in cloud environments. They are designed to simplify the login process for users and provide a secure method of accessing resources without repeatedly entering credentials. Tokens are typically issued after a user logs in with a username and password, and they can be used for subsequent authentication requests.

E. Risks Associated with Token Authentication

While token-based authentication can offer convenience and security, it also introduces specific risks if not properly managed. If threat actors obtain these tokens, they can gain access to accounts without needing to know the passwords. This can be particularly problematic if the tokens have a long validity period or if they are not adequately secured.

F. Adjusting Token Validity

The document notes that the default validity time of system-issued tokens can vary depending on the system in use. However, it is crucial for cloud platforms to provide administrators with the ability to adjust the validity time of these tokens to suit their security needs. Shortening the validity period of tokens can reduce the window of opportunity for unauthorized access if tokens are compromised.

G. Bypassing Password Authentication and MFA

The document details how actors have successfully bypassed password authentication on personal accounts through techniques such as password spraying and credential reuse. Password spraying involves attempting to access a large number of accounts using commonly used passwords, while credential reuse exploits the tendency of users to recycle the same passwords across multiple accounts. These methods exploit weaknesses in password-based authentication systems to gain initial access to accounts.

Furthermore, actors have employed a technique known as 'MFA bombing' or 'MFA fatigue' (T1621) to bypass multi-factor authentication (MFA) systems. This technique involves repeatedly sending MFA requests to a victim's device until the victim, overwhelmed or frustrated by the constant notifications, accepts the request. This method effectively exploits human psychology and the inconvenience of repeated notifications to circumvent an otherwise robust security measure.

H. Enrolling New Devices to the Cloud

Once past these initial security barriers, the document reports that actors have been observed registering their own devices as new devices on the cloud tenant (T1098.005). This step is critical for maintaining access to the cloud environment and facilitating further malicious activities. The success of this tactic hinges on the absence of stringent device validation rules within the cloud tenant's security configuration. Without proper device validation measures, attackers can easily add unauthorized devices to the network, granting them access to sensitive data and systems.

I. Defense Against Unauthorized Device Enrollment

The document highlights the importance of configuring the network with robust device enrollment policies as a defense mechanism against such attacks. By implementing strict device validation rules and enrollment policies, organizations can significantly reduce the risk of unauthorized device registration. Instances where these measures have been effectively applied have successfully defended against actors, denying them access to the cloud tenant.

J. Residential Proxies and Their Use by Actors

Residential proxies are intermediary services that allow users to route their internet traffic through an IP address provided by an internet service provider (ISP) that is typically assigned to a residential address. This makes the traffic appear as if it is originating from a regular home user, which can be particularly useful for cyber actors looking to blend in with normal internet traffic and avoid raising red flags.

The use of residential proxies by actors serves to obfuscate their true location and the source of their malicious activities. By making their traffic appear to come from legitimate ISP ranges used by residential broadband customers, they can significantly reduce the likelihood of their connections being flagged as malicious. This tactic complicates the efforts of cybersecurity defenses that rely on IP address reputation or geolocation as indicators of compromise.

K. Challenges Posed by Residential Proxies

The effectiveness of residential proxies in hiding the origin of traffic presents a challenge for network defenses. Traditional security measures that track and block known malicious IP addresses may not be effective against attackers using residential proxies, as these IP addresses may not have a prior history of malicious activity and are indistinguishable from those of legitimate users.

V. Authentication as a Key Step

A. Authentication as a Key Step in Cloud Security

In the evolving landscape of cybersecurity, the adaptation of cyber actors to target cloud services underscores a pivotal shift in the tactics of cyber espionage. This transition from exploiting on-premises network vulnerabilities to directly targeting cloud-based infrastructures marks a significant evolution in cyber threats. At the heart of this shift is the critical role of authentication as a key step in securing cloud-hosted networks against sophisticated cyber actors.

B. The Importance of Authentication in Cloud Environments

Authentication serves as the gateway to cloud services, determining whether access should be granted to a user or system. In cloud environments, where resources and data are hosted off-premises and accessed over the internet, the importance of robust authentication mechanisms cannot be overstated. Unlike traditional on-premises setups, where physical security measures and internal network defenses can provide layers of security, cloud services are inherently more exposed to the internet. This exposure makes the initial step of authentication not just a security measure, but a critical defense mechanism against unauthorized access.

C. Challenges in Cloud Authentication

The shift towards cloud services brings with it unique challenges in implementing effective authentication strategies.

One of the primary challenges is the diverse and dynamic nature of cloud environments. Users access cloud services from various locations, devices, and networks, necessitating flexible yet secure authentication mechanisms that can adapt to different contexts without compromising security.

Moreover, the scalability of cloud services means that authentication mechanisms must be able to handle a large number of access requests without introducing significant latency or reducing the user experience. This requirement for scalability and user-friendliness often conflicts with the need for stringent security measures, creating a delicate balance that organizations must navigate.

D. Strategies for Strengthening Cloud Authentication

To address the challenges of cloud authentication and protect against sophisticated cyber actors, organizations can adopt several strategies:

- **Multi-Factor Authentication (MFA)**: MFA adds an extra layer of security by requiring users to provide two or more verification factors to gain access. This approach significantly reduces the risk of unauthorized access, as obtaining multiple authentication factors is considerably more difficult for attackers.
- **Adaptive Authentication**: Adaptive authentication mechanisms adjust the authentication requirements based on the context of the access request. Factors such as the user's location, device, and behavior can influence the authentication process, allowing for stricter controls in higher-risk scenarios.
- **Zero Trust Architecture**: Adopting a zero-trust approach to cloud security, where no user or system is trusted by default, can enhance the effectiveness of authentication. This model requires strict identity verification for every user and device trying to access resources, regardless of their location or network.
- **Use of Biometrics**: Biometric authentication methods, such as fingerprint scans or facial recognition, offer a high level of security by leveraging unique physical characteristics of users. These methods can be particularly effective in preventing unauthorized access in cloud environments.
- **Encryption of Authentication Data**: Ensuring that all authentication data is encrypted, both in transit and at rest, can protect against interception and misuse by attackers. This includes encryption of passwords, authentication tokens, and other sensitive information involved in the authentication process.

VI. Increased Importance of Initial Access

A. The Increased Importance of Initial Access in Cloud Security

The shift in focus by cyber actors to cloud services has brought the importance of securing initial access to the forefront of cybersecurity efforts. In cloud environments, initial access represents the critical juncture at which the security of the entire system is most vulnerable. Unlike traditional on-premises networks, where multiple layers of security can be deployed, cloud services are accessed over the internet, making the initial point of entry a prime target for attackers.

B. Initial Access as a Foothold for Attackers

Gaining initial access to cloud services allows attackers to establish a foothold within the target environment. From this position, they can potentially escalate privileges, move laterally across the network, and access sensitive data. The distributed nature of cloud services also means that compromising a single account can have far-reaching consequences, potentially giving attackers access to a wide array of resources and data.

C. Challenges in Securing Initial Access

- **Remote Access**: Cloud services are designed to be accessed remotely, which inherently increases the attack surface. Remote access points must be secured against unauthorized entry while still providing legitimate users with the necessary access.
- **Identity and Access Management (IAM)**: In cloud environments, IAM becomes a critical component of security. Organizations must ensure that IAM policies are robust and that permissions are granted based on the principle of least privilege to minimize the risk of initial access by unauthorized entities.
- **Phishing and Social Engineering**: Attackers often use phishing and social engineering tactics to gain initial access. These methods exploit human factors rather than technical vulnerabilities, making them difficult to defend against with traditional security measures.

D. Examples of Initial Access Techniques

- **Credential Stuffing**: This technique involves using previously breached username and password pairs to gain unauthorized access to accounts, banking on the likelihood that individuals reuse credentials across multiple services.
- **Exploiting Misconfigurations**: Cloud services can be complex to configure correctly, and attackers often exploit misconfigurations, such as open storage buckets or improperly set access controls, to gain initial access.
- **Compromising Third-Party Services**: Attackers may target third-party services that integrate with cloud environments, such as SaaS applications, to gain initial access to the cloud infrastructure.

E. Mitigating the Risks of Initial Access

- **Comprehensive Access Policies**: Establishing and enforcing comprehensive access policies can help control who has access to cloud resources and under what conditions.
- **Regular Audits and Reviews**: Conducting regular audits and reviews of access logs and permissions can help identify and rectify potential vulnerabilities before they are exploited.

- **Security Awareness Training**: Educating employees about the risks of phishing and social engineering can reduce the likelihood of credentials being compromised.
- **Endpoint Security**: Ensuring that all devices used to access cloud services are secure and up-to-date can prevent attackers from exploiting endpoint vulnerabilities to gain initial access.
- **Anomaly Detection**: Implementing anomaly detection systems can help identify unusual access patterns or login attempts that may indicate an attempted breach.

VII. Expansion of Targeting

A. *The Expansion of Targeting*

The strategic expansion of targeting by cyber actors to a broader range of sectors is a concerning development in the realm of global cybersecurity. This diversification of targets reflects a calculated approach by these actors to exploit the interconnected nature of modern industries and the increasing reliance on cloud services across various sectors.

B. *Broadening the Scope of Espionage*

The expansion into sectors such as aviation, education, law enforcement, local and state councils, government financial departments, and military organizations demonstrates their intent to gather intelligence from a wide spectrum of sources. This broad targeting strategy suggests that the is not only interested in traditional national security-related information but also in acquiring a diverse set of data that could provide economic, political, or technological advantages.

C. *Implications for Different Sectors*

- **Aviation**: The aviation industry involves a complex ecosystem of airlines, airports, manufacturers, and support services, all of which handle sensitive data related to national security, safety, and proprietary technology.
- **Education**: Universities and research institutions are rich sources of cutting-edge research and intellectual property. They are often targeted for their groundbreaking work in science, technology, and defense-related areas.
- **Law Enforcement**: Law enforcement agencies hold sensitive data on criminal investigations, national security matters, and personal information of citizens, making them a high-value target for espionage.
- **Local and State Councils**: Local and state government entities manage critical infrastructure, citizen services, and have access to vast amounts of personal data, which can be exploited for various malicious purposes.
- **Government Financial Departments**: These departments handle sensitive economic data and have insights into national financial strategies and policies, which can be valuable for foreign intelligence services.
- **Military Organizations:** Military targets are of high interest due to their strategic importance and access to classified information on defense capabilities, operations, and technologies.

D. *Challenges in Defending a Wide Range of Targets*

- **Diverse Security Postures:** Different sectors have varying levels of cybersecurity maturity and resources, making some more vulnerable to sophisticated cyber threats.
- **Interconnectedness:** The interconnected nature of these sectors means that a breach in one area can have cascading effects on others, as seen in supply chain attacks.

E. *Strategies for Mitigating Expanded Targeting Risks*

- **Sector-Specific Cybersecurity Frameworks:** Developing and implementing cybersecurity frameworks tailored to the unique needs and risks of each sector can enhance overall security.
- **Information Sharing:** Sharing threat intelligence and best practices within and between sectors can help organizations stay ahead of emerging threats and coordinate responses to incidents.
- **Regular Security Assessments:** Conducting regular security assessments and penetration testing can help organizations identify and address vulnerabilities before they are exploited.
- **Supply Chain Security:** Strengthening the security of the supply chain is critical, as attackers often target less secure elements within the supply chain to gain access to larger organizations.
- **Incident Response Planning:** Having a well-defined incident response plan can ensure that organizations are prepared to quickly and effectively respond to a breach.

VIII. Use of Service and Dormant Accounts

A. *The Use of Service and Dormant Accounts in Attacks*

The exploitation of service and dormant accounts by cyber actors represents a sophisticated and often overlooked vector of cyber-attacks. These accounts, which are created for various operational purposes within an organization's cloud and on-premises environments, can provide attackers with the access they need to carry out their objectives if not properly managed and secured.

B. *Understanding Service and Dormant Accounts*

Service accounts are specialized accounts used by applications or services to interact with the operating system or other services. They often have elevated privileges to perform specific tasks and may not be tied to an individual user's identity. Dormant accounts, on the other hand, are user accounts that are no longer actively used, either because the user has left the organization or the account's purpose has been fulfilled. These accounts are particularly risky because they are frequently forgotten, left with more privileges than necessary, and not monitored as closely as active user accounts.

C. *Why Service and Dormant Accounts Are Targeted*

- **Elevated Privileges**: Service accounts often have elevated privileges necessary for system tasks, which can be exploited to gain wide access to an organization's network.

- **Lack of Monitoring**: Dormant accounts are not regularly used, making them less likely to be monitored for suspicious activity, and thus an attractive target for attackers.
- **Weak or Default Credentials**: Service accounts may be configured with weak or default credentials that are easier for attackers to guess or find through brute force attacks.
- **Bypassing User Behavior Analytics**: Since service accounts perform automated tasks, their behavior patterns can be predictable, allowing malicious activities to blend in with normal operations and evade detection.

D. *The Threat Posed by Compromised Accounts*

- **Move Laterally**: Use the account's privileges to move laterally within the network, accessing other systems and data.
- **Escalate Privileges**: Leverage the account to escalate privileges and gain administrative access to critical systems.
- **Maintain Persistence**: Establish a persistent presence within the network, making it more difficult to detect and remove the attacker.
- **Exfiltrate Data**: Access and exfiltrate sensitive data, leading to data breaches and intellectual property theft.

E. *Mitigating the Risks Associated with Service and Dormant Accounts*

- **Regular Audits**: Conduct regular audits of all accounts to identify and deactivate dormant accounts and ensure that service accounts have the minimum necessary privileges.
- **Strong Authentication Controls**: Enforce strong password policies and use multi-factor authentication (MFA) for service accounts where possible.
- **Monitoring and Alerting**: Implement monitoring and alerting mechanisms to detect unusual activities associated with service and dormant accounts.
- **Segregation of Duties**: Apply the principle of segregation of duties to service accounts to limit the scope of access and reduce the risk of misuse.
- **Automated Management Tools**: Utilize automated account management tools to keep track of account usage and lifecycle, ensuring that accounts are deactivated when no longer needed.

IX. Sophistication of Cyber Actors

A. *The Sophistication of Cyber Operations*

The actors has demonstrated a high level of sophistication in its cyber operations, reflecting a deep understanding of the global cyber landscape and an ability to adapt and innovate in the face of evolving security measures. This sophistication is not only evident in the technical capabilities but also in their strategic approach to cyber espionage, which involves careful target selection, meticulous planning, and the use of advanced tactics, techniques, and procedures (TTPs).

B. *Technical Prowess and Innovation*

Cyber operations are characterized by the use of custom malware and zero-day vulnerabilities—previously unknown software vulnerabilities that haven't been disclosed to the software maker or the public. The exploitation of these vulnerabilities allows them to infiltrate target networks undetected. An example of this is the SolarWinds supply chain attack, where is believed to have compromised the software development process to insert malicious code into a software update, affecting thousands of SolarWinds' clients, including government agencies and Fortune 500 companies.

C. *Operational Security and Stealth*

Operational security (OpSec) is a hallmark of operations, with the agency going to great lengths to cover its tracks and maintain stealth within compromised networks. This includes the use of encrypted channels for exfiltrating data, the careful management of command-and-control servers to avoid detection, and the use of legitimate tools and services (a technique known as "living off the land") to blend in with normal network activity. The ability to maintain a low profile within target networks often allows them to conduct long-term espionage operations without detection.

D. *Psychological and Social Engineering Tactics*

Beyond technical capabilities, it has shown adeptness in psychological and social engineering tactics. These methods are designed to manipulate individuals into divulging sensitive information or performing actions that compromise security. Phishing campaigns, spear-phishing, and other forms of social engineering are frequently used to gain initial access to target networks or to escalate privileges once inside.

E. *Target Selection and Intelligence Gathering*

The target selection process is strategic and aligned with Russia's national interests. Targets are carefully chosen based on their potential to provide valuable intelligence, whether it be political, economic, technological, or military. Once a target is compromised, the actors focus on long-term access and intelligence gathering, prioritizing stealth and persistence over immediate gains. This approach allows them to collect a comprehensive picture of the target's activities, relationships, and plans.

F. *Adaptability to the Cybersecurity Landscape*

One of the most defining aspects is its adaptability. The shift towards targeting cloud services and exploiting service and dormant accounts is a testament to this adaptability. By continuously refining their methods and exploring new vectors of attack, the actors remain a persistent and evolving threat in the cyber domain.

X. Defense through Cybersecurity Fundamentals

A. *Defense through Cybersecurity Fundamentals in the APT*

In the contemporary cybersecurity landscape, marked by the sophisticated operations of actors, the importance of adhering to cybersecurity fundamentals cannot be overstated. While advanced threats continue to evolve, leveraging cutting-edge tactics, techniques, and procedures (TTPs), a strong foundation in cybersecurity fundamentals remains a critical line of defense

for organizations across all sectors. This foundational approach to cybersecurity emphasizes the implementation of best practices, policies, and controls that are designed to protect against a wide range of threats, including those from highly sophisticated adversaries.

B. *Understanding Cybersecurity Fundamentals*

- **Access Control**: Ensuring that only authorized users have access to information systems and data, and that they are only able to perform actions that are necessary for their role.
- **Data Encryption**: Protecting data at rest and in transit through encryption, making it unreadable to unauthorized users.
- **Patch Management**: Regularly updating software and systems to address vulnerabilities and reduce the risk of exploitation.
- **Firewalls and Intrusion Detection Systems (IDS)**: Implementing firewalls to block unauthorized access and IDS to monitor network traffic for suspicious activity.
- **Multi-Factor Authentication (MFA)**: Requiring users to provide two or more verification factors to gain access to systems, significantly enhancing security.
- **Security Awareness Training**: Educating employees about cybersecurity risks and best practices to prevent social engineering attacks and other threats.
- **Incident Response Planning**: Preparing for potential security incidents with a well-defined plan for response and recovery.

C. *The Role of Fundamentals in Defending Against Sophisticated Threats*

While sophisticated cyber actors like the actors employ advanced techniques to bypass security measures, many of their strategies still exploit basic security weaknesses—such as poor password management, unpatched software, and insufficient access controls. By adhering to cybersecurity fundamentals, organizations can address these vulnerabilities, making it significantly more difficult for attackers to gain initial access or move laterally within a network.

For example, the implementation of MFA can prevent unauthorized access even if credentials are compromised. Regular patch management can close off vulnerabilities before they can be exploited in a zero-day attack. Security awareness training can reduce the risk of employees falling victim to phishing or other social engineering tactics.

D. *Challenges in Maintaining Cybersecurity Fundamentals*

Despite the clear benefits, maintaining a strong foundation in cybersecurity fundamentals can be challenging for organizations. This can be due to a variety of factors, including resource constraints, the complexity of modern IT environments, and the rapid pace of technological change. Additionally, as organizations increasingly adopt cloud services and other advanced technologies, the cybersecurity landscape becomes more complex, requiring continuous adaptation of fundamental security practices.

E. *Strategies for Strengthening Fundamental Defenses*

- **Continuous Risk Assessment**: Regularly assessing the organization's security posture to identify vulnerabilities and prioritize remediation efforts.
- **Leveraging Security Frameworks**: Adopting comprehensive security frameworks, such as the NIST Cybersecurity Framework, to guide the implementation of best practices and controls.
- **Automating Security Processes**: Utilizing automation to streamline security processes, such as patch management and monitoring, to enhance efficiency and effectiveness.
- **Fostering a Culture of Security**: Building a strong security culture within the organization, where cybersecurity is viewed as a shared responsibility among all employees.
- **Collaboration and Information** Sharing: Engaging in collaboration and information sharing with industry peers and government agencies to stay informed about emerging threats and best practices.

XI. Mitigations to Strengthen Defense

A. *Mitigations to Strengthen Defense Against APT*

In the context of heightened cyber threats from sophisticated actors, organizations must employ a comprehensive set of mitigations to strengthen their defenses. These mitigations are designed to address vulnerabilities across various aspects of an organization's infrastructure and operations, thereby reducing the risk of successful cyber-attacks. Implementing these mitigations requires a strategic approach that encompasses both technical solutions and organizational processes.

B. *Key Mitigation Strategies*

- **Implement Multi-Factor Authentication (MFA)**: MFA is one of the most effective controls for securing user accounts against compromise. By requiring multiple forms of verification, MFA makes it significantly more difficult for attackers to gain unauthorized access, even if they have obtained a user's credentials.
- **Regular Patching and Updates**: Keeping software and systems up to date with the latest patches is crucial for closing security gaps that could be exploited by attackers. A regular patch management process should be established to ensure timely application of updates.
- **Network Segmentation**: Dividing the network into smaller, controlled segments can limit an attacker's ability to move laterally within the network and access sensitive areas. Segmentation also helps contain potential breaches to a smaller subset of the network.
- **Endpoint Protection**: Deploying advanced endpoint protection solutions can help detect and prevent malicious activities on devices that access the organization's network. This includes the use of antivirus software, host-based intrusion prevention systems, and endpoint detection and response (EDR) tools.

- **Security Awareness Training**: Educating employees about cybersecurity risks and best practices is essential for preventing social engineering attacks, such as phishing. Regular training can help create a culture of security awareness within the organization.
- **Least Privilege Access Control**: Ensuring that users have only the access rights necessary for their role helps minimize the potential impact of account compromise. Access controls should be regularly reviewed and adjusted as necessary.
- **IR Planning**: Having a well-defined and tested incident response plan enables organizations to respond quickly and effectively to security incidents, minimizing damage and restoring operations as soon as possible.
- **Continuous Monitoring and Detection**: Implementing continuous monitoring and detection capabilities can help identify suspicious activities early on. This includes the use of security information and event management (SIEM) systems, intrusion detection systems (IDS), and network traffic analysis.
- **Secure Configuration and Hardening**: Systems should be securely configured and hardened against attacks. This involves disabling unnecessary services, applying secure configuration settings, and ensuring that security features are enabled.
- **Backup and Recovery**: Regular backups of critical data and systems, along with robust recovery procedures, are essential for resilience against ransomware and other destructive attacks. Backups should be tested regularly to ensure they can be relied upon in an emergency.

C. *Challenges in Implementing Mitigations*

While these mitigations are effective in theory, organizations often face challenges in their implementation. These challenges can include limited resources, the complexity of IT environments, the need for specialized skills, and the difficulty of balancing security with business requirements. Additionally, the rapidly evolving nature of cyber threats means that mitigation strategies must be continually reassessed and updated.

D. *Collaborative Efforts and Information Sharing*

To overcome these challenges and enhance the effectiveness of mitigations, organizations can engage in collaborative efforts and information sharing with industry partners, government agencies, and cybersecurity communities. This collaboration can provide access to shared knowledge, threat intelligence, and best practices that can inform and improve an organization's mitigation efforts.

XII. Benefits and Drawbacks of NSA's Advisory

A. *Benefits:*

- **Awareness and Understanding**: The document raises awareness about the shift in tactics towards cloud services, which is crucial for organizations to understand the current threat landscape.
- **Detailed TTPs**: It provides detailed information on the tactics, techniques, and procedures (TTPs) used by actors, including the use of service and dormant accounts, which can help organizations identify potential threats and vulnerabilities.
- **Sector-Specific Insights**: The document outlines the expansion of targeting to sectors such as aviation, education, law enforcement, and military organizations, offering sector-specific insights that can help these industries bolster their defenses.
- **Mitigation Strategies**: It offers practical mitigation strategies that organizations can implement to strengthen their defenses against initial access by actors, such as implementing MFA and managing system accounts.
- **Emphasis on Fundamentals**: The advisory emphasizes the importance of cybersecurity fundamentals, which can help organizations establish a strong baseline defense against sophisticated actors.
- **Global Supply Chain Relevance**: The document references the actors' involvement in the SolarWinds supply chain compromise, highlighting the global implications of such cyber espionage activities.

B. *Drawbacks:*

- **Resource Intensity**: Implementing the recommended mitigations may require significant resources, which could be challenging for smaller organizations with limited cybersecurity budgets and personnel.
- **Complexity of Cloud Security**: The document points out the inherent challenges in securing cloud infrastructure, which may require specialized knowledge and skills that not all organizations possess.
- **Evolving Tactics**: While the document provides current TTPs, the actors' tactics are constantly evolving, which means that defenses based solely on this advisory may quickly become outdated.
- **Potential for Overemphasis on Specific Threats**: Focusing too much on such actors could lead organizations to neglect other threat actors or vectors that are equally dangerous but not covered in the document.
- **Shared Responsibility Model**: The document implies a shared responsibility model for cloud security, which may lead to confusion about the division of security responsibilities between cloud providers and customers.
- **False Sense of Security**: Organizations might develop a false sense of security by relying on the mitigations suggested, without considering the need for a dynamic and adaptive security posture to respond to new threats.