Blog Threat Labs Cloud Threats Memo: Analyzing the Top 10 Initial Access Vectors By Paolo Passeri May 19 2022

_Share

Cloud Threats Memo: Analyzing the Top 10 Initial Access Vectors

A joint security advisory by the national cybersecurity agencies of the United States, Canada, New Zealand, the Netherlands, and the United Kingdom has identified the top 10 initial access vectors routinely exploited by threat actors to break into an organization.

Initial access brokers are emerging figures in the cyber criminal ecosystem, and their work is fueling a plethora of targeted ransomware attacks that have characterized the last few months' cyber attacks. The business model is pretty straightforward: poor security controls are routinely exploited by the initial access brokers and the resulting compromised credentials are sold or outsourced, generating a recurring revenue model. Similarly, buyers can focus their efforts on the execution rather than the initial access. A win-win situation for all the threat actors involved.

According to Alert (AA22-137A), the top routinely exploited weak security controls are:

- Multi-factor authentication (MFA) is not enforced
- Incorrectly applied privileges or permissions and errors within access control lists
- Software is not up to date
- Use of vendor-supplied default configurations or default login usernames and passwords
- Remote services, such as a virtual private network (VPN), lack sufficient controls to prevent unauthorized access
- Strong password policies are not implemented
- Cloud services are unprotected
- Open ports and misconfigured services are exposed to the internet
- Failure to detect or block phishing attempts
- Poor endpoint detection and response

The list is quite extensive and while some of the initial access vectors are quite obvious (such as unpatched software or poor endpoint detection and response), others are typical of the new era driven by cloud services and quickly becoming familiar to us: Unprotected or misconfigured cloud services, open ports exposed to the internet, or even the lack of multi-factor authentication for cloud accounts (a survey conducted in 2020 revealed that 78% of Microsoft365 administrators did not have multi-factor authentication enabled, and it looks like not much has changed since then). Others are more surprising, such as the lack of sufficient controls by traditional VPNs.

The first access control recommendation provided by the advisory is the adoption of a zero trust security model. Other recommendations include the implementation of credential hardening, a centralized log management infrastructure, an effective antivirus architecture, the adoption of tools to detect exploits and vulnerabilities at the endpoint, network, and infrastructure level, and finally a rigorous configuration and patching management program.

How Netskope mitigates the initial access vectors.

Despite the fact that the vectors outlined above affect multiple elements of the infrastructure, the following Netskope solutions can mitigate the risks related to remote access, exposed or misconfigured cloud services, and phishing.

Netskope Private Access (NPA) is Netskope's answer to the recommendation of adopting a zero trust security model. NPA allows you to publish resources in a simple and secure manner providing a zero trust alternative to legacy remote access technologies and preventing the direct exposure of services like SMB, RDP, or SSH, whether they are located in a local data center, or in a private or public cloud. NPA can also perform a check on the security posture of the endpoint before accessing the target application, overcoming the limitations of legacy remote access technologies. NPA mitigates several risks in the top 10, including the lack of controls in traditional VPNs, cloud services left unprotected, or open ports and misconfigured services exposed to the internet.

Netskope Public Cloud Security detects misconfigurations in IaaS environments, such as AWS, Azure, and Google Cloud Platform, which can be exploited by bad actors. A set of predefined profiles allows users to comply with best practice and industry standards such as NIST CSF, PCI-DSS, and CIS. Additionally, it is possible to easily build custom rules with a Domain Specific Language. The same protection is also available for SaaS applications (such as Microsoft 365, Salesforce, GitHub, Zoom, and ServiceNow) thanks to the new SSPM (SaaS Security Posture Management) module that allows administrators to make sure that multi-factor authentication is enabled for all Microsoft 365 users (for example).

The Netskope Next Gen SWG can reduce the phishing attack surface thanks to the following features:

- The content filtering engine offers 16 granular security risk categories, including phishing and malware distribution points.
- It is possible to enforce granular controls to thousands of unmanaged cloud services, differentiating corporate and non-corporate instances.
- Netskope Threat Protection offers multiple engines including signature-based AV, advanced heuristics, sandboxing, and a ML-based scanner for malicious documents and executables.
- The Cloud Exchange, a component of Netskope Cloud Exchange improves attack neutralization via bi-directional automated IoC sharing (hashes, IPs, domains, and URLs) with third-parties such as EDR technologies and threat intelligence feeds.

Finally, Netskope Advanced Analytics provides specific dashboards to assess the risk of cloud misconfigurations, with rich details and insights, supporting the security teams in the remediation process.

Stay safe!

< Threat Labs Next Story > < Back Next >

About the author Paolo supports Netskope's customers in protecting their journey to the cloud and is a security professional, with 20+ years experience in the infosec industry. He is the mastermind behind hackmageddon.com, a blog detailing timelines and statistics of all the main cyber-attacks occurred since 2011. It is the primary source of data and trends of the threat landscape for the Infosec community. Paolo supports Netskope's customers in protecting their journey to the cloud and is a security professional, with 20+ years experience in the infosec industry. He is the mastermind behind hackmageddon.com, a blog detailing timelines and statistics of all the main cyber-attacks occurred since 2011. It is the primary source of… Read Paolo Passeri's full Bio > More Articles by Paolo Passeri > Read full Bio > More articles >
Related ArticlesThreat Labs By Gustavo Palazolo RedLine Stealer Campaign Using Binance Mystery Box Videos to Spread GitHub-Hosted Payload

Read articleThreat Labs By Gustavo Palazolo Emotet: New Delivery Mechanism to Bypass VBA Protection

Read articleThreat Labs By Paolo Passeri Cloud Threats Memo: What We Can Learn From the Top 15 Routinely Exploited Threats of 2021

Read article Load More

Articles Contact UsContact Us

We'd love to hear from you!

Loading...