TIR-20260617 Before Ransomware: Understanding Initial Access Brokers

6/17/2026

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

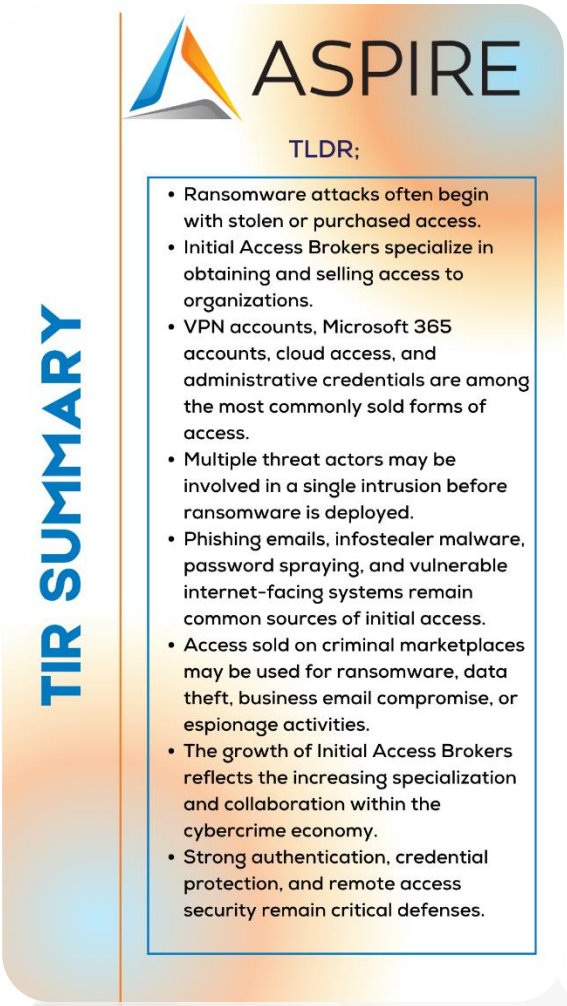
Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary

When a ransomware attack makes headlines, most people focus on the group responsible for encrypting systems or demanding payment. What is often overlooked is everything that happened beforehand. In many cases, the ransomware group was not responsible for gaining access to the victim's environment. The intrusion may have started weeks or even months earlier when credentials were stolen or unauthorized access was sold to another threat actor. By the time ransomware is deployed, multiple threat actors may have already been involved.

One group may steal credentials through phishing, infostealer malware, password spraying, or the exploitation of an internet-facing application. Rather than using that access themselves, they may verify that it works and offer it for sale on the dark web. These threat actors are known as Initial Access Brokers. Their customers may include ransomware affiliates, data theft groups, financial crime actors, or nation-state operators looking for a foothold inside a target organization. Access can take many forms, including VPN credentials, Microsoft 365 accounts, remote desktop access, cloud environments, or privileged administrative accounts.



This business model has transformed how many cyberattacks happen. As a result, organizations are not only defending against ransomware groups or phishing campaigns. They are also defending against a growing marketplace of threat actors whose sole purpose is to gain and sell access to corporate networks. Understanding how access is obtained and used can help organizations identify security gaps before they become a larger problem.

Initial Access

Initial access occurs when a threat actor gains unauthorized access to an organization's systems or accounts. It is often the starting point for data theft, ransomware attacks, and other malicious activity.

Many people picture hackers breaking through sophisticated security controls to gain entry into a network. While that does happen, initial access is often obtained through much simpler methods. Initial access can be obtained in several ways. Phishing emails may capture credentials, infostealer malware may expose saved passwords, and password spraying may provide access to VPN or cloud accounts. Attackers also routinely target vulnerable internet-facing systems.

Initial Access Brokers and Ransomware Attacks

Ransomware attacks rarely begin with ransomware. Before systems are encrypted, attackers often spend time learning about the environment they have accessed. They may identify critical servers, locate sensitive data, review backup systems, or search for accounts with elevated privileges. In many cases, the group deploying the ransomware is not the group that gained access to the environment.

Some threat actors specialize in obtaining and selling access to organizations. These actors are known as Initial Access Brokers (IABs). They obtain access through methods such as phishing, credential theft, password spraying, or vulnerability exploitation and then sell that access to other threat actors.

Access may be advertised on criminal forums or sold through private channels. Buyers may include ransomware affiliates, data theft groups, financial crime actors, or other threat actors looking for a foothold inside a target environment. The Initial Access Broker's profit comes from selling access rather than conducting the final attack.

The value of the access depends on what it provides. Access to a standard user account may have limited usefulness, while access to a cloud environment or domain administrator account can provide broad control over an organization's systems.

Common types of access sold by Initial Access Brokers include:

- VPN credentials that provide remote access to the corporate network
- Microsoft 365 or Google Workspace accounts
- Remote Desktop Protocol (RDP) access

- Citrix and virtual desktop environments
- Microsoft Entra ID accounts
- Active Directory user accounts
- Domain administrator credentials
- AWS, Azure, or Google Cloud access
- Remote management and monitoring platforms used by IT teams
- Administrative accounts with elevated privileges

For ransomware groups and other threat actors, purchasing access can provide a direct path into a target environment. The ransomware deployment often occurs after access has already been established.

How Threat Actors Obtain Access

Despite the attention given to software vulnerabilities and zero-days, many successful intrusions still begin with stolen credentials, phishing emails, infostealer malware, or weak passwords.

Phishing Emails

Phishing remains one of the most common ways attackers obtain access to organizations. These emails are designed to convince users to click a malicious link, open an attachment, or provide credentials through a fake login page. Modern phishing campaigns often impersonate trusted companies, coworkers, suppliers, or cloud service providers to increase the likelihood that a user will interact with the message.

Once credentials are obtained, attackers may use them to access email accounts, VPNs, cloud services, and other business applications. In some cases, phishing emails are also used to deliver malware. Despite years of security awareness training, phishing remains one of the most common ways attackers gain access to organizations.

Infostealer Malware

Infostealers are a category of malware designed to collect information from infected devices. Rather than encrypting files or disrupting operations, these programs focus on gathering data that can be used or sold later. Common targets include saved browser

passwords, session cookies, cryptocurrency wallets, authentication tokens, autofill data, and browser history.

Infostealers have become a common source of stolen credentials used in ransomware attacks. Credentials collected from infected devices are frequently sold on criminal marketplaces, purchased by other threat actors, and used to access corporate environments.

Weak and Reused Passwords

Password reuse continues to create opportunities for attackers. Many individuals use the same password across multiple personal and professional accounts. When a third-party website suffers a breach, those credentials often become available on criminal forums and credential marketplaces.

Attackers frequently use credential stuffing techniques to test previously exposed usernames and passwords against VPN portals, Microsoft 365 environments, cloud applications, and other services. Even if the original breach had nothing to do with the targeted organization, password reuse can allow attackers to gain access using valid credentials. This approach requires little technical skill and is effective because many users continue to reuse passwords across multiple platforms.

Password Spraying

Unlike traditional brute-force attacks that target a single account with numerous password attempts, password spraying focuses on many accounts using a small number of commonly used passwords. This technique helps attackers avoid account lockouts while increasing the likelihood of success.

Threat actors often target internet-facing services such as Microsoft 365, VPN portals, and remote access platforms. If users select weak or predictable passwords, attackers may gain access without exploiting a vulnerability or delivering malware. Nation-state actors, ransomware groups, and financially motivated cybercriminals have all been observed using password spraying as an initial access technique.

Exploitation of Internet-Facing Applications

Organizations frequently expose applications and services to the internet to support remote work, customer access, and business operations. These systems may include VPN appliances, firewalls, web applications, remote management platforms, and cloud

services. When vulnerabilities exist and patches are not applied in time, attackers may exploit those weaknesses to gain access.

Internet-facing systems are a common target for threat actors. VPN appliances, Microsoft Exchange servers, remote access platforms, and edge devices are frequently targeted because they can provide direct access to an organization's environment. After gaining access, attackers often establish persistence or look for additional opportunities to expand their access.

MFA Fatigue Attacks

Multi-factor authentication is one of the most effective defenses against account compromise. However, attackers have adapted their tactics to target the user rather than the technology itself. One increasingly common technique is known as MFA fatigue.

In an MFA fatigue attack, a threat actor first obtains valid credentials through phishing, infostealer malware, or another method. The attacker then repeatedly attempts to log in, generating a stream of authentication prompts on the victim's device. The goal is to frustrate or confuse the user into approving one of the requests. Threat groups such as Scattered Spider have successfully used this technique during high-profile attacks. Once a request is approved, the attacker gains access to the account and can begin additional activity within the environment.

Token Theft and Device Code Phishing

As organizations have moved more services to the cloud, attackers have adapted their tactics. In addition to targeting usernames and passwords, they now target authentication tokens. These tokens allow users to remain signed in to applications without repeatedly entering credentials. If a token is stolen, an attacker may be able to access the account without needing the user's password.

Recent phishing campaigns have shown how attackers can obtain Microsoft 365 access tokens by abusing legitimate authentication processes. Rather than delivering malware, these campaigns rely on social engineering and legitimate Microsoft services. Because the login activity appears to come from a valid user session, it can be more difficult to detect than a traditional credential theft attack.

Whether the goal is a password, authentication token, or VPN account, the objective is to gain access to the target environment.

THE BUSINESS OF SELLING ACCESS

Not every threat actor is interested in deploying ransomware or stealing data. Some make money by gaining access to organizations and selling that access to other criminals. In many cases, the group responsible for the final attack is not the group that originally gained entry into the environment.

The value of access depends on what it provides. Access to a standard user account may have limited value, while access to a cloud environment, remote management platform, or domain administrator account can provide broad control over an organization's systems. As a result, higher levels of access typically command higher prices. Underground criminal marketplace listings often include information about the target organization, such as its industry, geographic location, annual revenue, and type of access available. This helps buyers determine whether the target aligns with their objectives.

Organizations in healthcare, government, financial services, manufacturing, and technology sectors are frequently advertised because they often possess valuable data and critical business operations.

Commonly advertised access includes:

- VPN credentials
- Microsoft 365 accounts
- Remote Desktop Protocol (RDP) access
- Citrix environments
- Domain administrator accounts
- Microsoft Azure, AWS, and Google Cloud access
- Remote management and monitoring platforms
- Corporate email accounts

Known Initial Access Brokers:

- Scattered Spider
- UNC961 (also known as Gold Melody and Prophet Spider)
- Interlock (also known as LaZagne, Hive0163, and Oyster)
- Ex-Conti Affiliates and TrickBot Clusters

Recent Attacks

MGM Resorts International

MGM Resorts was hit by a major cyberattack in September 2023 that affected hotel operations, reservations, and payment systems. The attack was attributed to Scattered Spider, which has a history of targeting user accounts and authentication processes to gain access to organizations.

The attackers impersonated an employee and persuaded MGM's help desk to reset account credentials. That access allowed them to enter the environment and move further into MGM's systems. The attack illustrates how a single compromised account can become the starting point for a much larger intrusion. It also shows why access to corporate accounts and identity systems is highly sought after by threat actors.

Colonial Pipeline

In May 2021, Colonial Pipeline suffered a ransomware attack attributed to the DarkSide ransomware group. The incident led to the temporary shutdown of pipeline operations that supplied fuel across portions of the eastern United States. The disruption contributed to fuel shortages in multiple states and brought national attention to the impact cyberattacks can have on critical infrastructure.

The attackers gained access through a VPN account that was no longer being used. The account was protected by a password and did not have multi-factor authentication enabled. Although there is no evidence that the access was purchased from an Initial Access Broker, the incident highlights why VPN credentials continue to be bought and sold within criminal marketplaces. A valid VPN account can provide direct access to an organization's environment without requiring malware or the exploitation of a software vulnerability.

What These Incidents Have in Common

Both incidents began with access to a legitimate account. The ransomware was not the first step. Whether access is obtained through social engineering, stolen credentials, infostealer malware, or criminal marketplaces, gaining entry into an organization remains one of the most important stages of an intrusion.

CONCLUSION

One of the most significant changes in cybercrime over the past several years has been the separation of duties among threat actors. Access brokers, ransomware affiliates, data theft groups, and other criminal actors often play different roles in the same attack. Understanding how the cybercrime economy operates can help organizations better understand how modern attacks develop and where opportunities exist to disrupt them.

RECOMMENDATIONS

Threat actors are often successful because they find weaknesses that have been overlooked. Addressing common entry points can make it more difficult for attackers to gain access and move forward with an attack.

- **Require** multi-factor authentication (MFA) for all remote access services, including VPNs, Microsoft 365, cloud platforms, and administrative accounts.
- **Implement** phishing-resistant authentication methods such as passkeys, FIDO2 security keys, or number matching where supported.
- **Disable** dormant accounts that are no longer needed and regularly review user accounts for unnecessary privileges.
- **Enforce** strong password policies and prohibit password reuse across corporate systems and applications.
- **Monitor** for exposed employee credentials and investigate accounts that appear in public breaches or credential marketplaces.
- **Patch** internet-facing systems promptly, particularly VPN appliances, firewalls, remote access platforms, and web applications.
- **Review** and monitor remote access services for unusual login activity.
- **Provide** regular security awareness training focused on phishing attempts and suspicious authentication requests.
- **Monitor** authentication logs for password spraying, credential stuffing, and repeated failed login attempts.

There is no single control that prevents every intrusion. A layered approach can make it more difficult for threat actors to obtain and use access successfully.

MITRE MAP

***Note**: These TTPs are the most relevant to initial access brokers.*

Initial Access	T1566 – Phishing T1190 – Exploit Public-Facing Application T1133 – External Remote Services (VPN, RDP, etc.)
Credential Access	T1110.003 – Password Spraying T1555 – Credentials from Password Stores T1621 – Multi-Factor Authentication Request Generation
Defense Evasion	T1078 – Valid Accounts T1078.004 – Valid Accounts: Cloud Accounts
Command and Control	T1219 – Remote Access Software (RMM Tools)

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.

- Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

SUPPORTING DOCUMENTATION

From URLs to Malware: How Threat Actors Abuse Domain Name Security in 2025

Protecting Against Malicious Use of Remote Monitoring and Management Software | CISA

FBI warns about PhaaS platform used to access Microsoft 365 environments | Cybersecurity Dive

Understanding Initial Access Exploits | Blog | VulnCheck

Biggest Cyber Attack Vectors | Arctic Wolf

Initial Access Vectors for Ransomware Cases - Surefire Cyber

How Initial Access Brokers Lead to Ransomware | Proofpoint US

Initial Access Brokers have Shifted to High-Value Targets and Premium Pricing

How Do Initial Access Brokers Enable Ransomware Attacks?

From Stealers to Systems: The New Model of Credential Theft | Trend Micro (US)

What Is an Infostealer? How Credential-Stealing Malware Works

Initial access techniques used by Iran-based threat actors | SOPHOS

GOLD MELODY: Profile of an Initial Access Broker

Disrupting Initial Access Brokers: Best Practices and Future Trends

Access Brokers: Their Targets and Their Worth | CrowdStrike

Stolen Credentials and Valid Account Abuse Remain Integral to Financially Motivated Intrusions | FortiGuard Labs

Initial Access in Cybersecurity: The Attack Stage Most Businesses Miss | Huntress

What Are Initial Access Brokers? - A Comprehensive Guide 101

Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®

The Missing Link: How Infostealers Fuel Ransomware Attacks (and Our New Partnership with Ransomware.live) | InfoStealers

What Is Access Control & How Crucial Is It to Cybersecurity? | Okta

What is Access Control? Types, Importance & Best Practices

10 ways attackers gain access to networks

Access Brokers: Their Pivotal Role in Cybercrime...

How to Stop Infostealers and Next-Gen Ransomware with an Identity-Centric Security Approach - Cyber Defense Magazine

Dark web vendors are selling remote access to corporate PCs for as little as $3 | ZDNET

Prevent Credential Stuffing: How to Protect VPNs & Remote Access

FortiBleed leak exposes Fortinet VPN credentials for 73,000 devices.

Investigating the Emerging Access-as-a-Service Market | Trend Micro (US)

How Threat Actors Are Selling Access to Corporate Networks

FBI links First VPN Service to ransomware gangs, botnets, criminal dark web activity; calls for layered defensive controls - Industrial Cyber

Why VPN Users Are Prime Targets Without Dark Web Monitoring

Understanding MFA fatigue attacks: How they work and how to defend against them — WorkOS

Strengthening authentication with passkeys: A CISO playbook | SOPHOS

Multi-Factor Authentication Request Generation, Technique T1621 - Enterprise | MITRE ATT&CK®

Understanding and Protecting Against Infostealer Malware: A Comprehensive Guide | Flashpoint

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.