Exponential Token Propagation Attack (ETPA)

Author: Anthony Terrano
Attack Class: Token Abuse / Identity Propagation
Severity (Conceptual): High
Attack Vector: Network
Privileges Required: Low (valid user account)
User Interaction: Required
Scope: Changed
Impact: Confidentiality, Integrity

Overview

The **Exponential Token Propagation Attack (ETPA)** is an identity-based attack pattern targeting cloud collaboration platforms that leverage OAuth authentication and external file-sharing workflows, such as **Microsoft 365 SharePoint Online and OneDrive**.

ETPA begins with the compromise of a single user account and abuses **legitimate SharePoint sharing operations**, **OAuth token behavior**, and **Exchange mailbox rules** to propagate access across additional accounts. Each successful interaction creates new opportunities for compromise, resulting in **exponential growth** without exploiting a traditional software vulnerability or deploying malware.

Because the attack relies on valid tokens, trusted domains, and normal collaboration features, it is difficult to detect using signature-based or IOC-driven security controls.

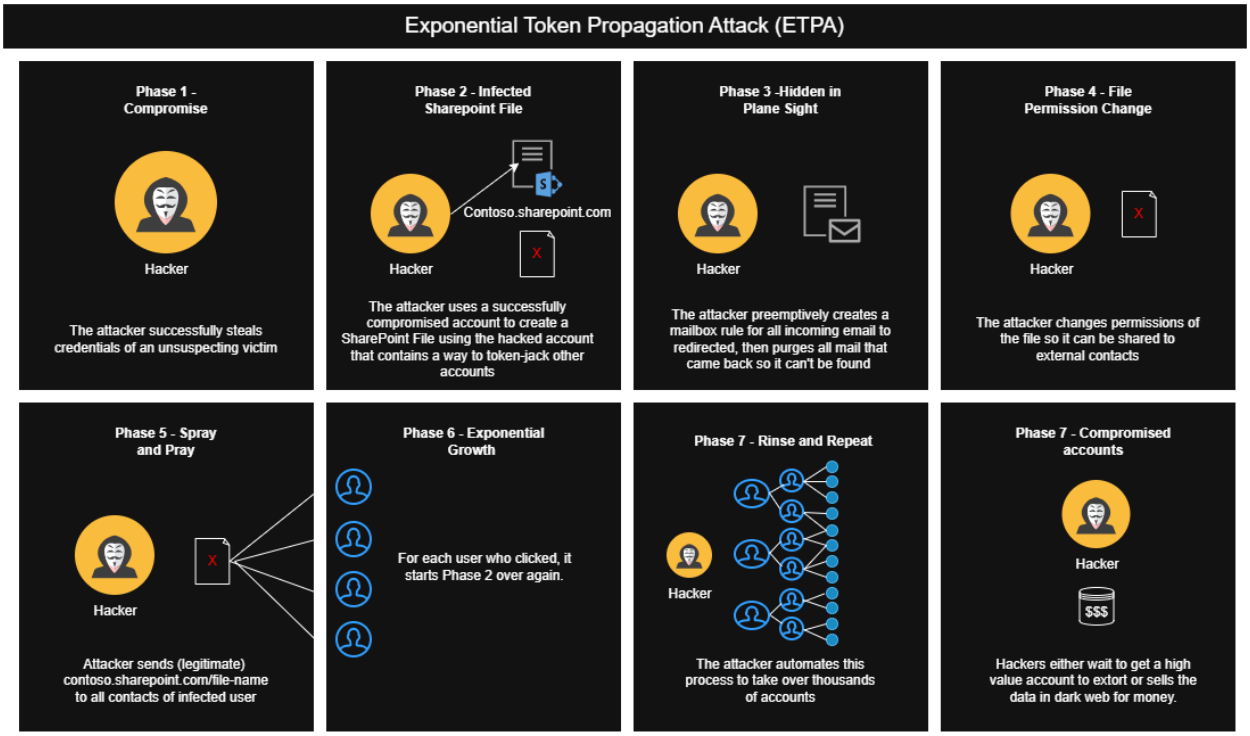
Key Characteristics

- No malware required
- No software vulnerability exploited
- Uses trusted Microsoft 365 services
- Blends into normal user activity
- Enables exponential account compromise
- Can spread cross-tenant and supply-chain style

Attack Flow Summary

1. Initial user account compromise
2. Malicious SharePoint file or link creation
3. Mailbox rule manipulation to suppress detection
4. Permission changes enabling external sharing
5. Legitimate sharing links sent to contacts
6. Each interaction compromises additional accounts
7. Automated repetition at scale

Attack Phases (Detailed)



Phase 1 – Compromise

The attacker obtains valid credentials or authentication tokens through phishing, token theft, session hijacking, or prior compromise.

Phase 2 – Infected SharePoint File Creation

The attacker creates or modifies a SharePoint or OneDrive file containing a malicious mechanism designed to capture or reuse authentication tokens when accessed by other users.

The file is hosted within the tenant, increasing trust and legitimacy.

Phase 3 – Hidden in Plain Sight (Mailbox Rule Abuse)

Mailbox rules are created to:

- Redirect inbound email
- Auto-delete messages
- Suppress sharing notifications or security alerts

This prevents the victim from noticing abnormal activity.

Phase 4 – File Permission Change

The attacker modifies file permissions to:

- Allow external sharing
- Broaden recipient access
- Enable secure sharing links

Phase 5 – Spray and Pray

Legitimate SharePoint sharing links (e.g., contoso.sharepoint.com/…) are sent to all contacts of the compromised user.

Because the links originate from trusted domains and trusted senders, recipients are more likely to interact with them.

Phase 6 – Exponential Growth

Each user who interacts with the shared file becomes compromised, restarting the attack chain at Phase 2.

This creates exponential propagation across users and tenants.

Phase 7 – Rinse and Repeat (Automation)

The attacker automates this process to compromise thousands of accounts with minimal infrastructure.

Phase 8 – Post-Compromise Activity

Once sufficient scale or high-value accounts are obtained, attackers may:

- Monitor email and documents
- Exfiltrate sensitive data
- Perform extortion or ransomware operations
- Sell access or data on underground markets

Impact

- Large-scale account compromise
- Persistent access via OAuth tokens
- Unauthorized data access and exfiltration
- Abuse of trusted collaboration platforms
- Difficult detection and attribution

Affected Systems

- Microsoft 365
    - SharePoint Online
    - OneDrive
    - Exchange Online
- Any SaaS platform using:

    - OAuth tokens
    - External file sharing
    - Trust-based collaboration workflows

Microsoft Audit Log Indicators

The following indicators map directly to **Microsoft Purview / Unified Audit Log** events.

Phase 1 – Compromise

Indicators

- UserLoggedIn
- Entra ID SignInLogs with:
    - Unfamiliar IP addresses
    - Impossible travel
    - Token-based sign-ins without MFA

Phase 2 – Infected File Creation

Operations

- SharePointFileOperation
    - FileCreated
    - FileModified
    - FileModifiedExtended

Fields to Monitor

- SiteUrl
- SourceFileName
- ClientIP
- UserAgent

Phase 3 – Mailbox Rule Abuse

Operations

- New-InboxRule
- Set-InboxRule

Red Flags

- Rules that delete mail
- Rules that redirect mail externally
- Rules matching keywords such as:
    - shared
    - access
    - security
    - Microsoft

Phase 4 – File Permission Changes

Operations

- SharePointSharingOperation
    - SharingLinkCreated
    - AddedToSharingLink
    - UserAddedToSecureLink

Indicators

- Multiple permission changes in short timeframes
- External users added
- Sharing immediately after file creation

Phase 5 – Spray and Pray

Patterns

- Same file shared with many recipients
- External recipients added rapidly
- Same ClientIP and timestamp clusters

Phase 6 – Exponential Growth

Correlated Indicators

- Multiple users performing identical sharing actions
- Similar file names or link structures
- Repeating patterns every few minutes or hours

Detection should pivot from single-user alerts to **behavioral correlation**.

Phase 7 – Automation Indicators

- High-frequency sharing operations
- Inbox rule creation across many users
- Reused IP ranges or automation fingerprints

Phase 8 – Post-Compromise Indicators

- FileAccessed
- FileDownloaded
- SearchQueryPerformed
- Long-lived token activity without interactive logins

Classification

- **Attack Type:** Token Abuse / Identity Propagation
- **MITRE ATT&CK Techniques**

    - Valid Accounts (T1078)
    - Token Impersonation / Theft
    - Lateral Movement via Trusted Relationships
- **CWE (Conceptual):** Improper Authentication Token Handling