C0027, Campaign C0027 | MITRE ATT&CK®

Archived: 2026-04-05 14:15:53 UTC

Enterprise T1087 .003 Account Discovery: Email Account

During C0027, Scattered Spider accessed Azure AD to identify email addresses.[1]

.004 Account Discovery: Cloud Account

During C0027, Scattered Spider accessed Azure AD to download bulk lists of group members and to identify privileged users, along with the email addresses and AD attributes.[1]

Enterprise T1098 .001 Account Manipulation: Additional Cloud Credentials

During C0027, Scattered Spider used aws_consoler to create temporary federated credentials for fake users in order to obfuscate which AWS credential is compromised and enable pivoting from the AWS CLI to console sessions without MFA.[1]

.003 Account Manipulation: Additional Cloud Roles

During C0027, Scattered Spider used IAM manipulation to gain persistence and to assume or elevate privileges.[1]

.005 Account Manipulation: Device Registration

During C0027, Scattered Spider registered devices for MFA to maintain persistence through victims' VPN.[1]

Enterprise T1530 Data from Cloud Storage

During C0027, Scattered Spider accessed victim OneDrive environments to search for VPN and MFA enrollment information, help desk instructions, and new hire guides.[1]

Enterprise T1213 .002 Data from Information Repositories: Sharepoint

During C0027, Scattered Spider accessed victim SharePoint environments to search for VPN and MFA enrollment information, help desk instructions, and new hire guides.[1]

Enterprise T1190 Exploit Public-Facing Application

During C0027, Scattered Spider exploited CVE-2021-35464 in the ForgeRock Open Access Management (OpenAM) application server to gain initial access.[1]

Enterprise T1133 External Remote Services

During C0027, Scattered Spider used Citrix and VPNs to persist in compromised environments.[1]

Enterprise T1589 .001 Gather Victim Identity Information: Credentials

During C0027, Scattered Spider sent phishing messages via SMS to steal credentials.[1]

Enterprise T1656 Impersonation

During C0027, Scattered Spider impersonated legitimate IT personnel in phone calls and text messages either to direct victims to a credential harvesting site or getting victims to run commercial remote monitoring and management (RMM) tools.[1]

Enterprise T1105 Ingress Tool Transfer

During C0027, Scattered Spider downloaded tools using victim organization systems.[1]

Enterprise T1578 .002 Modify Cloud Compute Infrastructure: Create Cloud Instance

During C0027, Scattered Spider used access to the victim's Azure tenant to create Azure VMs.[1]

Enterprise T1621 Multi-Factor Authentication Request Generation

During C0027, Scattered Spider attempted to gain access by continuously sending MFA messages to the victim until they accept the MFA push challenge.[1]

Enterprise T1046 Network Service Discovery

During C0027, used RustScan to scan for open ports on targeted ESXi appliances.[1]

Enterprise T1588 .002 Obtain Capabilities: Tool

During C0027, Scattered Spider obtained and used multiple tools including the LINpeas privilege escalation utility, aws_consoler, rsocx reverse proxy, Level RMM tool, and RustScan port scanner.[1]

Enterprise T1003 .006 OS Credential Dumping: DCSync

During C0027, Scattered Spider performed domain replication.[1]

Enterprise T1069 .003 Permission Groups Discovery: Cloud Groups

During C0027, Scattered Spider accessed Azure AD to download bulk lists of group members and their Active Directory attributes.[1]

Enterprise T1566 .004 Phishing: Spearphishing Voice

During C0027, Scattered Spider impersonated legitimate IT personnel in phone calls to direct victims to download a remote monitoring and management (RMM) tool that would allow the adversary to remotely control their system.[1]

Enterprise T1598 .001 Phishing for Information: Spearphishing Service

During C0027, Scattered Spider sent Telegram messages impersonating IT personnel to harvest credentials.[1]

.004 Phishing for Information: Spearphishing Voice

During C0027, Scattered Spider used phone calls to instruct victims to navigate to credential-harvesting websites. [1]

Enterprise T1572 Protocol Tunneling

During C0027, Scattered Spider used SSH tunneling in targeted environments.[1]

Enterprise T1090 Proxy

During C0027, Scattered Spider installed the open-source rsocx reverse proxy tool on a targeted ESXi appliance. [1]

Enterprise T1219 .002 Remote Access Tools: Remote Desktop Software

During C0027, Scattered Spider directed victims to run remote monitoring and management (RMM) tools.[1]

Enterprise T1021 .007 Remote Services: Cloud Services

During C0027, Scattered Spider used compromised Azure credentials for credential theft activity and lateral movement to on-premises systems.[1]

Enterprise T1078 .004 Valid Accounts: Cloud Accounts

During C0027, Scattered Spider leveraged compromised credentials from victim users to authenticate to Azure tenants.[1]

Enterprise T1102 Web Service

During C0027, Scattered Spider downloaded tools from sites including file.io, GitHub, and paste.ee.[1]

Enterprise T1047 Windows Management Instrumentation

During C0027, Scattered Spider used Windows Management Instrumentation (WMI) to move laterally via Impacket.[1]
