Leafminer, Raspite, Group G0077 | MITRE ATT&CK®

Archived: 2026-04-05 12:58:41 UTC

Enterprise T1110 .003 Brute Force: Password Spraying

Leafminer used a tool called Total SMB BruteForcer to perform internal password spraying.[1]

Enterprise T1059 .007 Command and Scripting Interpreter: JavaScript

Leafminer infected victims using JavaScript code.[1]

Enterprise T1136 .001 Create Account: Local Account

Leafminer used a tool called Imecab to set up a persistent remote access account on the victim machine.[1]

Enterprise T1555 Credentials from Password Stores

Leafminer used several tools for retrieving login and password information, including LaZagne.[1]

.003 Credentials from Web Browsers

Leafminer used several tools for retrieving login and password information, including LaZagne.[1]

Enterprise T1189 Drive-by Compromise

Leafminer has infected victims using watering holes.[1]

Enterprise T1114 .002 Email Collection: Remote Email Collection

Leafminer used a tool called MailSniper to search through the Exchange server mailboxes for keywords.[1]

Enterprise T1083 File and Directory Discovery

Leafminer used a tool called MailSniper to search for files on the desktop and another utility called Sobolsoft to extract attachments from EML files.[1]

Enterprise T1046 Network Service Discovery

Leafminer scanned network services to search for vulnerabilities in the victim system.[1]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

Leafminer obfuscated scripts that were used on victim machines.[1]

Enterprise T1588 .002 Obtain Capabilities: Tool

Leafminer has obtained and used tools such as LaZagne, Mimikatz, PsExec, and MailSniper.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Leafminer used several tools for retrieving login and password information, including LaZagne and Mimikatz.[1]

.004 OS Credential Dumping: LSA Secrets

Leafminer used several tools for retrieving login and password information, including LaZagne.[1]

.005 OS Credential Dumping: Cached Domain Credentials

Leafminer used several tools for retrieving login and password information, including LaZagne.[1]

Enterprise T1055 .013 Process Injection: Process Doppelgänging

Leafminer has used Process Doppelgänging to evade security software while deploying tools on compromised systems.[1]

Enterprise T1018 Remote System Discovery

Leafminer used Microsoft's Sysinternals tools to gather detailed information about remote systems.[1]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

Leafminer used several tools for retrieving login and password information, including LaZagne.[1]
