**Scattered Spider**

**Aliases**

UNC3944

0ktapus

Muddled Libra

Scatter Swine

Storm-0875

Octo Tempest

LUCR-3

Star Fraud

**Scattered Spider Modus Operandi**

The step by step attack flow along with the mapping to cyber kill chain and MITRE ATT&CK Framework.

Step 1: SMS Phishing, Help Desk phone calls, sim swapping. (Reconnaissance, Initial Access)

Step 2: Social Engineering techniques to compromise creds. (Weaponization)

Step 3: Maintaining persistence through AnyDesk, ScreenConnect (legit tools). (Delivery, Persistence)

Step 4: Escalate privileges using Secretsdump and Mimikatz. (Command and Control, Privilege Escalation)

Step 4: Moving laterally through SSH, RDP. (Lateral Movement)

Step 5: Disable security, services and perform their end goal which could be data exfil, ransomware operations. (Actions on objectives, Exfiltration, Impact)

**IOCs**

ADRecon, AnyDesk, DCSync, FiveTran, FleetDeck, gosecretsdump, Govmomi, Hekatomb, Impacket, LaZagne, LummaC2, Mimikatz, Ngrok, PingCastle, ProcDump, PsExec, Pulseway, Pure Storage FlashArray, RedLine, Rsocx, RustDesk, ScreenConnect, SharpHound, Socat, Spidey Bot, Splashtop, Stealc, TacticalRMM, Tailscale, TightVNC, VIDAR, WinRAR, WsTunnel, and various Living off the Land techniques.

**File transfer IOCs**

put[.]io, transfer[.]sh, wasabi[.]com, and gofile[.]io

**File Transfer Agent**

Cyberduck

**Tunnelling software**

RSocs