Monthly Threat Intelligence Briefing

Lab Environment Focus

IronGrid Security | Period covered: October 2023 to December 2023

Prepared by Mahdi Ghaznawy

Period and sources

This briefing summarizes activity and trends that inform lab detections. Sources include CISA advisories, open intelligence feeds, vendor blogs, and lab telemetry in Splunk and ELK. Indicators shown are for simulation only.

Executive highlights

• Credential harvesting campaigns using Microsoft 365 brand impersonation increased during this period. OAuth consent phishing was observed in multiple labs.

• Commodity loaders delivered via ISO attachments rose in frequency then used remote scripting for follow up actions. Living off the land tools were favored for persistence.

• Ransomware operators continued to target exposed RDP and misconfigured VPN. MFA fatigue techniques remained effective.

Top TTPs to monitor

Technique: T1059 Command and Scripting Interpreter

Detection idea: Alert on suspicious PowerShell and cscript with signs of obfuscation.

Technique: T1078 Valid Accounts

Detection idea: First time source IP for a privileged user with an impossible travel correlation.

Technique: T1112 Modify Registry

Detection idea: Monitor Run keys and AppInit DLLs along with Shell open commands.

Technique: T1566 Phishing

Detection idea: Block known lookalike domains and tighten SPF and DMARC checks.

Technique: T1047 WMI

Detection idea: Hunt for process creation with wmic and remote WMI providers.

Lab observed indicators

Type: IP

Indicator: 185.243.56.71

Context: Observed during brute force then success on svc-backup

Type: Domain

Indicator: login-secure-microsoft[.]com

Context: Brand impersonation phishing site used in simulation

Type: Hash

Indicator: 4f2a9d1b7b0a7f0f69d9db44d38a6a21

Context: Sample ransomware dropper used in the lab

Type: URL

Indicator: hxxps://cdn-storage.example[.]net/officeupdate.iso

Context: Loader delivery in simulated campaign

Recommended priority actions

• Expand MFA to all administrative and service accounts and review conditional access policies.

• Deploy an OAuth consent alert in SIEM to flag risky app grants and disable unverified apps.

• Harden email security with strict DMARC alignment then quarantine failures.

• Update EDR detection for vssadmin delete shadows and unusual backup deletion attempts.

Appendix: Sample SIEM content

index=auth sourcetype=okta OR sourcetype=azure:signins | iplocation src_ip | eval last_seen=if(user==user AND src_ip!=last_ip AND abs(diff_in_hours) < 2, 1, 0) | search last_seen=1 | table _time, user, src_ip, City, Country