Purple Team Lifecycle

Overall
Status: **Completed**

PB1100 - Enterprise Recon Profile, Hunt, Defend

Lifecycle Project Manager
Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2021
- Simulation Start: 2/3/2021
- Simulation End: 2/6/2021
- Configuration Identified: 11/29/2020
- Change Management Referred: 2/6/2021
- Configuration Deployed: TBD

Status Code Legend
- Attack Simulation
- Defense Simulation
- System Configuration Change
- Information

APT Lifecycle Ingest and Research	• Lifecycle Type: **Attack Simulation** • Lifecycle Objective: **Alert, Defend**	• Ingest Source: **MITRE T1277** https://attack.mitre.org/techniques/T1277/ • Acquire OSINT data sets and information
	• Use OSINT sources to identify information available to the public due to intentional, unintentional, or malicious disclosures. Research defense opportunities and deploy domain monitoring and other brand awareness tools. Determine if any disclosures of intellectual property have occurred.	
Attack methodology	• Build OSINT Profile of Organization, Infrastructure and key employees. • Data Sources: Social Media - Organization Information, Employee information Pastebin, GitHub – Identify source code, other information HackerTarget, URLCrazy – DNS Enumeration, Landscape Shodan.IO – Identify External Landscape, Vulnerabilities GrayHatWarefare – Search for S3 Buckets LinkedIn, GlassDoor, Monster – Gather business organizational information, technologies Hunter.io: Identify employees, organizational relationships BeenVerified: Build Employee Profiles • Post fictitious breach.	
Defense methodology	• Work with HR, Marketing to limit publicly sensitive information • Post Deceptive Information: Pastebin: "Breach" disclosure of account hashes and VPN endpoint VPN Service: Alert on account login. • Automated Counter-defense Deny-list IP addresses from any successful logins on honey-VPN service	
Lifecycle Adjustments	• Work with Legal to remove any IP from public internet (Pastebin, Github, etc) • Configure alerting on Pastebin, Github, Shodan.IO, HIBP • Work with Marketing Department, HR Department, DevOps regarding Awareness Practices • Post Deceptive Information on Pastebin • Build Honey VPN Service • Demy-list IP's on Enterprise WAN from all successful Deceptive VPN Logins	

Change Management	• Deploy new VPN Service. Create accounts. • Self-Disclose accounts and hashes on Pastebin. • Capture SRC IP of Deceptive VPN Login, update deny list on all endpoints and edges with SRC IP. • Users Affected: Security Team will receive new alerts regarding data disclosures from Pastebin, GitHub Network Team: will receive new alerts regarding network perimeter changes from Shodan.io
Lessons Learned	• Attack included a fictious post on Pastebin. It was necessary to configure Pastebin account for alerting on trigger keywords. • Deceptive service can be hosted anywhere besides enterprise data center. VPN was disclosed in deceptive breach. The Deceptive VPN can capture SRC IPs of successful logins and update the Deny-list utilized by enterprise Data Center edge routers and all endpoints protection solutions.