FORENSIC INVESTIGATION ON WIDGET CO.

Team - 09

Bhuvantej Ramachandra Reddy
Pramath Yaji
Faraz Ahmed
Phani Varun Munukuntla

Investigation Overview

- Investigate suspected breach on October 12, 2022
- Analyze provided logs using Splunk to identify any indicators of compromise (IOCs)
- Deliver findings to both technical and non-technical stakeholders

Why Splunk?

- Industry-standard log analysis tool
- Allows ingestion of multiple data types and sources (VPN, DNS, Cloud, etc.)
- Supports real-time anomaly detection and IOC correlation
- Highly visual and customizable dashboards
- Enables both in-depth technical analysis and high-level summarization

Forensic Investigation Approach

- **Log Ingestion:** Loaded 10 datasets into Splunk
- **IOC Matching:** Compared logs with known IP Addresses and DNS
- **Timeline Creation:** Traced event sequences to build incident narrative
- **Dashboard Development:** Created visualization to support evidence and simplify understanding

Was There a Breach?

- **Oct 12:** Phishing link (glasslu.com) clicked by user **BDRVLS**
- **Oct 12–26:** MFA bypass attempts across Productivity Suite, Billing, and WidgetApp
- **Oct 13:** Password vault accessed via suspicious IP (180.76.54.93)
- **Oct 14 & 24:** Lateral movement using stolen **DDDXUB** credentials to access Cloud and IT Admin

Attack Path:
Phishing → Credential Theft → MFA Bypass → Lateral Movement → Privilege Escalation

Recommendations for Leadership

Security Culture & Training

- Launch quarterly phishing simulations
- Mandatory cybersecurity training for all departments

Policy & Incident Planning

- Update incident response plan with phishing and lateral movement playbooks
- Introduce a breach notification and recovery procedure

Resource Allocation

- Hire a dedicated SOC Analyst
- Allocate time for regular internal security audits

Access & Role Management

- Quarterly reviews of user access and roles
- Implement just-in-time access where possible

Recommendations for IT/Security Team

Improve Access Security

- Enforce geo-restricted logins
- Expand MFA to cover all systems, including legacy apps

Real-Time Monitoring

Configure real-time alerts in Splunk for:

  - *IOC detections*
  - *After-hours logins*
  - *High-risk user activity*

Automate Security Hygiene

- Automatic password rotation
- Scheduled access reviews and privilege audits

Conclusion

In summary, our investigation confirmed a breach that began with phishing and escalated through weak access controls. Using Splunk, we identified key events and visualized the attack path and provided clear, actionable recommendations. By implementing these changes, Widget Co. can significantly improve its security posture and reduce future risk.