



## Scenario 1: Performing a Query with Chronicle

<b>Date:</b>  November 05 2024.	<b>Entry: # 1</b>
<b>Description</b>	This report documents an investigation into phishing activity targeting employees at the company. The investigation focuses on identifying impacted assets, employee interactions with the malicious domain, and indicators of compromise.
<b>Tool(s) used</b>	<ul style="list-style-type: none"><li>• <b>Chronicle:</b> Used for log analysis, domain investigation, and identifying indicators of compromise.</li></ul>
<b>The 5 W's</b>	<ul style="list-style-type: none"><li>• <b>Who:</b> A malicious actor leveraging a spoofed domain to steal employee credentials.</li><li>• <b>What:</b> A phishing security incident involving the domain <code>signin.office365x24.com</code>.</li><li>• <b>Where:</b> Affected assets include three employee machines and accounts at a financial services company.</li><li>• <b>When:</b> Activity was observed from January 31, 2023, to July 8, 2023.</li><li>• <b>Why:</b> The attackers used a spoofed domain resembling a legitimate Office 365 login page ( <code>login.office365x24.com</code> ). Employees unknowingly entered their credentials, resulting in POST requests to <code>/login.php</code>, indicating successful phishing attempts.</li></ul>
<b>Additional</b>	<b>Domain Context:</b> VirusTotal flagged the domain as malicious with



notes	<p>reports from 12 security vendors.</p> <p><b>Resolved IPs:</b> Two IP addresses associated with the domain (104.215.148.63 and 40.100.174.34).</p> <p><b>Sibling Domains:</b> login.office365x24.com was identified as a related domain.</p> <p><b>Key Findings:</b></p> <p><b>Malicious Domain:</b> signin.office365x24.com was identified as malicious by multiple security vendors.</p> <p><b>Affected Assets:</b> Three employee machines accessed the domain and interacted with it via POST requests.</p> <p><b>Infrastructure Reuse:</b> The attackers reused the same IP address across multiple phishing domains, indicating a broader campaign.</p> <p><b>Credential Compromise:</b> POST requests suggest that credentials were likely exfiltrated.</p>
-------	--

<b>Reflections for Scenario 2: Follow-Up Analysis and Actions</b>	<p><b>Employee Awareness:</b> The success of this phishing attack highlights the need for enhanced employee training on identifying suspicious emails and domains.</p> <p><b>Phishing Campaign:</b> The attacker's use of infrastructure reuse suggests a broader campaign that may target other organizations.</p> <p><b>Log Analysis:</b> Chronicle's detailed log analysis and procedural filtering were instrumental in tracing the interactions with the malicious domain.</p>
---	---



**Follow-Up  
Actions**

1. **Employee Training:** Conduct mandatory phishing awareness training sessions.
2. **Network Monitoring:** Increase monitoring of network traffic to detect suspicious domains or unauthorized data exfiltration attempts.
3. **Threat Intelligence Sharing:** Share findings with relevant industry threat intelligence groups to prevent similar incidents elsewhere.
4. **Blocking Malicious Domains:** Update firewall and DNS rules to block `signin.office365x24.com`, `login.office365x24.com`, and associated IP addresses.
5. **Credential Reset:** Require impacted employees to reset their passwords immediately and enforce multi-factor authentication (MFA).