Severity

Medium

Analysis Summary

In late March it was reported that LAPSUS$ had breached T-Mobile. The Ransomware and Extortionist group had also breached Okta which provides services to big names like Hitachi, T-Mobile, HP, and Siemens. T-Mobile has now confirmed the LAPSUS$ breach and issued the following statement:

“Several weeks ago, our monitoring tools detected a bad actor using stolen credentials to access internal systems that house operational tools software. The systems accessed contained no customer or government information or other similarly sensitive information, and we have no evidence that the intruder was able to obtain anything of value. Our systems and processes worked as designed, the intrusion was rapidly shut down and closed off, and the compromised credentials used were rendered obsolete.”

According to a Security Researcher, organizations should invest in scrapping criminal bot services like the Russian Market and Genesis regularly. They should also buy back the employee credentials available online to better protect themselves.

Impact

- Financial Theft
- Data Breach

Remediation

- Logging — Log your eCommerce environment’s network activity and web server activity.
- Passwords — Ensure that general security policies are employed including: implementing strong passwords, correct configurations, and proper administration security policies.
- Admin Access — limit access to administrative accounts and portals to only relevant personnel and make sure they are not publicly accessible.
- WAF — Web defacement must be stopped at the web application level. Therefore, set up a Web Application Firewall with rules to block suspicious and malicious requests.
- Patch — Patch and upgrade any platforms and software timely and make it into a standard security policy. Prioritize patching known exploited vulnerabilities and zero-days.
- Secure Coding — Along with network and system hardening, code hardening should be implemented within the organization so that their websites and software are secure. Use testing tools to detect any vulnerabilities in the deployed codes.
- 2FA — Enable two-factor authentication.
- Antivirus — Enable antivirus and anti-malware software and update signature definitions in a timely manner. Using a multi-layered protection is necessary to secure vulnerable assets