CIRT Playbook Battle Card: **GSPBC-1001 - Initial Access - Exploit Enterprise Resources - Mobile Device SIM Attacks**

(P) Preparation

1. Favor use of authenticator apps over SMS
2. Create a strong account PIN or Passphrase
3. Use a dedicated number for high-value accounts
   a. Alternative: Use a free Google Voice number
4. Use a password manager
5. Never store passwords, payment methods, etc. in your phone's browser
6. Prepare backup communications ability to allow you to respond more quickly to a compromise
   a. Hangouts, GVoice, Skype, Line, etc.
7. Conduct user awareness training
8. Conduct response training (this PBC)

(I) Identification

1. Monitor for:
   a. Unexplained, prolonged loss of cell service
   b. Unexpected customer service calls, "Sorry we got disconnected …"
   c. Alerts about password/authentication changes to your accounts
   d. Alerts on your phone, "Are you trying to log in from <City> , <State>?"

(C) Containment

1. Notify your mobile carrier as soon as you can
2. Explain the situation:
   a. "I am a high-value-target individual and my phone number was ported approximately 3 hours ago to a new SIM that I do not control …"
3. Request that the number be completely disabled:
   a. "Since this is an active situation, please remove my phone number from that SIM immediately, meaning no one can receive phone calls or text messages to my number …"
4. Request that your number to be moved back to your SIM
   a. This may be more difficult than getting the number disabled
5. Record the employee's name/number and dates
6. Record all case/support ticket numbers
7. Request that all logs for your IMEI be saved
8. Change all of your passwords from a non-compromised trusted device
   a. Change your major email accounts first
   b. Prioritize: Most to least valuable
   c. Document your actions as you are conducting them, including times and screen shots

(E) Eradication

1. Request that your mobile service block all swap attempts for one week
2. See additional steps in "Containment"

(R) Recovery

1. Retain legal counsel
2. Contact appropriate law enforcement agencies
3. Contact affected business partners
   a. Follow the advice of your legal counsel
4. Retain the services of security professionals
5. Regain control of your various compromised accounts
   a. Every provider will be different
   b. Document dates, times, names, and steps

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Be aware of all 2FA options when setting up new accounts, disabling all weak, SMS-based options
3. Be aware that the vulnerability is with your mobile provider and you have limited control over it
   a. Focus instead on what you can control
   b. Defense-in-depth and compartmentalization of your accounts

References:

1. MITRE ATT&CK Technique T1451: https://attack.mitre.org/techniques/T1451/

Resources:

➔ GuardSight GSVSOC Incident Response Plan: https://github.com/guardsight/gsvsoc_cybersecurity-incident-response-plan
➔ IT Disaster Recovery Planning: https://www.ready.gov/it-disaster-recovery-plan
➔ Report Cybercrime: https://www.ic3.gov/Home/FAQ

GUARDSIGHT