VPN Breach Containment & Recovery Plan

Playbook

Purpose

Contain the adversary, preserve evidence, eradicate access, and **restore safely**—with specific actions for VPN led intrusions (Citrix “Bleed”-style session hijacking; Cisco ASA brute force/CVE 2023 20269; generic credential theft).

Assumptions:

- Initial access happened via the **VPN gateway or its authentication path** (IdP/RADIUS/LDAP).
- Multi factor may have been **bypassed** (e.g., stolen session tokens) or **absent**.
- Attackers may already have **domain/identity footholds** and be staging data exfiltration (Rclone/WinSCP/MEGA, etc.).

0) "First Hour" Quick Start *(Do these in parallel)*

1. **Establish control & communications**
   - Activate IR plan; name an **Incident Commander (IC)**
   - Switch to **out of band comms** (phone bridge/secure chat not tied to SSO/Email)
   - Start an **evidence log** (who did what/when) per NIST IR guidance

2. **Contain access through the suspected VPN**
   - **Block internet exposure** to the affected VPN listener(s) at the upstream firewall or ACL **without powering devices off** (preserves volatile evidence)
   - If business can't tolerate full block: immediately restrict to a **temporary allowlist** of known admin IPs

3. **Freeze the blast radius (identity & sessions)**
   - **Force sign out / revoke refresh tokens** for all users with VPN access (IdP wide if necessary)
     - Microsoft Entra ID: Revoke user sessions/refresh tokens
     - Okta: Revoke all sessions and OAuth tokens
     - Google Workspace: Reset sign in cookies/passwords for impacted accounts and review OAuth grants

4. **Engage cyber insurance and legal early**
   - Most policies require **prompt notice** and often prefer panel IR firms—loop them in now to avoid coverage issues
   - If you're insured with At Bay, engage their claims/response flow immediately

5. **Kick off threat hunting for exfil & staging**
   - Hunt for **Rclone/WinSCP/FileZilla/WinRAR, AnyDesk/Ngrok**, and large egress to cloud storage (MEGA/OneDrive/S3)

1) Decision Tree: What kind of VPN compromise is this?

A. **Session/credential hijack (Citrix/NetScaler "Bleed" style)**
   - Symptoms: suspicious sessions despite MFA; tokens persist after password resets
   - **Action**: Patching **alone is not enough**—you must **invalidate/kill all active sessions** on the appliance **after** patching to evict hijacked tokens

B. **Brute force / auth bypass (Cisco ASA CVE 2023 20269)**
   - Symptoms: burst of VPN login attempts; unexpected clientless SSL VPN sessions; VPN local admin creation
   - **Action**: Patch per Cisco SA; enforce MFA; limit failed logins; check for unauthorized clientless sessions

C. **Full device compromise / persistence suspected**
   - Symptoms: config tampering, unknown processes, unexplained reboots, egress from appliance
   - **Action**: Treat like a **network edge device compromise—isolate, image/collect forensic artifacts**, then **rebuild to a known good version and rotate all secrets** tied to the device

2) Containment (detailed)

1. **Network & Gateway**
   - **Isolate the specific VPN VIP/port** upstream. Do **not** power down yet (preserve memory and sessions for IR)
   - **Collect forensic snapshots/artifacts** before changes (configs, logs, core/memory dumps where supported)
     - For Cisco ASA/FTD, CISA has directed federal agencies to **collect core dumps and assess compromise**; the same principle helps enterprise IR.

2. **Identity & sessions**
   - **Tenant wide conditional access "squeeze"** (temporarily require compliant devices + MFA, block legacy auth)
   - **Revoke user sessions/refresh tokens** at IdP, then **reset passwords** for accounts with VPN rights
   - **Review privileged identities** (Global Admins/Domain Admins) for anomalous sign ins and **rotate creds**

3. **Vendor-specific hotfixes**
   - **Citrix/NetScaler (CVE 2023 4966 "CitrixBleed")**
     - Update to fixed firmware, then kill all active/persistent sessions (ICA/AAA/LB, not just VPN)
     - Review appliance logs for hijacked sessions; regenerate any exposed secrets

   - • **Cisco ASA/FTD (CVE 2023 20269)**
     - Apply Cisco SA mitigations/updates
     - Enforce **MFA** on VPN; rate limit failed logins; remove unused clientless SSL profiles; check for unknown local users/profiles

4. **Endpoint & server "blast radius freeze"**
   - **Quarantine suspicious hosts** surfaced by EDR (especially jump boxes, hypervisors, DCs, backup servers)
   - **Disable lateral tools** detected (PsExec, remote sched tasks, ScreenConnect/AnyDesk, Ngrok).
   - **Throttle egress** to known exfil services (MEGA, Dropbox, S3, GDrive) at proxies/firewalls.

3) Investigation & Scoping (in parallel with containment)

1. **Evidence to collect (minimum)**
   - **VPN appliance**: running version, config, session tables, auth logs, web access logs, core/memory if available
   - **Identity**: IdP sign in logs, MFA events, token issue/revocation logs
   - **Domain**: DC security logs (4624/4625/4672/4768/4769), new user/group membership, GPO changes
   - **EDR/NDR**: detections, process trees for Rclone/WinSCP/FileZilla/7 Zip/WinRAR, beaconing, exfil volumes
   - **Network**: firewall/proxy logs for large outbound to cloud storage. (Rclone/WinSCP are common in ransomware exfil.)

2. **Hunt Playbook (examples)**
   - **Identity**: impossible travel; sudden MFA disable; new OAuth grants; new app registrations/service principals
   - **Windows**: look for creation of new local admins; Scheduled Tasks (4698), Service installs (7045); LSASS access; VSS deletion
   - **Exfiltration**: Rclone/WinSCP/MEGA usage; huge TAR/ZIP/RAR creation; long lived TLS to cloud endpoints

4) Eradication

1. **Appliance re baselining (preferred over “cleanup”)**
   - **Back up evidence**, then **factory reimage/upgrade** the VPN gateway to a **vendor fixed build**
   - **Do not restore old configs wholesale**—re enter minimal, hardened configuration (no unused portals/profiles)
   - **Rotate all secrets linked to the appliance**:
     - TLS server certs/keys, IPsec pre shared keys, RADIUS/LDAP shared secrets, local VPN user passwords
     - **Invalidate all sessions** (Citrix specifically requires this after patching due to token theft behavior)

2. **Identity & domain hardening**
   - **Tenant wide session revocation** and **password reset** for VPN enabled users completed? Verify
   - **Application secrets & SAML signing certs**: rotate on IdP/SP pairs to eliminate stolen credentials/tokens
   - **Active Directory (if Kerberos tickets may be stolen)**: rotate **KRBTGT twice** with the required interval so old TGTs expire (Microsoft guidance)

3. **Contain data theft and prep for extortion**
   - Review logs for **data staging** and **cloud exfil** (Rclone/WinSCP/MEGA). Build your evidence package
   - Align with legal on breach reporting; if personal data is implicated in the EU/UK, **72 hour regulator notice** may apply under GDPR Article 33

5) Recovery & Restore (bring the business back safely)

1. **Safer remote access "bridge"**
   - **Do not simply re open the old VPN**. Stand up a **hardened interim**:
     - Patched gateway on a **new IP/DNS, MFA enforced, client certs if possible**, and **allowlist** to known user egress ranges
     - Or, use a **cloud ZTNA** broker for critical apps while you rebuild (consistent with insurer and At Bay guidance to consider modern cloud based access)

2. **Clean restore of endpoints/servers**
   - **Reimage compromised systems**; restore data from **known good, tested** backups. Follow CISA ransomware recovery guidance/checklists
   - **Scan restored hosts** with EDR before reconnecting
   - **Staged reconnect** to the network: lowest risk segments first, then progressively enable access

3. **Validate "no re entry"**
   - Continuous monitoring for:
     - New anomalous VPN sessions; token re issue surges; reappearance of exfil utilities; beaconing
   - Run a **post restore purple team check** (password spray against IdP blocked? exfil controls effective?)

6) Communications, Insurance & Regulatory

1. **Safer remote access “bridge”**
    - **Insurer**: keep a **single liaison** with your carrier; follow **panel vendor** rules to preserve coverage. Log all actions and time stamps
    - **Law enforcement**: per CISA, reporting ransomware/extortion events is encouraged; align with counsel
    - **Regulators & affected parties**: apply applicable breach notification regimes (e.g., GDPR 72 hour clock if personal data was at risk)
    - **PR/Customer comms**: coordinate statements; avoid operational detail that aids the adversary

7) Hardening before reopening the VPN

2. **Minimum bar before go live**
    - **Patched** to fixed builds; **no default**/legacy tunnels; **clientless portals disabled** unless needed
    - **MFA mandatory**; add **client certificates** for admins; **lock out** on repeated failures
    - **Segmentation**: VPN user roles map to least privilege network access (no flat /16 reachability)
    - **Logging & telemetry** shipped off box; **centralized monitoring** (SIEM/MDR)
    - **Externally test** (scan the listener; validate headers/ciphers; enumerate portals)
    - **Session hygiene**: periodic forced re auth; short refresh token lifetimes; OAuth grant reviews

8) Appendixes

1. **Vendor specific gotchas**
    - **Citrix/NetScaler "CitrixBleed" (CVE 2023 4966)**
        - Nature: memory disclosure → **session token theft, MFA bypass**
        - Remediation: **Patch + invalidate all sessions** (ICA/AAA/VPN/LB). Patch only leaves stolen sessions valid
    - **Cisco ASA/FTD (CVE 2023 20269)**
        - Nature: auth separation flaw enabling **brute force** and **unauthorized clientless sessions**; exploited by Akira affiliates
        - Remediation: **Patch**, enable **MFA**, harden profiles, **limit failed logins**, review for unknown users/sessions

2. **Minimal hunt checklist (what to look for)**
    - **Identity**: sudden MFA disables; new OAuth grants/app registrations; unfamiliar API/service principals
    - **Windows audit**:
        - Logons: 4624/4625 (Type 3/10), new admin privileges (4672), Kerberos TGS (4769) surges
        - Lateral movement: new services (7045), scheduled tasks (4698), RDP enablement, admin share usage
    - **Exfiltration: Rclone/WinSCP/MEGA**; large archive creation via 7 Zip/WinRAR; long lived TLS to cloud storage

3. **Roles & RACI (suggested)**
    - **Incident Commander (Security)** – overall control, comms cadence, acceptance of risk.
    - **Network Lead** – isolation, captures, rebuilds of edge devices
    - **Identity Lead** – session revocation, MFA, token & cert rotation, AD KRBTGT rotation if needed
    - **Forensics Lead (DFIR)** – evidence, scoping, attacker TTPs, exfil assessment
    - **IT Ops** – rebuilds, backup restoration, change control
    - **Legal/Privacy** – notification obligations
    - **Insurance Liaison** – carrier comms & panel coordination
    - **Comms/PR** – internal & external messaging

4. **Acceptance criteria to declare "contained" and "recovered"**

- **Contained**
  - Patched/rebuilt VPN; **all sessions invalidated; IdP tokens revoked**; no active IOCs in 48–72h; outbound exfil channels blocked

- **Recovered**
  - Clean re images restored; **EDR green**; staged reconnect complete; privileged identities rotated (incl. **KRBTGT x2** when warranted); business services meet **RTO/RPO**

- **Post/Incident**
  - Lessons learned per **NIST SP 800 61r3**; prioritize migration path to **ZTNA/SASE** to shrink VPN exposure surface (aligned with insurer guidance)

Disclaimer

The materials, documents, and tools shared by Point Break Security GmbH and The Daily Signal channel are provided free of charge for the purpose of supporting and educating our audience.

While every effort is made to ensure accuracy and usefulness, Point Break Security GmbH, The Daily Signal, and any individual involved in producing or distributing this content do not guarantee the quality, accuracy, or suitability of the information or materials provided.

We cannot be held responsible or liable for any damages, losses, or issues that may arise from the use, misuse, or interpretation of these materials.

Users are solely responsible for verifying that any scripts, configurations, or recommendations are compatible with their own environment and for thoroughly testing them in a controlled or non-production setting before applying them to live systems.

By using these materials, you acknowledge that you do so at your own risk and accept full responsibility for how they are implemented.