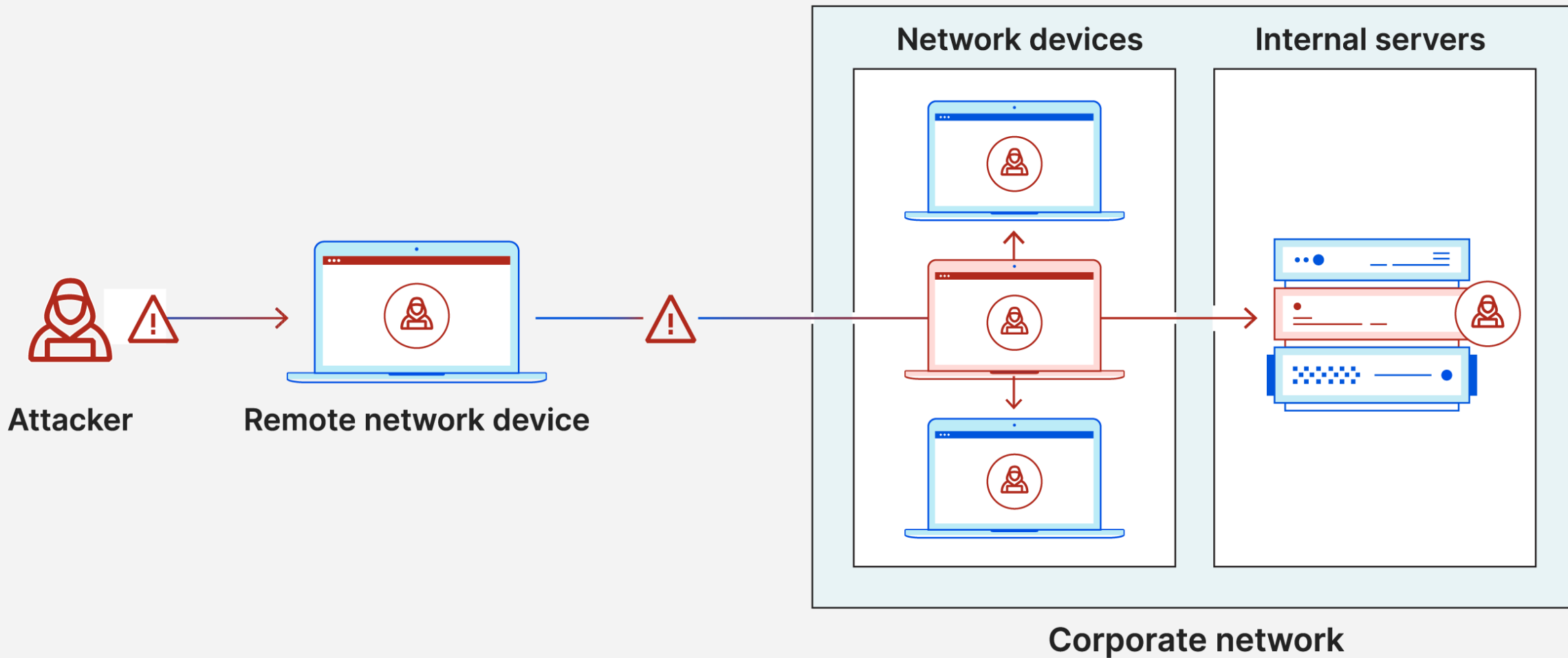


Movimiento lateral y persistencia en ciberataques corporativos



Linux Persistence Techniques

System Services

Systemd Service Persistence

Modifying systemd service files to execute malicious code upon system initialization.

SysV Init (init.d) Persistence

Leverages older SysV init system, using scripts in /etc/init.d/ to run malware during system initialization.

User-level Persistence

SSH Key Persistence

Adds a backdoor SSH key to authorized keys, allowing attacker to log in remotely.

Shell Profile Persistence

Modifying shell profile files like .bashrc ensures malicious scripts run on each shell session.

Cron Jobs and Scheduled Tasks

Cron Job Persistence

Adds cron jobs to ensure script execution at regular intervals or system reboots.

At Job Persistence

Schedules one-time or recurring tasks to maintain persistence.

File and Package Modifications

Malicious Packages (DPKG/RPM)

Creates malicious Debian/RPM packages to install backdoors and ensure persistence during installations/updates.

Password and User Modifications

Adding new users to /etc/passwd or modifying existing user passwords to maintain access.

Other Techniques

SUID Backdoor

Modifying SUID binaries can grant an attacker elevated privileges when running specific programs.

Docker Container Persistence

Uses a Docker container with a host escape mechanism to maintain access across reboots.

Cron Jobs and Scheduled Tasks

Cron Job Persistence

Adds cron jobs to ensure script execution at regular intervals or system reboots.

At Job Persistence

Schedules one-time or recurring tasks to maintain persistence.

Laboratorio & Herramientas



Atacante

TCP Reverse shell



Puerto 4444



ServidorA

Persistencia



ServidorB

Movimiento lateral

172.12.1.0/24

Código

#Explotación inicial con metasploit

```
nano config.json
```

```
"admin_server": {  
    "listen_url": "0.0.0.0:3333",  
    ...  
},  
"phish_server": {  
    "listen_url": "0.0.0.0:80",  
    ...  
}
```

Código

#Instalación Gophish

```
nano config.json
```

```
"admin_server": {  
    "listen_url": "0.0.0.0:3333",  
    ...  
},  
"phish_server": {  
    "listen_url": "0.0.0.0:80",  
    ...  
}
```

Recomendaciones para remediación o prevención

- Implementar la microsegmentación y protegerlas individualmente.
- Mantener un enfoque de confianza cero que priorice la seguridad.
- Asegurarse de que todo el personal comprenda y respete los protocolos de seguridad comunes
- Adoptar un enfoque de confianza cero.

