
CERISAC
BY ART REBULTAN

TABLETOP

Imagine this – you are in charge of protecting the critical infrastructure of your country from cyberattacks. You must deal with hackers constantly trying to break into your systems and cause chaos. You must keep your firewalls updated and secure and monitor your network for suspicious activity. Sounds like a tough job, right?

Now imagine that one day, you wake up to discover that the biggest cyberattack has hit your country in its history. A group of unknown attackers has exploited a vulnerability in a popular firewall brand you and many others use. They have gained access to your network and are trying to steal your data, sabotage your operations, or worse. You have to act fast and stop them before they do more damage. Sounds like a nightmare, right?

This is not a fictional scenario. This is what happened to Denmark in May 2023. According to a report by SektorCERT, the organization responsible for the cybersecurity of critical infrastructure in Denmark, 22 companies were breached in just a few days by multiple groups of attackers. Some of them were using zero-day exploits, exploiting vulnerabilities that were not publicly known or patched. Some of them were linked to Sandworm, a notorious Russian cyber unit that was behind the devastating NotPetya attack in 2017.critical infrastructure cybersecurity

BUSINESS IMPACT

- Loss of revenue and reputation: The cyberattacks caused disruption and downtime for 22 critical infrastructure organizations, affecting their operations and services. Some had to enter island mode, disconnecting from the internet and other networks, which reduced their efficiency and productivity. The cyberattacks also damaged their reputation and trust among customers and partners and exposed them to potential legal and regulatory consequences.

- Cost of recovery and prevention: The cyberattacks required the organizations to invest in incident response, remediation, and recovery efforts, which involved replacing compromised devices, restoring data and systems, and improving security measures. The organizations also had to pay external experts, vendors, and consultants to assist them. Additionally, the organizations had to implement preventive actions, such as updating their software, patching their vulnerabilities, and enhancing their monitoring and detection capabilities.

- Risk of escalation and recurrence: The cyberattacks demonstrated the vulnerability and attractiveness of Danish critical infrastructure to foreign actors, who may have different motives and capabilities. The cyberattacks also showed the coordination and sophistication of some attackers, who used zero-day exploits and were potentially linked to a nation-state actor. The cyberattacks could escalate into more destructive or disruptive actions or recur in the future, posing a severe threat to the national security and public safety of Denmark.

CAMPAIGN

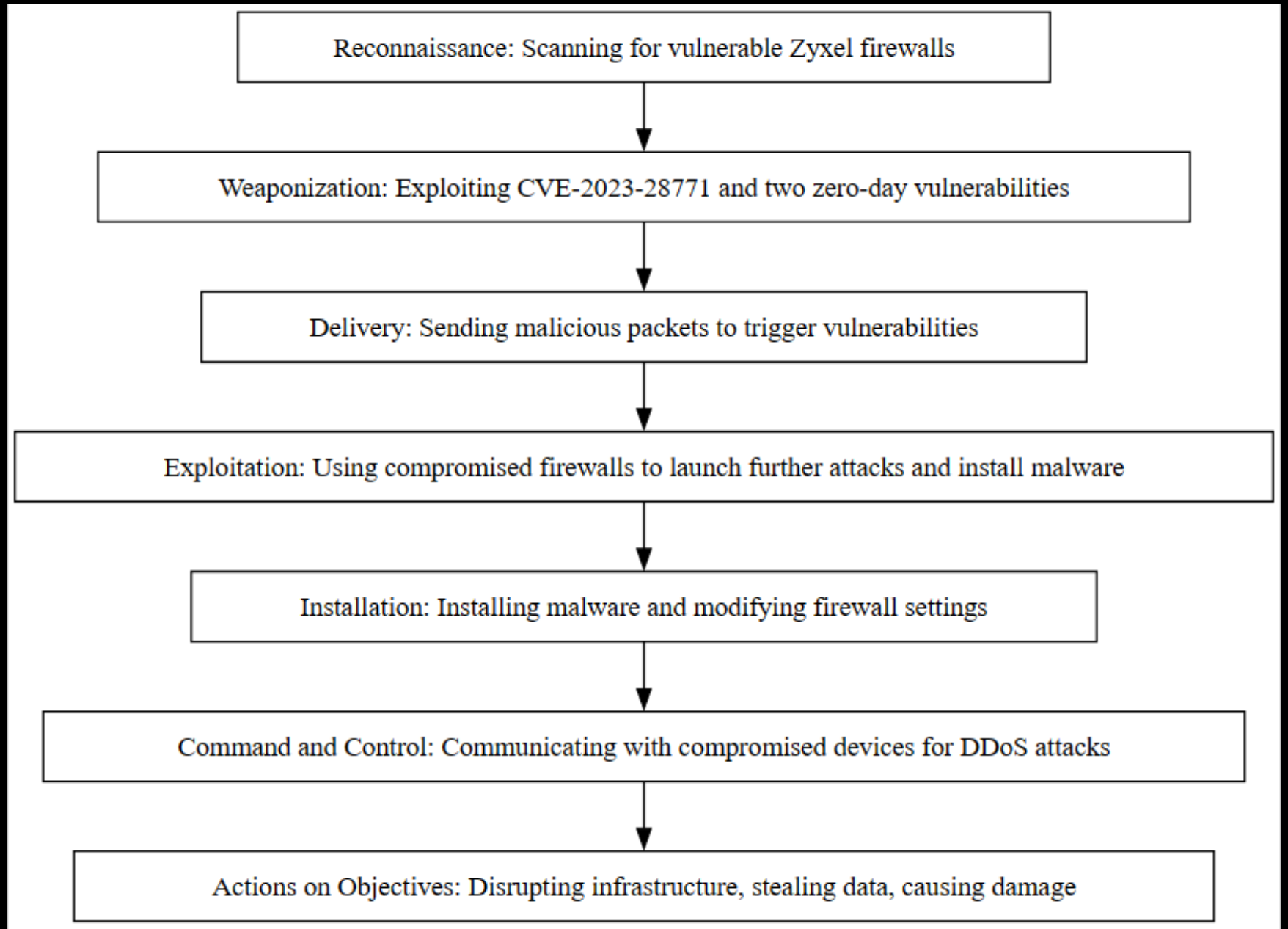
The adversary is trying to disrupt operations and steal sensitive data by launching cyberattacks using exploits in Zyxel firewalls. Multiple waves of attacks happened.

The attackers used coordinated and targeted methods to scan and compromise the firewalls and, in some cases, used zero-day exploits or APT techniques. They also used the compromised devices for botnet and DDoS activities.

The attacks affected 16 energy organizations and one other organization that runs critical infrastructure in Denmark.

Start investigating by checking the firewall logs and configurations for any signs of unauthorized access or changes and patching the Zyxel vulnerabilities as soon as possible.

ATTACK VECTOR



INDICATOR OF ATTACK

- **Zyxel firewall exploits**: The attackers used CVE-2023-28771 and two other zero-day vulnerabilities to compromise Zyxel firewalls and gain remote access to the networks of critical infrastructure organizations.
  - Unusual network traffic from or to the firewall devices
  - Firewall configuration changes or downloads over insecure connections
  - Firewall logs showing failed or successful authentication attempts

- **Mirai botnet activity**: One of the compromised organizations was used as part of the Mirai botnet to launch DDoS attacks against US and Hong Kong targets.
  - High outbound traffic from the organization's network to the DDoS targets
  - Malware infection or persistence on the organization's devices
  - Communication with known Mirai command and control servers

- **Sandworm APT traffic**: One of the organizations detected traffic from an IP address previously linked to the Sandworm APT group, a Russian state-sponsored cyber unit.
  - Connection attempts from or to the suspicious IP address
  - Malicious payloads or scripts delivered by the traffic
  - Evidence of lateral movement or data exfiltration within the network

COUNTERMEASURES

1. Perimeter Security: Configure firewalls to block all unnecessary inbound and outbound traffic. Regularly update and patch firewall devices to fix known vulnerabilities. In the case of Zyxel firewalls, ensure that the latest firmware updates are installed to patch the CVE-2023-28771 vulnerability.

2. Network Security: Implement network segmentation to limit the lateral movement of attackers within the network. Use intrusion detection and prevention systems (IDS/IPS) to detect and block malicious network activities.

3. Endpoint Security: Install and update antivirus software on all endpoints. Enable automatic updates to ensure the software can detect and remove the latest threats. Regularly scan all devices for malware and suspicious activities.

4. Application Security: Regularly update and patch all software applications to fix known vulnerabilities. Disable unnecessary features and services in software applications to reduce the attack surface.

5. Data Security: Encrypt sensitive data at rest and in transit. Implement strong access controls to prevent unauthorized access to sensitive data. Regularly backup important data and test the restore process to ensure data availability in case of an attack.

6. User Awareness and Training: Educate users about phishing and social engineering attack risks. Encourage them to report any suspicious activities or incidents.

7. Incident Response and Recovery: Have an incident response plan and regularly test it to ensure its effectiveness. The plan should include steps to identify, contain, eradicate, and recover from an attack.

INDICATORS OF COMPROMISE

- CVE IDs: The attackers exploited multiple vulnerabilities in Zyxel firewalls and access points (APs), including CVE-2023-22913, CVE-2023-22914, CVE-2023-22915, CVE-2023-22916, CVE-2023-22917, and CVE-2023-229181. The most critical vulnerability is CVE-2023-28771, which allows for remote code execution.
- Affected devices: The affected devices belong to multiple Zyxel product lineups, including ATP, USG FLEX - ZLD, VPN - ZLD, and ZyWALL/USG - ZLD.
- Malicious activities: The attackers could modify device configuration data, execute unauthorized OS commands, cause denial-of-service (DoS) conditions, and retrieve encrypted information of the administrator.
- Mirai botnet: One of the groups targeting vulnerable Zyxel devices is Mirai, which is usually used for distributed denial of service (DDoS) attacks.

LESSONS LEARNED

- Keep your devices updated: The attackers exploited unpatched vulnerabilities in Zyxel firewalls announced on April 1. Many organizations did not update their devices or were unaware of the updates. This gave the attackers weeks to carry out the attacks. Updating your devices regularly can prevent such attacks or reduce their impact.
- Know your network: Some organizations did not know they had Zyxel firewalls in their network because third-party suppliers installed them or did not have an overview of their devices. This made it harder to detect and respond to the attacks. Knowing what devices are connected to your network and who is responsible for them can help you secure and respond faster to incidents.
- Be prepared for multiple threats: The attackers used different methods and motives to target Danish critical infrastructure. Some were trying to steal data, some to create a botnet, and some were potentially linked to a nation-state actor. The attacks also occurred in waves, with periods of silence in between. Being prepared for multiple and evolving threats can help you defend your network and mitigate the damage.
- Collaborate and share information: SektorCERT praised the fast responses of its experts and the affected organizations. They also shared information and alerts with their members and encouraged them to install the updates. Collaborating and sharing information with other organizations and authorities can help you prevent, detect, and deal with cyberattacks.

REFERENCES

How Denmark nulled record attacks on critical infrastructure • The Register

Zyxel security advisory for OS command injection vulnerability of firewalls | Zyxel Networks

Vulnerability in Zyxel firewalls may soon be widely exploited (CVE-2023-28771) - Help Net Security

Critical Zyxel Firewall Bug Under Active Attack After PoC Exploit Debut (darkreading.com)

Zyxel security advisory for multiple vulnerabilities of firewalls and APs | Zyxel Networks

A critical security flaw is affecting Zyxel firewall devices - here's what you need to know | TechRadar


TO GOD
BE THE
GLORY