Forescout Research: Clearing the Fog of War

forescout.com/blog/analysis-of-energy-sector-cyberattacks-in-denmark-and-ukraine/

January 11, 2024

Clearing the Fog of War – A critical analysis of recent energy sector cyberattacks in Denmark and Ukraine

Jos Wetzels | January 11, 2024

The “fog of war” is a military term used to denote the uncertainty and confusion experienced on the battlefield. During periods of growing geopolitical conflict, it becomes increasingly hard to keep pace with new developments.

With the goal of clearing the fog of war, Forescout Vedere Labs’ new threat briefing examines two recently published cyberattacks targeting the energy sector in Denmark and Ukraine, which have been attributed (or loosely connected) to the Russian military threat actor known as Sandworm, one of the most notorious APT groups in activity.

Our conclusions include the following:

- Our evidence suggests that the two waves of attacks on Danish infrastructure reported by SektorCERT, the Danish CERT for critical infrastructure, were unrelated. It also suggests that the second wave was simply part of a mass exploitation campaign against unpatched firewalls, not part of a targeted attack by Sandworm or another state-sponsored actor.
- Our data reveals that the campaign described as the “second wave” of attacks in Denmark started before, and continued after, the period reported by SektorCERT, targeting firewalls indiscriminately in a very similar way – only changing staging servers periodically. We see a prevalence of exploitation attempts in Europe, where nearly 80% of potentially vulnerable firewalls are located.
- There is little evidence that OT attacks using ‘living off the land’ (LotL) techniques are faster than approaches using custom malware. However, these techniques provide a stealth benefit to attackers and show that attackers continue to deploy new OT-oriented TTPs rather than rely on existing capabilities alone. There is also one previously undiscussed advantage to LotL: allowing attackers to abstract away from legacy and proprietary OT protocols that lack open-source implementations or extensive available documentation.
- We continue to see an increase in attacks leveraging vulnerabilities in network infrastructure devices. Poorly secured routers and firewalls, for instance, pose great risks to organizations. We advise organizations worldwide to prioritize securing these devices.

The findings of the report highlight the importance of correlating observed events with other sources of threat intelligence, such as malicious IPs and currently known exploited vulnerabilities. They also mean that critical infrastructure organizations all over Europe should remain alert to attacks on unpatched network infrastructure devices. **Dismissing these events as targeted to a specific country or specific organizations can be risky for other vulnerable organizations**.

The analysis of both incidents is detailed in the report. Below, we summarize the attacks on Denmark, their implications based on data observed from Forescout's Adversary Engagement Environment (AEE), and recommended risk mitigation actions.

Attacks on Zyxel firewalls in the energy sector

On November 13, 2023, SektorCERT published a report detailing how, between the 11th and 30th of May 2023, two waves of attacks gained access to the infrastructure of 22 companies in the Danish energy sector via vulnerabilities in their Zyxel firewalls. While the SektorCERT sensor network quickly noticed the attacks, allowing for a rapid response, the attackers reportedly had access to the industrial control systems of multiple companies, compelling some to go into island mode (operating without being connected to the energy grid).

The first wave of attacks exploited CVE-2023-28771 before there was a public exploit available and used exploit payloads specific to compromised devices, which suggests a potentially targeted attack (even if the exploit was trivial to develop).

The second wave saw attackers downloading Mirai botnet variants on the firewalls of victims starting on the 22nd of May 2023.

Our observations on the second wave of attacks

During the same period of the attacks on Danish infrastructure (more precisely May 24-26), we observed on our AEE (Adversary Engagement Environment) 12 attacks that were very similar to those mentioned in the SektorCERT report. All the attacks came from an IP address *not* mentioned in that report, but they all targeted CVE-2023-28771 and used exploits with similar payloads as a public proof of concept.

That IP address downloaded the same two files from the same staging servers mentioned in the SektorCERT report. Other researchers observed that one of the files was dropped by the same IP address around the same date (May 25th) following mass Internet scan of vulnerable Zyxel firewalls on May 20th (one day after the PoC publication and prior to the second wave of attacks on Danish infrastructure).

Another botnet sample mentioned in the report was also made available on an open malware sharing platform on May 27th, using an IP address that we also observed performing port scanning on the AEE as late as July (more than a month after the Danish attacks).

All of the above evidence points to the second wave of attacks on Danish organizations as being part of a larger campaign of indiscriminate botnet exploitation using a newly "popular" CVE, *not* a targeted attack or something related to the first wave. The first wave had used payloads specific to Zyxel and occurred before public proofs-of-concept were available.

Beyond Denmark: the risks of Zyxel networking devices on European critical infrastructure

Attacks on Zyxel devices are common. Prior to the incidents reported by SektorCERT, we observed on the AEE seven attempts to exploit CVE-2020-9054 and two attempts to exploit CVE-2022-30525 (previous vulnerabilities affecting Zyxel devices) between February 16 and May 14 of 2023. They all targeted our sensors in the United States.

We reported (above) how we observed attacks exploiting CVE-2023-28771 during the second wave of attacks on Danish organizations. However, *after* those reported incidents, we continued to observe other IPs exploiting the same vulnerability in a very similar way:

- 207.200[.]42, 109.207.200[.]43, 109.207.200[.]44, 109.207.200[.]47 between June 15 and June 21, using 185.180.199[.]41 as C2.
- 112.74[.]166 between August 24 and 25, using the same 185.180.199[.]41 as C2.
- 128.232[.]108 between September 1 and October 1, using 193.34.212[.]225 as C2.
- 54.51[.]106 between October 17 and 22, using the same 193.34.212[.]225 as C2.

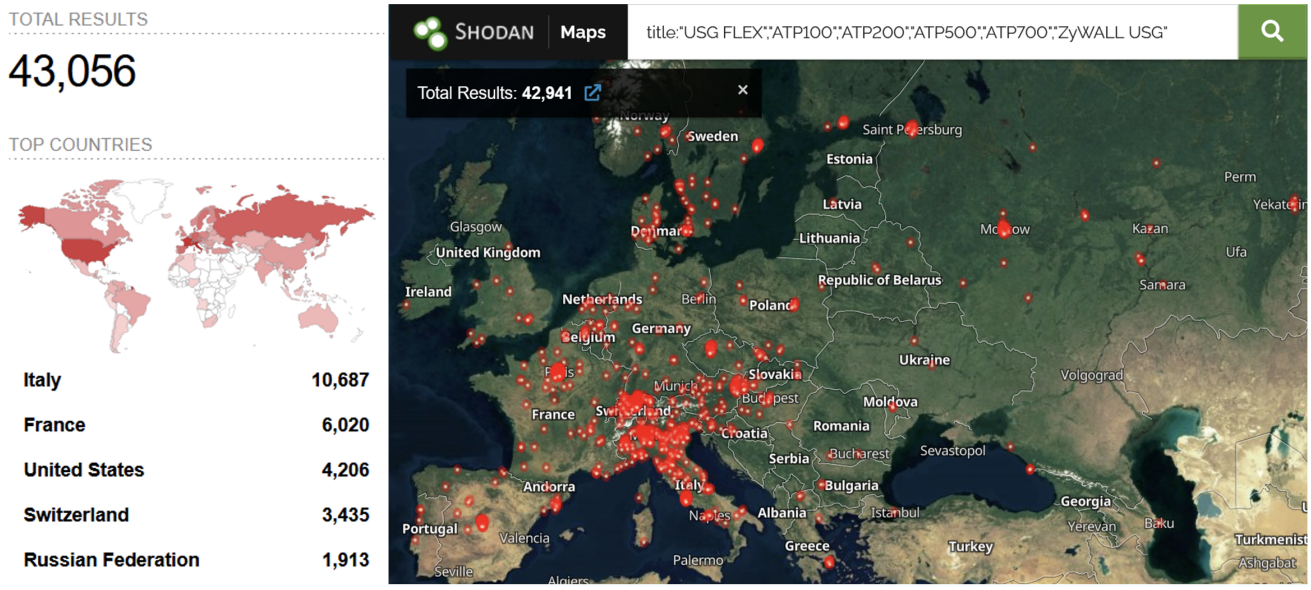
We also observed 193.34.212[.]225 (the last C2 server) performing *thousands* of scans on IKE port 500 between September 27th and October 29th. All the activity we saw in this period focused on our European sensors.

Although these attacks attempt to exploit a specific Zyxel vulnerability, their targeting is indiscriminate since they hit both real and simulated devices – Zyxel or not – that we host on the AEE. This is further evidence that exploitation of CVE-2023-27881, rather than being limited to Danish critical infrastructure, is ongoing and targeting exposed devices, some of which just happen to be Zyxel firewalls safeguarding critical infrastructure organizations.

This does not mean that these attacks deserve less attention. On the contrary, whether or not the operator behind a botnet is a nation-state, once initial access to networking infrastructure is obtained, the threat actor may choose to move further within the network and potentially reach the "crown jewels," such as sensitive information or operational technology.

Given that conventionally criminal mass-exploitation campaigns frequently resell or lease compromised devices as part of Initial Access Broker services, including specific access to OT systems, they may eventually end up in the hands of more targeted attackers. So, it is critical to remain vigilant.

There are more than 43,000 Zyxel firewalls currently exposed on Shodan. European organizations rely on Zyxel more than their counterparts in any other region of the world. **A massive 78% of the exposed Zyxel firewalls are in Europe, with 25% in Italy alone**. The only country outside Europe that has a significant presence of Zyxel firewalls is the U.S. (with approximately 10% of these devices)



Briefly looking at the organizations to which the IP addresses hosting these firewalls are registered, we see at least six in the power sector of different European countries, with a total of 161 firewalls, as well as an embassy and other municipal utilities on the continent. This is just a fraction of many other critical infrastructure organizations that will use these devices on IPs registered to their ISPs, for instance.

Conclusion and mitigation recommendations

There are two main takeaways from the analysis of these incidents targeting the energy sector:

1. While the Danish energy sector incident demonstrates the power of extensive network monitoring and a quick and coordinated response (no easy feat during massive exploitation campaigns), it also shows the uncertainty around attacker intent and incident seriousness that can arise during such an event. Distinguishing between a state-sponsored campaign targeted at disrupting critical infrastructure and crimeware mass-exploitation campaigns, and accounting for possible overlaps between the two, is easier in hindsight than in the heat of the moment. Yet, contextualization based on detailed threat and vulnerability intelligence can help security professionals identify where to focus. In addition, this incident demonstrates, once again, the frailty of perimeter security devices and the continuing need for complementary monitoring.

2. Rather than a major leap forward, the emergence of OT-oriented LotL TTPs in the October 2022 Ukrainian incident primarily represents a stealth benefit to attackers. This is due to the common lack of detection and hardening capabilities around native OT scripting functionality. It also shows attackers continue to deploy new OT-oriented TTPs rather than rely on existing capabilities alone.

The full report analysis and the above conclusions lead to several risk mitigation recommendations:

- **Identify, patch, and harden exposed network infrastructure/perimeter devices.** These devices are leveraged by threat actors both in targeted attacks and in mass-exploitation attempts. Keeping track of a growing number of vulnerabilities affecting these devices is a challenge. However, security teams must know which devices are exposed on their network perimeters and how they are vulnerable. They must be able to patch or mitigate them as soon as possible. Regardless of new vulnerabilities emerging in networking devices, they often have management interfaces and other services that should not be made available on the Internet. Ensure you have full visibility on what services are exposed and what credentials are used in those services.
- **Segment the network to prevent lateral movement from/to exposed assets.** There may be critical IT or OT devices connected directly to, or residing in, the same network as the exposed network infrastructure. It is important to limit communications from/to these perimeter devices as much as possible, possibly only to a limited list of trusted peers, to prevent attackers from moving deeper into the network from a newly compromised device.
- **Monitor OT networks to detect ongoing threats.** Even if a network is well-segmented, it is crucial to use OT-aware deep packet inspection solutions to monitor device communication. Such solutions can issue alerts whenever communications are known to be malicious or look suspicious, possibly indicating an attack. Although LotL makes it more difficult to detect anomalous communication using specific protocols, network monitoring allows for threat detection and response solutions to correlate multiple signals from the network, and possibly endpoints, to find incidents in real time.
- **Use up-to-date threat intelligence, such as malicious IPs and known exploited vulnerabilities.** This intelligence helps the network monitoring tools to detect malicious communications, files, and actions by matching those to known indicators. In the report, we provide a list of indicators of compromise that can be used to identify possible attacks coming from the campaign targeting Zyxel firewalls. These IoCs are also available on our public threat feed.

How Forescout helps

Forescout eyeInspect enables organization to identify devices using passive or active fingerprinting based on proprietary protocol matching or banners such as SSH, FTP, and HTTP. eyeInspect leverages specific fingerprinting capabilities for Zyxel devices.

eyeInspect also performs vulnerability matching based on the captured fingerprints to highlight vulnerable devices. It incorporates exploit detection tailored for vulnerabilities on network infrastructure devices such as Zyxel firewalls, Fortinet, Juniper, Cisco, and others.

The monthly updated threat intelligence database in eyeInspect includes the IOCs derived automatically from the analysis of botnets and other malware captured in Forescout Vedere Labs' AEE.

For more information, download the full report, "Clearing the Fog of War"
Download Report