

Clearing the Fog of War

A Critical Analysis of Recent
Energy Sector Attacks in
Denmark and Ukraine

January 11, 2024

Contents

- 1. Executive Summary 3
- 2. The Danish incidents: attacks on Zyxel firewalls in the energy sector 4
 - 2.1. First wave of attacks 4
 - 2.2. Second wave of attacks 5
 - 2.3. A critical analysis of both attack waves 7
 - 2.4. Beyond Denmark: the risks of Zyxel networking devices on European critical infrastructure 7
- 3. The Ukrainian incident: implications of new Sandworm TTPs targeting electricity substations 8
 - 3.1. Stealth 9
 - 3.2. Process comprehension 9
 - 3.3. Speed and scalability 10
 - 3.4. An additional benefit of LotL 10
- 4. Conclusions and recommended mitigations 11
- 5. Indicators Of Compromise (IOCs) 12

1. Executive Summary

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. This complicates analysis of new TTPs and makes it difficult to distinguish between targeted, state-sponsored attacks and conventional criminal activity leveraging new vulnerabilities. The past few months have shown that adversaries will take advantage of conflicts – even to advertise [attacks or entire campaigns](#) that did not actually take place – potentially leading defenders astray and increasing overall confusion. Thus, SOC teams may not be equipped with the right information to prioritize their investigations and proactive defensive activities.

With the goal of clearing this fog of war, we examine two recently published attacks targeting the energy sectors in Denmark and Ukraine. Thus far, the attacks have been attributed, or loosely connected, to the Russian military threat actor known as [Sandworm](#), one of the most notorious APT groups currently active.

Our conclusions include the following:

1. Evidence suggests that the two waves of attacks on Danish infrastructure reported by SektorCERT 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.
2. Our data reveals that the campaign described as the “second wave” of attacks on Denmark, started before, and continued after, the period reported by SektorCERT, targeting firewalls indiscriminately in a very similar manner, only changing staging servers periodically. We see a prevalence of exploitation attempts in Europe, where nearly 80% of publicly identifiable and potentially vulnerable firewalls are located.
3. There is little evidence that OT attacks using ‘living off the land’ (LotL) techniques are faster than approaches using custom malware. However, LotL techniques provide a stealth benefit to attackers and demonstrate that they continue to deploy new OT-oriented TTPs rather than rely on existing capabilities alone. There is also one previously undiscussed advantage to LotL techniques: enabling attackers to abstract away from legacy and proprietary OT protocols that lack open-source implementations or extensive available documentation.

These conclusions highlight the importance of correlating observed events with other sources of threat intelligence, such as malicious IPs and current known exploited vulnerabilities. The first and second conclusions are especially important because they indicate that critical infrastructure organizations across Europe should remain alert to attacks on unpatched network infrastructure devices. Dismissing these events as targeted to a specific country or organization(s) can put other vulnerable organizations at risk.

Analysis of both incidents highlights the increasing need for OT-specific network monitoring. With this in mind, we present mitigation recommendations and indicators of compromise (IOCs) at the end of this report.

What is Forescout's AEE?

Some observations in this report come from data in the **Vedere Labs Adversary Engagement Environment (AEE)**, a set of honeypots on the open internet luring attackers and recording their actions. The AEE is different from what is seen in many honeypots because it contains either real or simulated OT/IoT devices – including exposed protocols, banners and parts of the filesystem – instead of generic honeypots capturing every kind of attack.

Find out more about the AEE [on our website](#) and see how we use it [for our research](#).

2. The Danish incidents: attacks on Zyxel firewalls in the energy sector

On November 13, SektorCERT, the Danish CERT for critical infrastructure, [published a report](#) detailing what it calls “*the most extensive cyber-related attack [...] experienced [by critical infrastructure] in Denmark to date.*”

In that report, SektorCERT describes how, between the 11th and 30th of May 2023, two waves of attacks (loosely connected to Sandworm by the report's authors) managed to gain 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 some companies, forcing several to go into island mode (operating without being connected to the energy grid).

2.1. First wave of attacks

In the first wave of attacks, starting on the 11th of May 2023, a group of attackers exploited [CVE-2023-28771](#), a pre-authentication OS command injection vulnerability in the Internet Key Exchange (IKE) packet decoder of several unpatched Zyxel firewalls, reachable via port 500/UDP on the WAN interface, and resulting in a root shell.

This serious vulnerability was [first made public](#), together with available patches, on April 25th – more than two weeks before the attacks. Although the [first public writeup and PoC](#) were only made public on May 19th, a week after the first attack wave began, the exploit was fairly trivial. Even though the firmware was encrypted, potentially complicating differential patch analysis, a public bypass was available, allowing any moderately skilled attacker to develop an exploit in those two weeks. After achieving initial access, the exploited firewalls connected back to 46.8.198[.]196 and received a command to retrieve current usernames and configuration information.

The SektorCERT report mentions that, at the time of the first wave, no public information was available regarding which exposed Zyxel firewalls were vulnerable to CVE-2023-28771 and which were not, and no scans prior to the attack were observed. It is not feasible to determine the exact vendor, model, and firmware revision from IKE alone – though some [older coarse IKE fingerprinting](#) tooling exists. The [Metasploit module](#) for CVE-2023-28771 also lacks an IKE fingerprinting method.

However, at the time of writing this report, HTTP fingerprinting via [Shodan](#) shows approximately 43,000 Zyxel firewalls (700+ located in Denmark), and [Censys](#) shows 1,239 Zyxel firewalls in Denmark (with 687 exposing IKE). While the exact firmware revision cannot be determined beforehand, attackers could have built up a list of likely Zyxel firewalls from a mix of HTTP and coarse IKE fingerprints and simply assumed they were vulnerable. SektorCERT does not mention whether they are certain of the absence of exploitation attempts against non-vulnerable firewalls.

2.2. Second wave of attacks

In the second wave, starting on the 22nd of May 2023, (potentially different) attackers started downloading MIPS binaries over HTTP from 45.89.106[.]147 to Zyxel firewalls in a targeted energy sector organization. The binaries in question are Mirai variants containing indicators of the [Moobot](#) flavor.

After installing the malware, the firewalls started communicating on port 56999/TCP (a known C2 port for Mirai variants) with a server at “[www.joshan\[.\]pro](#)” (registered three weeks before the attack) resolving to 185.44.81[.]147. The firewalls then started participating in DDoS and SSH brute-force attacks against targets in Hong Kong, the U.S., and Canada. **Interestingly, one of the DDoS targets seems to be historically associated (through domain resolution both at the time of the attacks and prior to it) with infrastructure hosting many kinds of generic malware, such as adware and droppers.**

In the days after this initial attack of the second wave, Zyxel firewalls at other SektorCERT member organizations were observed similarly trying to download Mirai variants from various staging servers. **Investigation of these staging server IPs shows that they were historically associated with distribution of many kinds of malware, such as Mirai and BASHLITE/Gafgyt variants, adware, ransomware, as well as different campaigns, including Log4j exploitation attempts. In addition, some of the filenames under which the malware was dropped appear in 3-year old public code of a QBot variant.** Successful infection of the firewalls was followed by C2 communications with the same IP on port 56999/TCP.

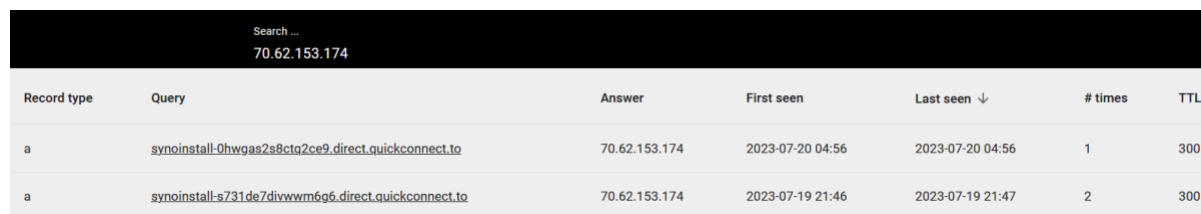
During the same period when the attacks on Danish infrastructure were occurring (more precisely on May 24-26), we observed, within our AEE, 12 attacks that were very similar to the ones mentioned in the SektorCERT report. All these attacks came from 109.207.200[.]43, an address not mentioned in that report. All the attacks targeted CVE-2023-28771 and used exploits with similar payloads, indicating that they were adapted from a [public proof of concept](#). Exactly as reported by SektorCERT, those IPs downloaded two files from staging servers: [http://145.239.54\[.\]169/mipskiller](#) and [http://91.235.234\[.\]81/proxy2](#) (these servers and files are the same as those shown in that report). We also observed one exploit that had a single “reboot” command as payload, which was not reported by SektorCERT. The “mipskiller” payload is a Mirai botnet variant and was also observed being dropped by the same IP address by [other researchers](#), around the same date (May 25). This was subsequent to a [mass Internet scan](#) for vulnerable Zyxel firewalls on May 20 – a day after the PoC publication and prior to the second wave of attacks on Danish infrastructure.

The botnet sample [http://45.128.232\[.\]143/bins/paraiso.mips](#) that was described in the SektorCERT report was made available on [MalwareBazaar](#) on May 27. Several other similar samples for different architectures coming from the same staging server were also observed on May 27, such as [paraiso.arm5](#), [paraiso.arm6](#), [paraiso.mpsl](#), [paraiso.x86](#), which is common for botnets that exploit devices running on multiple architectures. This same IP address was also seen dropping [another unrelated botnet sample](#) shortly after the attacks (on June 2), and we observed it performing port scanning on our AEE as late as July (more than a month after the Danish attacks).

Another sample related to those dropped in the Danish incident was made available on [MalwareBazaar](#) on June 13, shortly after the attacks. The sample is [205.147.101\[.\]170/fuckjewishpeople.x86](#), whereas the .mips version downloaded from the same server was observed by SektorCERT.

All the above evidence points to the second wave of attacks on Danish organizations being part of a larger campaign of indiscriminate botnet exploitation using a newly “popular” CVE, rather than a targeted attack or something related to the first wave, which had used payloads specific to Zyxel and had happened before public proofs-of-concept were available.

Among this activity, SektorCERT also observed traffic, consisting of two single 1340-byte packets, on ports 10049/TCP and 20600/TCP to the IPs 217.57.80[.]18 and 70.62.153[.]174. Since those IPs have been historically associated with C2 infrastructure for the Sandworm-attributed Cyclops Blink malware, this raised alarm at SektorCERT. Since Cyclops Blink has been known to target WatchGuard and ASUS network devices. Both of those C2 IPs have since been reported by the Romanian National Cyber-Security Directorate as part of the infrastructure of the Katana Mirai variant botnet which has been associated with DDoS attacks against Ukraine as well as exploitation of CVE-2023-28771. We observed on passive DNS databases that in July, shortly after the attacks, one of the “Sandworm” IPs was probably used by a Synology NAS device, as shown in the figure below. This means that the connection to Sandworm is very thin, since this IP address could simply be a compromised device, part of a broader IoT botnet with shared APT/criminal infrastructure.



The screenshot shows a search for the IP address 70.62.153.174. The results table contains two entries:

| Record type | Query | Answer | First seen | Last seen ↓ | # times | TTL |
|-------------|---|---------------|------------------|------------------|---------|-----|
| a | synoinstall-0hwggs2s8ctq2ce9.direct.quickconnect.to | 70.62.153.174 | 2023-07-20 04:56 | 2023-07-20 04:56 | 1 | 300 |
| a | synoinstall-s731de7divwwm6g6.direct.quickconnect.to | 70.62.153.174 | 2023-07-19 21:46 | 2023-07-19 21:47 | 2 | 300 |

One of the unexplained aspects of this second wave is the initial access vector into the Zyxel firewalls. SektorCERT assesses this was likely achieved by exploiting two new vulnerabilities, CVE-2023-33009 and CVE-2023-33010 (disclosed on May 24). This would make the vulnerabilities zero-days at the time of supposed exploitation. While they have since been added to CISA Known Exploited Vulnerabilities (KEV) catalog, there is still no public PoC available (as of December 2023). Given that they are both buffer overflow vulnerabilities, rather than the far easier to exploit command injection of CVE-2023-28771, this is inconsistent with the rest of the second wave attacks. We find it difficult to believe that anyone would waste such a capability on an approach as sloppy as the second wave of attacks.

The SektorCERT report does conclusively state whether or not the second wave targets were hit by CVE-2023-28771. Notably, the second attack wave started only days after the Metasploit module for CVE-2023-28771 was made public, an event which has led to mass exploitation by Mirai-based botnets. Alternatively, the second wave targets could have been compromised previously, for instance during the first wave, gone unnoticed, with access handed over to Mirai botnet operators.

All the activity we see around that time on the AEE exploiting Zyxel firewalls *is*, in fact, leveraging CVE-2023-28771, which, coupled with the discussion above about this being an indiscriminate attack mistaken for a targeted incident, indicates that the botnet activity observed by SektorCERT was likely leveraging CVE-2023-28771. Any evidence to the contrary would strongly suggest a more targeted attack.

2.3. A critical analysis of both attack waves

The SektorCERT report states, “*whether Sandworm was involved in the attack cannot be said with certainty. Individual indicators of this have been observed, but we have no opportunity to neither confirm nor deny it*”.

Below are the conclusions we can reach based on the shared report, the evidence from our AEE, and other information obtained from open sources:

- The first wave exploited a straightforward, if PoC-less, n-day against a limited number of targets. This was followed by constrained information retrieval behavior.
- The second wave consisted of Zyxel firewalls becoming infected via unexplained means from staging servers with a broad mass exploitation and crimeware history. The connection to Sandworm is very thin. The C2 IPs in question have also been associated with the Katana botnet, and while shared infrastructure between criminal and state-sponsored operators cannot be ruled out, the behavior of the infected firewalls (immediate DDoS and SSH brute-forcing – including against targets with dubious reputations themselves) corresponds more to crimeware botnet-building than to state-attributed campaigns looking to infiltrate critical infrastructure.
- There is no direct connection between the first and second attack waves.

It is likely that the second wave was part of regular mass exploitation by botnets which happened to catch the Danish energy sector in its wide net, rather than targeting it specifically. The first wave is less clear and more sophisticated than the second. Attackers had to create their own exploit and show more constrained behavior. As such, a specific focus on critical infrastructure cannot be ruled out. But there seems to be no direct link to Sandworm.

2.4. 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 from the following IPs: 27.19.56[.]44, 179.43.145[.]90, 123.26.149[.]179, 77.64.229[.]43 and 193.32.162[.]159. They all targeted our sensors in the United States.

As we reported in section 2.2, 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 the following IPs exploiting the same vulnerability in a very similar way:

- 109.207.200[.]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.
- 64.112.74[.]166 between August 24 and 25, using the same 185.180.199[.]41 as C2.
- 45.128.232[.]108 between September 1 and October 1, using 193.34.212[.]225 as C2.
- 84.54.51[.]106 between October 17 and 22, using the same 193.34.212[.]225 as C2.

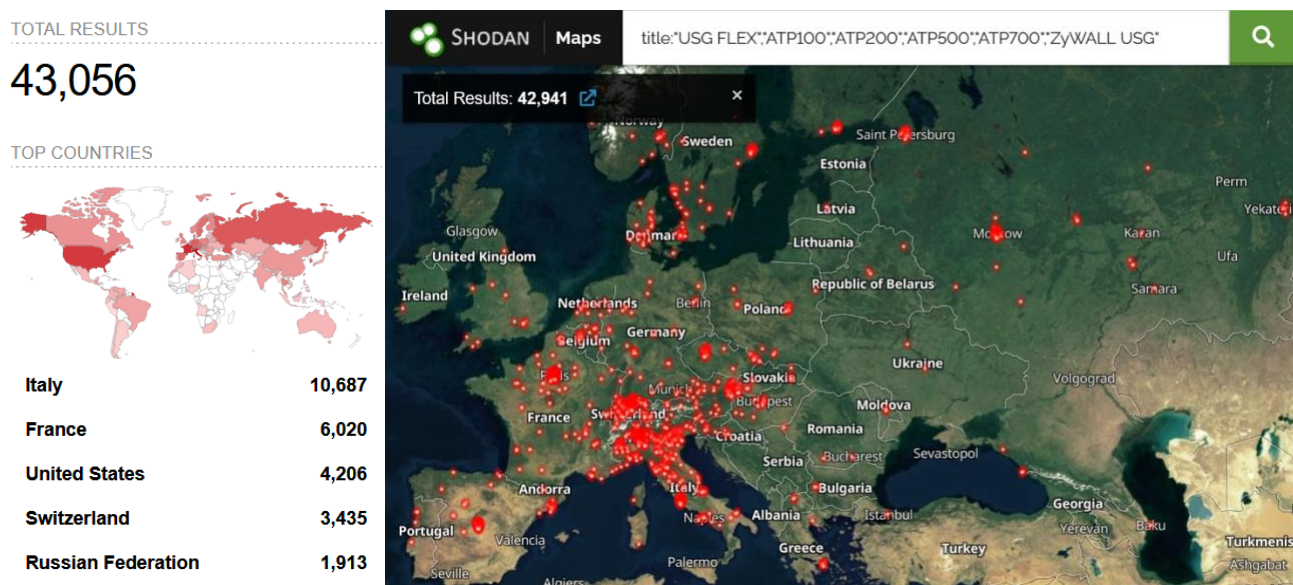
We also observed 193.34.212[.]225 (the last C2 server) performing *thousands* of scans on IKE port 500 between September 27 and October 29. All the activity we saw in this period focused on our European sensors.

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 happen to be Zyxel firewalls safeguarding critical infrastructure organizations.

This does not mean that these attacks deserve less attention. On the contrary, whether the operator behind a botnet is state-affiliated or not, 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 conventional 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. This makes remaining vigilant critical.

As noted above, 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 of Europe that has a significant presence of Zyxel firewalls is the U.S., with approximately 10% of these devices. (See image below).



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 the critical infrastructure organizations that will use these devices on IPs registered to their ISPs.

3. The Ukrainian incident: implications of new Sandworm TTPs targeting electricity substations

On November 9, Mandiant [released a blog post](#) detailing their response to two disruptive events at a Ukrainian electricity substation in mid-October 2022. In the incident, the attackers – attributed by Mandiant to Sandworm – tripped the substation circuit breakers to cause a power outage that coincided with a series of Russian missile strikes across Ukraine. The incident was part of a [larger wave of simultaneous cyber and missile attacks](#) on Ukrainian critical infrastructure in 2022 that included the [Industroyer2](#) attack – also attributed to Sandworm.

One aspect worth highlighting from the October 2022 incident is Sandworm's use of a new TTP. Unlike the original [Industroyer](#) and [Industroyer2](#) incidents, where circuit breakers were opened via IEC-104 telecontrol protocol messages, the 2022 attackers used native SCADA scripting capabilities.

The attackers compromised a hypervisor instance hosting the [MicroSCADA](#) (produced by Hitachi Energy, previously ABB) instance for the targeted substations and executed a malicious [Supervisory Control Implementation Language \(SCIL\)](#) script via the native `scilc.exe` utility ([T0807](#), [T0871](#)). This utility is an interpreter for the proprietary SCIL language which allows operators to automate interactions with the MicroSCADA environment. While unable to retrieve the malicious script due to anti-forensic measures employed by the attackers, Mandiant assessed that it likely consisted of a series of commands to open circuit breakers ([T0855](#), [T0831](#)) which MicroSCADA would translate to telecontrol commands to the RTU, for instance via IEC-104/101.

In the paragraphs below, we compare this LotL approach to the manual HMI interaction of the [2015 Sandworm attacks on Ukraine](#) and the custom malware approach of the original [Industroyer](#) and [Industroyer2](#) attacks. For more details about [Industroyer2](#), see our [dedicated analysis](#).

3.1. Stealth

The use of native utilities, especially a proprietary scripting language, is certainly stealthier than custom executable malware. It is unlikely that XDR solutions will raise alerts on malicious scripts in such proprietary scripting languages, neither while the script is in transit nor as it is executing natively. In addition, depending on an attacker's implementation, a SCIL approach could compare favorably in terms of stealth to [Industroyer's](#) noisy IEC-104 *Information Object Address* (IOA) brute-forcing approach.

3.2. Process comprehension

This LotL approach benefits an attacker with regards to [process comprehension](#) requirements, such as the need to understand significant parts of the target system and physical process:

- First, unlike with [Industroyer](#), attackers do not have to communicate directly with RTUs nor do they have to know brute-force telecontrol addressing information like IEC-104 IOAs.
- Second, SCIL enables attackers to automatically list MicroSCADA application objects, including *Process objects* (e.g., switches, sensors and breakers), associated with *Process stations*, such as RTUs, PLCs, and IEDs, that fulfill given conditions and type criteria (e.g., listing all breakers), and read and set their attributes, such as breaker positions, via SCIL statements.

This enables attackers to blindly enumerate breakers and open them without knowing the particulars of a given substation configuration, [Industroyer](#) already had such a fire-and-forget capability, albeit noisier and cruder. In addition, if an attacker wishes to achieve a particular outcome, such as causing outages at *specific* substations, this approach still requires some degree of non-automated process comprehension, such as knowing the correct station numbers.

3.3. Speed and scalability

While certainly faster and more accurate than the manual HMI-based approach of the 2015 attacks, a native script does not necessarily get the job done faster than custom malware.

It has been argued that this LotL approach is both nimbler and less development-time-intensive than attacks driven by custom malware. While Mandiant reported that the October 2022 incident unfolded over a short period (with access reportedly being obtained only 3 months prior to the power outage), it is unclear whether this was due to less complex attack requirements or highly compressed timelines arising from battlefield conditions. While some of the deployed scripts reportedly had timestamps dating back to September 2022, suggesting the attackers may have developed the SCIL-capability only 2 months after initial access, it is equally likely that the attackers already possessed such a capability and simply created the launch scripts after deciding upon execution timelines and targets.

Since the threat actor needs to learn a new proprietary scripting language, development of the SCIL capability could have been performed in advance (a sensible investment given the popularity of MicroSCADA in the electricity sector). By contrast, while developing custom malware capabilities for OT protocols seems far more development intensive, [prior reporting by Forescout Vedere Labs on Industroyer2](#) and by Mandiant on [COSMICENERGY](#) suggests that both lifted their IEC-104 protocol implementations from open-source projects. Therefore, this data alone does not conclude which approach is more time intensive.

3.4. An additional benefit of LotL

One previously unmentioned benefit of the LotL approach is that it abstracts away from legacy and proprietary OT protocols. While most modern substations typically use the likes of IEC-104/101, IEC 61850, and/or DNP3, there still exist many older substations where one may encounter protocols like [RP-570/571](#), SINAUT, or one of the Telegyr flavors, *all of which lack easy to copy-paste open-source protocol stack implementations*. This benefit is even more pronounced when targeting Distributed Control Systems (DCS) rather than SCADA, given that the former are dominated by proprietary protocols. Simply reverse-engineering such protocols takes anywhere from weeks to six months, as shown by [prior Forescout Vedere Labs research](#).

Many SCADA and DCS solutions have native scripting capabilities that are similar to MicroSCADA's SCIL. Typically, the former consist of server and/or HMI scripting engines that allow for automation code to be run either directly or by a trigger, such as time or condition. Examples include:

- IEC 61131-3 capabilities in [Siemens SICAM PAS](#) and [Schneider GeoSCADA](#) servers
- VBA and/or VBS capabilities in [Siemens WinCC / SICAM SCC](#), [Schneider GeoSCADA](#), [GE iFix](#), [Honeywell Experion LX](#), and [ABB 800xA](#)
- Proprietary scripting languages in [VTScada](#) and [Siemens WinCC OA / PVSS](#)

4. Conclusions and recommended mitigations

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

1. While the Danish energy sector incident shows 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 the level of 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 more easily done in hindsight than in real time. Contextualization based on detailed threat and vulnerability intelligence can help security professionals identify where to focus. In addition, this incident shows 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 due to the common lack of detection and hardening capabilities around native OT scripting functionality. It also shows attackers continue to develop new OT-oriented TTPs rather than rely solely on existing capabilities.

The analysis in this report and the conclusions above inform several 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 that affect these devices is a challenge. Yet, security teams must be aware of which devices are exposed on their network perimeters and how they are vulnerable. They must be able to patch or mitigate as soon as possible. Regardless of new vulnerabilities emerging in networking devices, they often have exposed management interfaces and other services that should not be made available on the Internet. Ensure you have full visibility of the services that are exposed and which 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 **set** 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 and could indicate 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 endpoints, to find incidents in real time.
- **Use up-to-date threat intelligence, such as malicious IPs and known exploited vulnerabilities.** This intelligence helps network monitoring tools to detect malicious communications, files, and actions by matching against known indicators. Below, we provide a list of indicators of compromise (IoCs) that can be used to identify potential attacks related to the campaign targeting Zyxel firewalls. These IoCs are also available on our [public threat feed](#). We do not include the original SektorCERT IoCs, which can be obtained from [their report](#), nor the Sandworm IoCs, which can be obtained from Mandiant's [blog post](#) on the topic.

5. Indicators Of Compromise (IOCs)

| Indicator | Type |
|---|------|
| 109.207.200[.]43 | IPv4 |
| http://145.239.54[.]169/mipskiller | URL |
| http://91.235.234[.]81/proxy2 | URL |
| 45.128.232[.]143 | IPv4 |
| http://45.128.232[.]143/bins/paraiso.mips | URL |
| http://45.128.232[.]143/bins/paraiso.arm5 | URL |
| http://45.128.232[.]143/bins/paraiso.arm6 | URL |
| http://45.128.232[.]143/bins/paraiso.mpsl | URL |
| http://45.128.232[.]143/bins/paraiso.x86 | URL |
| http://45.128.232[.]143/.router/twitter | URL |
| 27.19.56[.]44 | IPv4 |
| 77.64.229[.]43 | IPv4 |
| 123.26.149[.]179 | IPv4 |
| 179.43.145[.]90 | IPv4 |
| 193.32.162[.]159 | IPv4 |
| 109.207.200[.]42 | IPv4 |
| 109.207.200[.]43 | IPv4 |
| 109.207.200[.]44 | IPv4 |
| 109.207.200[.]47 | IPv4 |
| 185.180.199[.]41 | IPv4 |
| 64.112.74[.]166 | IPv4 |
| 45.128.232[.]108 | IPv4 |
| 193.34.212[.]225 | IPv4 |
| 84.54.51[.]106 | IPv4 |
| ddf33ab2a548d8cd5eac19b7ead99f94 | MD5 |
| 3c7d50169783e17c6951388c409f0ee2 | MD5 |
| d7d965dce3b520475a53918495d041ca | MD5 |
| 5b41cfbeba46bce34b90a3f3e1d7e9a1 | MD5 |
| 405f380654dc6eb1d9816f89ad702c19 | MD5 |
| c89b1d07cdbe80d9c6d885b5243de139 | MD5 |

© 2024 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products or service names may be trademarks or service marks of their respective owners. 01_01