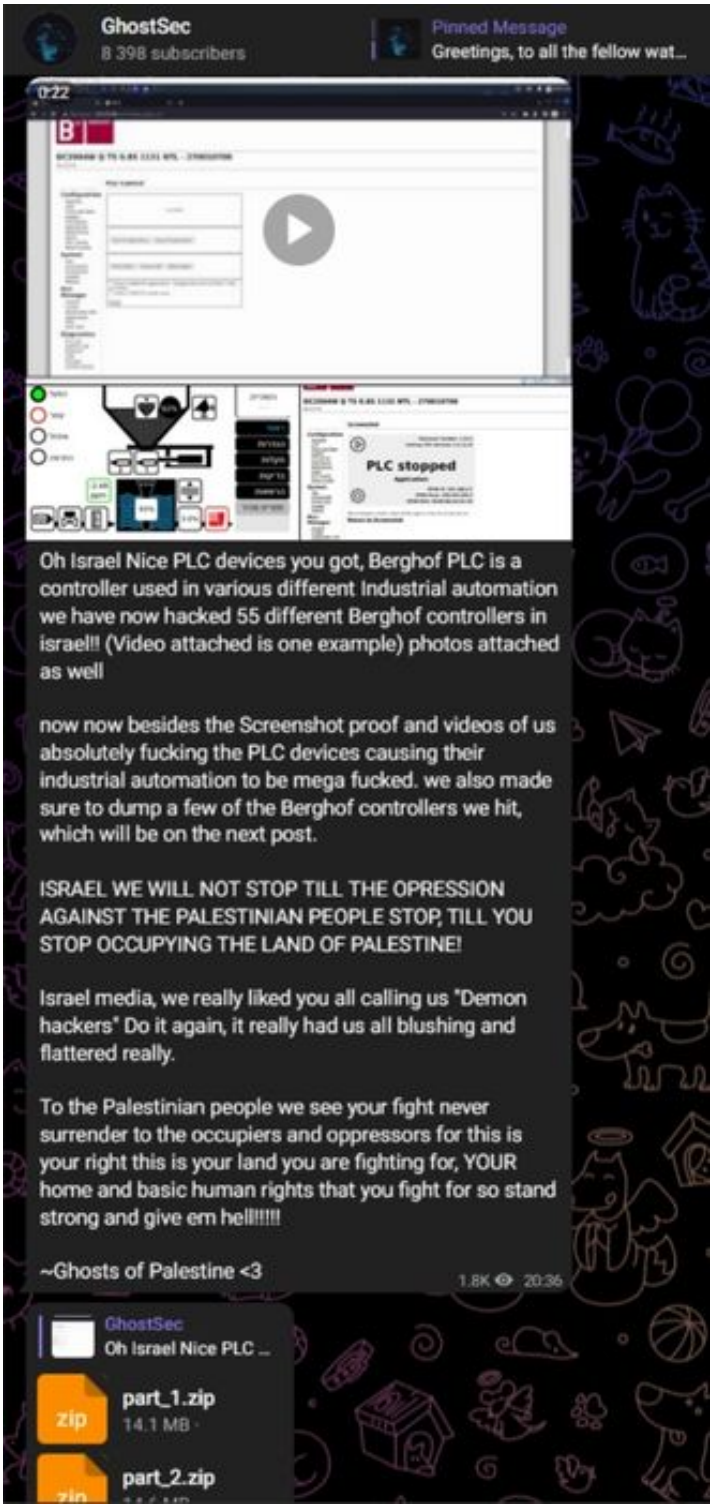
Pro-Palestinian Hacking Group Compromises Berghof PLCs in Israel

otorio.com/blog/pro-palestinian-hacking-group-compromises-berghof-plcs-in-israel/

By David Krivobokov, Research Team Leader

Overview: Berghof PLCs being compromised

On September, 4th, 2022, a hacktivist group “GhostSec” that was previously observed targeting Israeli organizations and platforms, announced on social media and its Telegram channel that the group successfully breached 55 Berghof PLC devices in Israel.

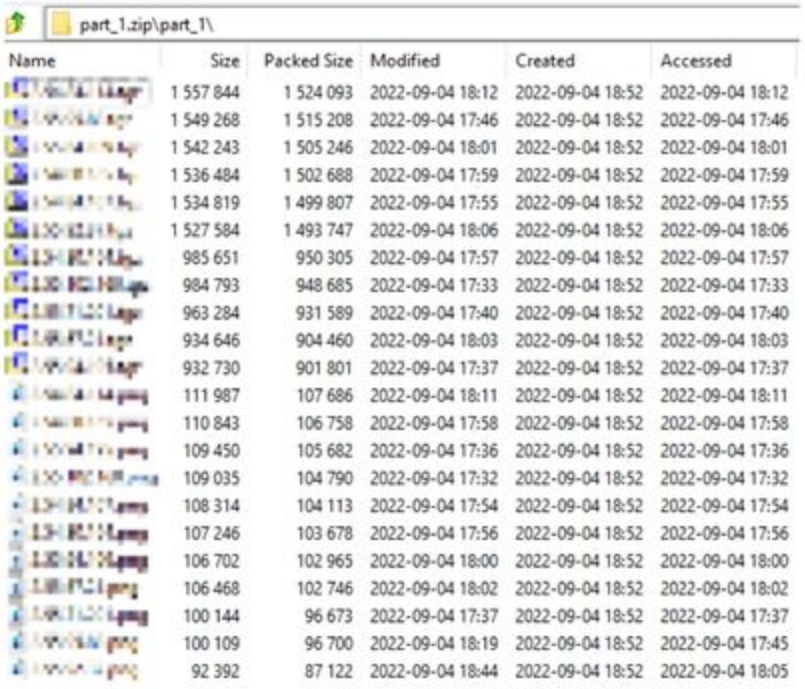


In the message it published, GhostSec attached a video demonstrating a successful log-in to the PLC's admin panel, together with an image of an HMI screen showing its current state and control of the PLC process, and another image showing that the PLC had been stopped. In the following message *(inset)* the group published the dumped data from the breached PLCs.

OTORIO's Research group decided to further investigate the details of this incident with the goal of understanding how "GhostSec" was able to gain control over these PLCs and assess the underlying risks.

Diving Into The Breach's Artifacts

Observing the published system dump of ZIP archives (part_1.zip and part_2.zip) revealed the public IP addresses *(below)* of the affected PLCs. This suggests that the devices were/are publicly exposed to the internet.

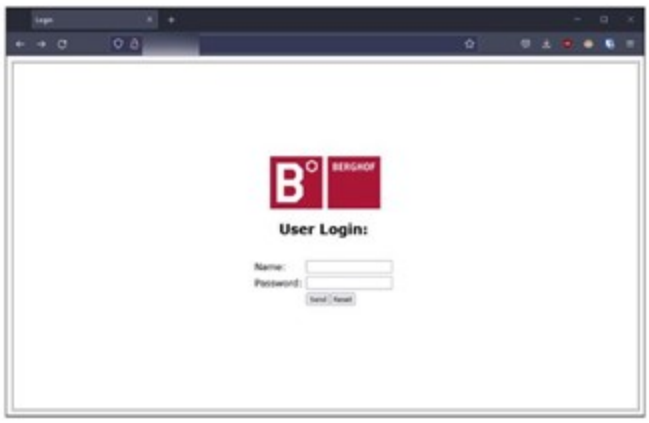


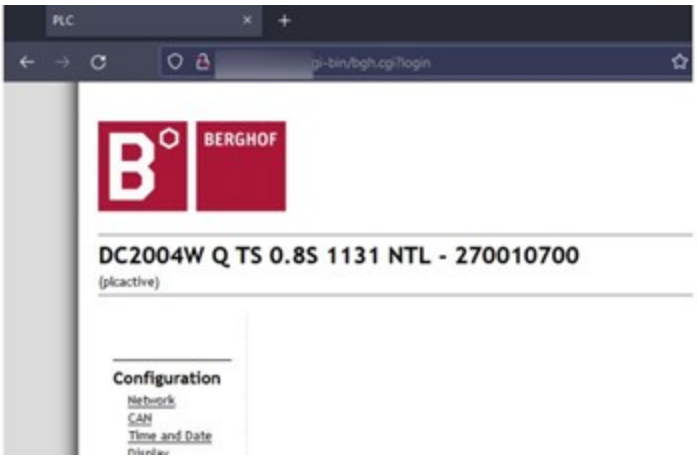
Name	Size	Packed Size	Modified	Created	Accessed
[redacted]	1 557 844	1 524 093	2022-09-04 18:12	2022-09-04 18:52	2022-09-04 18:12
[redacted]	1 549 268	1 515 208	2022-09-04 17:46	2022-09-04 18:52	2022-09-04 17:46
[redacted]	1 542 243	1 505 246	2022-09-04 18:01	2022-09-04 18:52	2022-09-04 18:01
[redacted]	1 536 484	1 502 688	2022-09-04 17:59	2022-09-04 18:52	2022-09-04 17:59
[redacted]	1 534 819	1 499 807	2022-09-04 17:55	2022-09-04 18:52	2022-09-04 17:55
[redacted]	1 527 584	1 493 747	2022-09-04 18:06	2022-09-04 18:52	2022-09-04 18:06
[redacted]	985 651	950 305	2022-09-04 17:57	2022-09-04 18:52	2022-09-04 17:57
[redacted]	984 793	948 685	2022-09-04 17:33	2022-09-04 18:52	2022-09-04 17:33
[redacted]	963 284	931 589	2022-09-04 17:40	2022-09-04 18:52	2022-09-04 17:40
[redacted]	934 646	904 460	2022-09-04 18:03	2022-09-04 18:52	2022-09-04 18:03
[redacted]	932 730	901 801	2022-09-04 17:37	2022-09-04 18:52	2022-09-04 17:37
[redacted]	111 987	107 686	2022-09-04 18:11	2022-09-04 18:52	2022-09-04 18:11
[redacted]	110 843	106 758	2022-09-04 17:58	2022-09-04 18:52	2022-09-04 17:58
[redacted]	109 450	105 682	2022-09-04 17:36	2022-09-04 18:52	2022-09-04 17:36
[redacted]	109 035	104 790	2022-09-04 17:32	2022-09-04 18:52	2022-09-04 17:32
[redacted]	108 314	104 113	2022-09-04 17:54	2022-09-04 18:52	2022-09-04 17:54
[redacted]	107 246	103 678	2022-09-04 17:56	2022-09-04 18:52	2022-09-04 17:56
[redacted]	106 702	102 965	2022-09-04 18:00	2022-09-04 18:52	2022-09-04 18:00
[redacted]	106 468	102 746	2022-09-04 18:02	2022-09-04 18:52	2022-09-04 18:02
[redacted]	100 144	96 673	2022-09-04 17:37	2022-09-04 18:52	2022-09-04 17:37
[redacted]	100 109	96 700	2022-09-04 18:19	2022-09-04 18:52	2022-09-04 17:45
[redacted]	92 392	87 122	2022-09-04 18:44	2022-09-04 18:52	2022-09-04 18:05

Both archives contained the same types of data – system dumps and HMI screenshots, which were exported directly from the Berghof admin panel. The panel has this functionality by design, allowing logged-in users to create a backup and see the current HMI state via a screenshot.

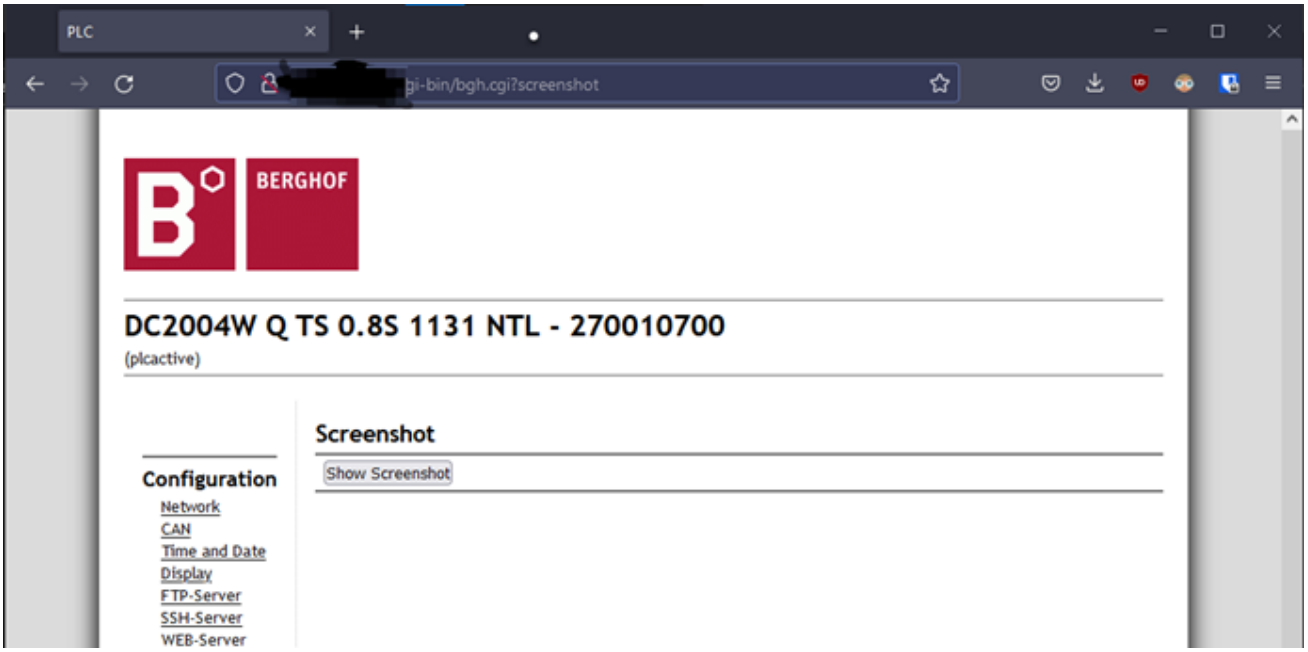
How were the Berghof PLCs Breached?

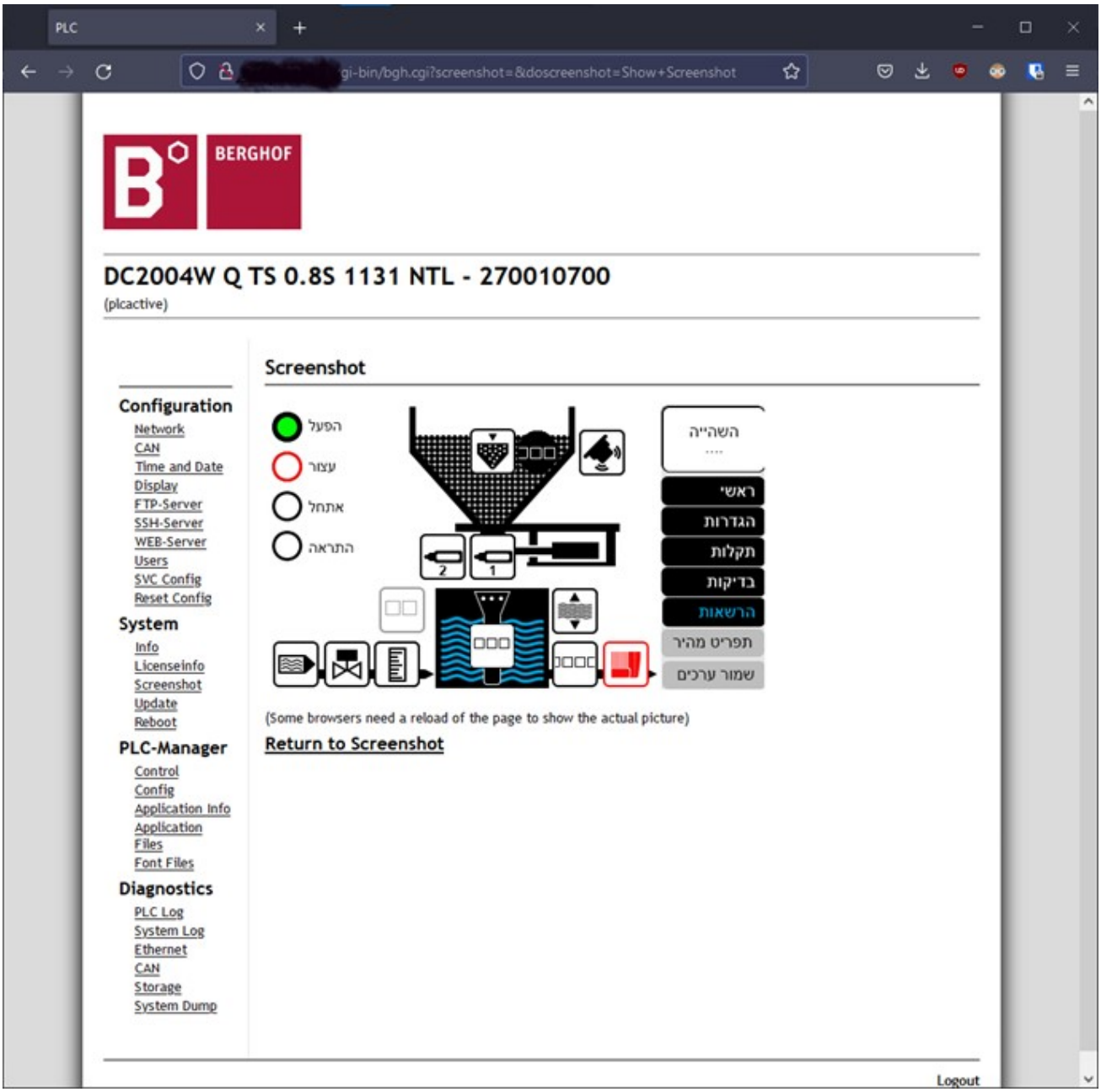
At the time of our investigation, the IPs were still accessible through the Internet. Access to the admin panel is password-protected. However, trying a few default and common credentials resulted in a successful login.



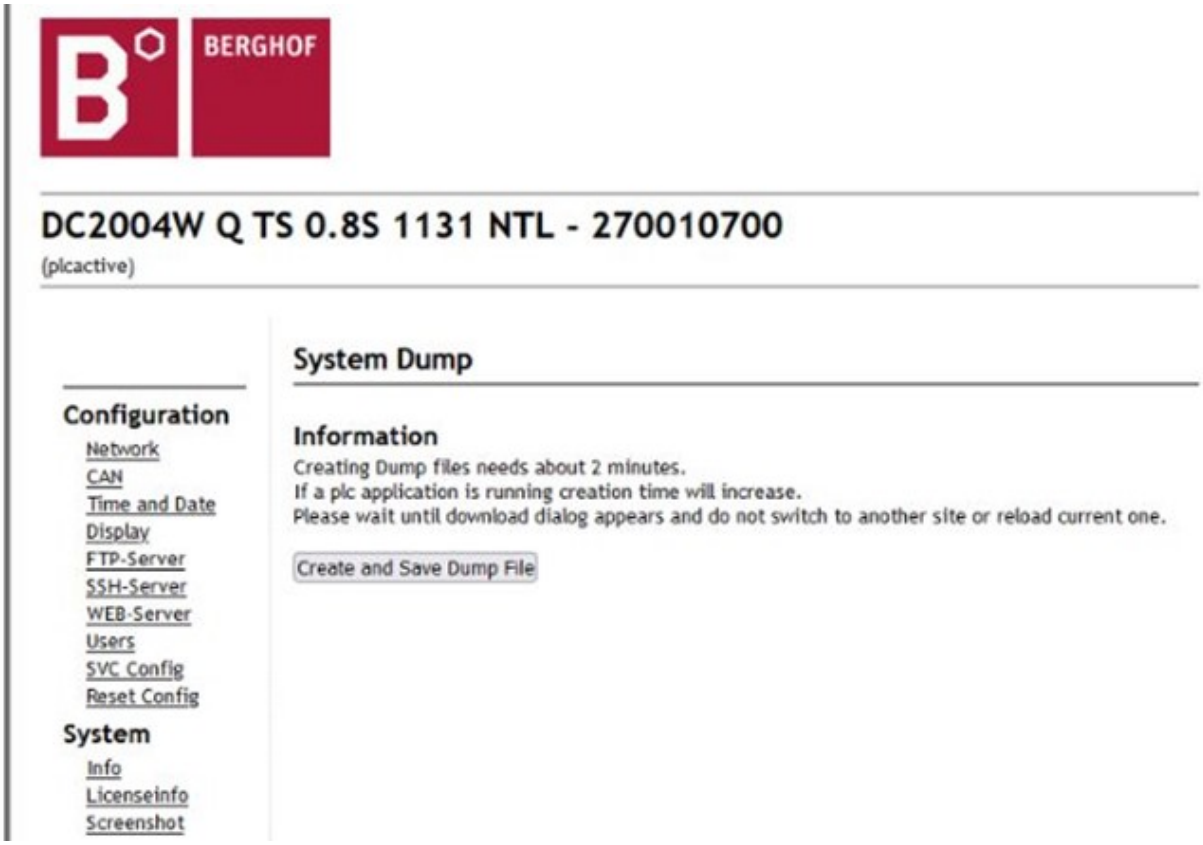


The HMI screenshots can be taken and viewed simply by accessing the “Screenshot” tab:





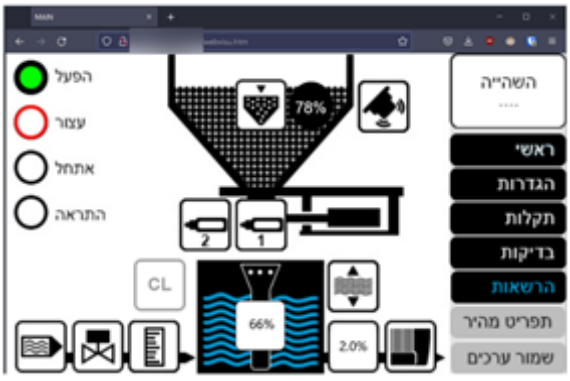
The system dumps were similarly done by just accessing the “System Dump” tab in the admin panel:



Although access to the admin panel provides full control over some of the PLC's functionality, it does not provide direct control over the industrial process. It is possible to affect the process to some extent, but the actual process configuration itself isn't available solely from the admin panel.

Does GhostSec have OT Capabilities?

From our research, we concluded that Berghof uses CODESYS technology as its HMI, and is also accessible via the browser at a certain address. From our observations of GhostSec's proofs of breach, we did not know whether GhostSec gained access to the HMI. But we've confirmed that the HMI screen was also publicly available.



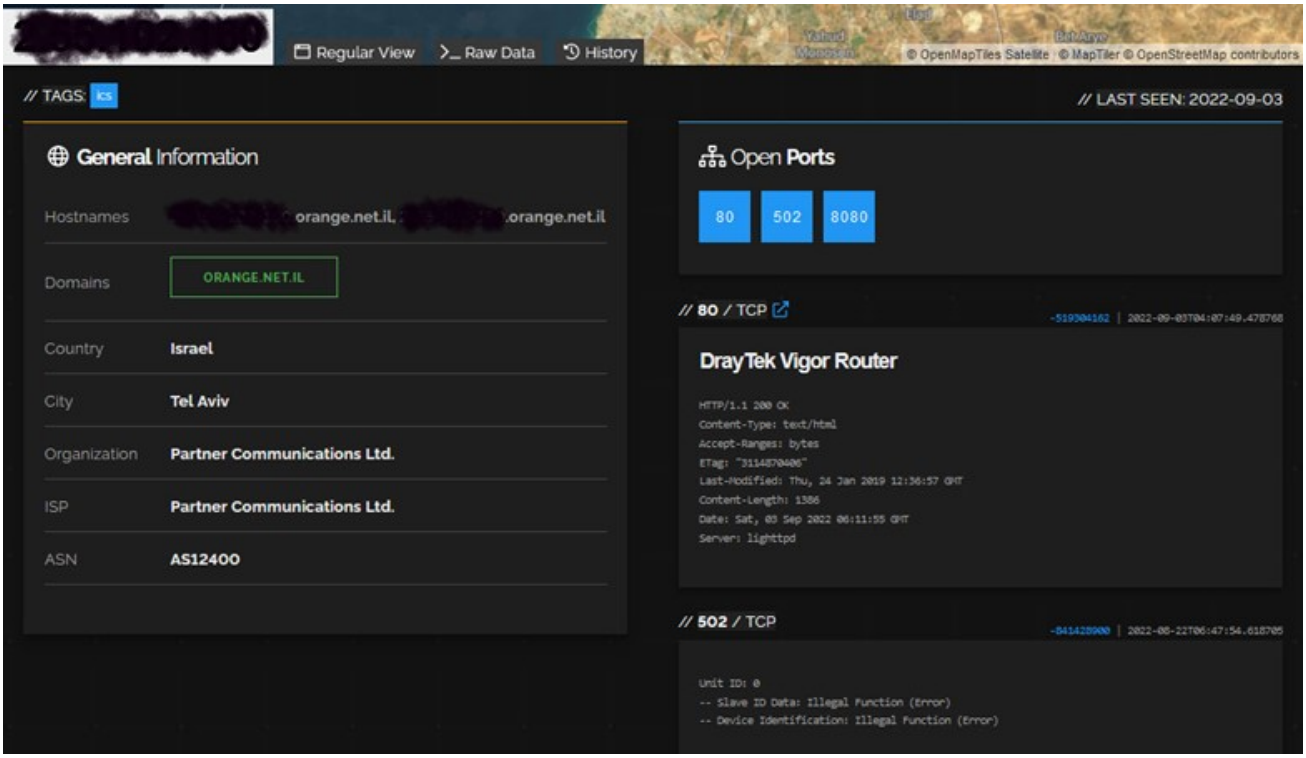
The HMI exposes the configuration of the industrial process:

With Shodan Anyone Can Be a Hacker

Communication in industrial networks is maintained over dedicated industrial protocols. Looking at the scanning results in the Shodan, search engine for Internet-connected devices shows that this PLC has few open ports:

- 80 - HTTP
- 8080 - HTTP

- 502 – Modbus



While the HTTP ports provide access to web services, Modbus is the industrial protocol. Modbus allows transferring data between the PLC to the HMI/SCADA systems, as well as probing and changing its values.

Conclusion

Unlike cyber attacks on IT infrastructure, OT security breaches can be extremely dangerous since they can affect physical processes and, in some cases, even lead to life-threatening situations.
While GhostSec's claims are of a sophisticated cyber attack, the incident reviewed here is simply an unfortunate case where easily overlooked misconfigurations of industrial systems led to an extremely unsophisticated attempt to breach the systems themselves.

The fact that the HMI probably wasn't accessed, nor manipulated by GhostSec, and the hackers were not exploiting the Modbus interface, shows an unfamiliarity with the OT domain. To the best of our knowledge, GhostSec hadn't brought critical damage to the affected systems, but only sought to draw attention to the hacktivist group and its activities.

Despite the low impact of this incident, this is a great example where a cyber attack could have easily been avoided by simple, proper configuration. Disabling the public exposure of assets to the Internet, and maintaining a good password policy, especially changing the default login credentials, would cause the hacktivists' breach attempt to fail.
OTORIO"s **reconOT** helps critical infrastructure companies and industrial manufacturers prevent these kinds of breaches, whether of Berghof PLCs or those from other manufacturers. It does so via automatic, OT-centric reconnaissance to discover a company's assets as they are seen by a potential attacker.

To learn more, **contact** OTORIO's OT security professionals.