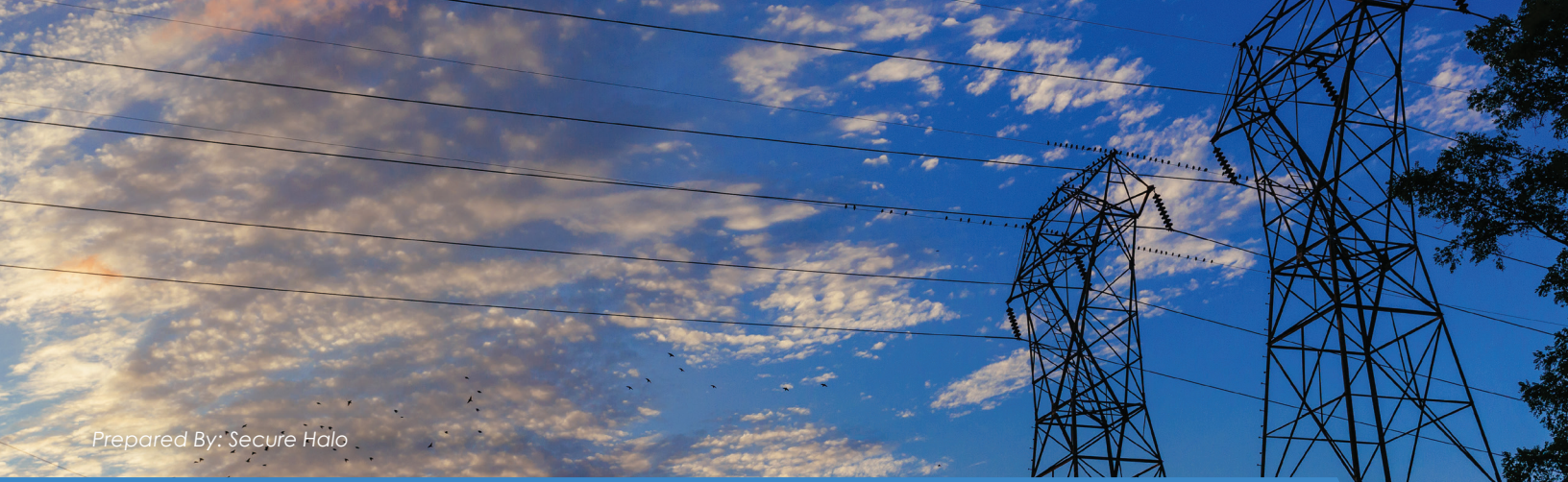

Prepared By: Secure Halo

McGRIFF, SEIBELS & WILLIAMS, INC.

CYBER INSIGHTS

SECURE HALO
SECURING THE ENTERPRISE

DRAGONFLY 2.0 SHOWS ENERGY COMPANIES REMAIN IN GEOPOLITICAL CROSSHAIRS

A recent report by Symantec security researchers generated a flurry of news stories that the U.S. and European energy sector is being targeted by hackers who may now have the ability to sabotage operational systems. Symantec said the group, known as Dragonfly or Energetic Bear, has carried out a multi-year campaign, from 2011 to 2014 and again from 2015 to present, with a "distinct increase in activity in 2017."

The Symantec report reaffirms the presence of attacks aimed at the energy sector that, while originally reported in 2014, continue to this day. Based on the network elements compromised, the attackers are interested in gaining access to IT as well as OT systems. These objectives often indicate that the attacks remain at exploratory and reconnaissance phases, with the goal of informing plans and models of attack to be used at a later date.

"The Dragonfly group appears to be interested in both learning how energy facilities operate and also gaining access to operational systems themselves, to the extent that the group now potentially has the ability to sabotage or gain control of these systems should it decide to do so," Symantec wrote, noting that the hackers had taken screen shots of control panels. Security experts will debate whether having access to systems equals a capability to manipulate them, however, there is precedent in the remote cyber intrusions which caused power outages in Ukraine in 2015 and 2016.

ENERGY-SPECIFIC CHALLENGES

The energy industry faces multiple sector-specific challenges. Operational constraints limit the type and scope of security controls that can be put in place without affecting real time operations, while at the same time, the threat landscape is vastly more motivated and capable.

The overlap of professionals who specialize in security, risk management, and operational engineering is exceptionally small. As a result, professionals who can balance the real-time operational needs with risk-determined security controls are in great demand. In fact, the Department of Homeland Security's ICS Red Team exercise at Idaho National Labs is an attempt to start bridging that divide, by teaching each group (security/risk/operations) about the essential aspects of the others.

While government bodies and the public are rightly focused on transmission, the distribution units Secure Halo has assessed are at a much more "basic" level of maturity. The combination of smart grid technologies and other IoT interfaces is creating increasing complexity. Many of the groups we've spoken to do not meet even the CIP Low Impact requirements. As a result, those groups weren't operating under CIP requirements or the IT security protocols of their organization's corporate environment. In essence, they were flying solo.

The level of risk to Regional Transmission Organizations (RTO) and Independent System Operators (ISO) may also be overlooked. Secure Halo has found that, while the potential impact to the grid was quite high, the level of security controls and security capabilities among some ISOs we have assessed were quite low. Given their less mature cybersecurity posture, ISOs could be a target for state-sponsored actors, as disabling or impacting one of them could create a large interruption of service.

RECOMMENDED BEST PRACTICES

- **Basic cyber hygiene remains important**. The methods employed by Dragonfly include run-of-the-mill techniques such as spear-phishing emails that trick a recipient into opening them, and water hole attacks that reach victims by compromising a website they're likely to visit. The attackers then harvest user credentials and gain remote access to their machines. Basic cyber hygiene continues to be your best form of defense, with added attention applied to remote access, credential compromise, and trojans masquerading as software updates. If your organization possesses the resources, setting up honeypots to observe the targeted elements as well as the attackers' means and methods outside of operational systems could prove useful in maturing defensive techniques.

- **Connections into and out of networks must be very tightly controlled**. One-way diodes are often used to allow information to flow to the corporate side of the network while preventing any traffic from flowing back in. Where possible, there should be NO remote access or open ingress points to the electronic security perimeter (ESP). Needed remote access should be through monitored sessions. For example, many providers allow vendor maintenance to work through monitored web-sharing services.

- **No connections to public networks should be permitted in the ESP**. All patches or other 'research' should be conducted from other networks outside of the ESP. Once vetted and verified, patches can be brought in through scanned removable media, or internal file transfer. This won't necessarily protect against malware (the nuclear industry has detected malware in air-gapped systems), but it makes the attacker's job all the more difficult.

In the same vein that criminals attack payment systems because that is where the money is, nation-states incorporate attacks on critical infrastructure as part of a broader military strategy such as denying an adversary access to systems critical to its defense. In peacetime, the U. S. energy sector will therefore remain in the cross hairs of those seeking to disrupt, deny or damage instruments of US power, from our economy to our national security.

To discuss insurance coverage issues/implications, please contact a member of your account service team. Please contact Secure Halo for more information about our cyber assessment support to U.S. critical infrastructure.

McGRIFF, SEIBELS & WILLIAMS, INC.

Suzanne Gladle, Director, Cyber Program Operations | sgladle@mcgriff.com
(302) 239-2046 | www.mcgriff.com

SECURE HALO
SECURING THE ENTERPRISE

(202) 629-1960 | www.securehalo.com