Comments from Waterfall Security Solutions on the US Department of Energy Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure

By Andrew Ginter, VP Industrial Security
Waterfall Security Solutions

Delivered via Email to ElectricSystemEO@hq.doe.gov

Thank you for the opportunity to provide comments regarding the security of the US electric grid. Waterfall Security Solutions is the world's leading provider of Unidirectional Security Gateways. We work with many of the world's most secure industrial sites and critical infrastructure sites.

Waterfall would like to provide input regarding RFI question #3:

3. What actions can the Department take to facilitate responsible and effective procurement practices by the private sector? What are the potential costs and benefits of those actions?

A very important action the department can take is to provide clear information and guidance regarding software supply chain and Internet-based services supply chain risks and effective remediations.

Software Supply Chain Risks

While many commentators focus on hardware and software suppliers that are subject to undue influence by foreign governments, a neglected but very important risk is that of a sophisticated actor compromising civilian software suppliers. The recent SolarWinds breach is a classic example - a sophisticated threat actor inserted remote-control malware into the build process of the SolarWinds Orion product, thus embedding the malware in digitally signed and apparently authentic security updates. The malware was subsequently downloaded by between 17,000 and 18,000 victims, and presumably installed by a large fraction of these victims.

The malware was not discovered until six months after it was introduced into the security update. The malware connected to an Internet-based command and control center and thus provided the threat actor with remote control of the attack code in the victims' networks. At least two hundred government and other sites were reported to have been actively exploited by remote control in this way.

This outcome was not a result of a foreign government putting undue pressure on a software technology provider. This is the result of a nation-state-grade cyber breach of a legitimate, friendly software provider. The breach itself represents a major investment in technology and tactics by the threat actor. The return on that investment was access to thousands of potential victims, access that was exploited over two hundred times.

This kind of breach is not unique to nation-state actors. Any threat actor with enough time, talent, and money could have accomplished this end. In the future, any such actor with a strong expectation of a return on such an investment should be expected to carry out attacks of similar sophistication.

For example, targeted ransomware groups have seen steadily increasing success in targeting businesses, governments, and critical infrastructures. Such groups are rapidly adopting the types of tools and attack techniques that were pioneered only a few years ago by nation-state adversaries. It is only a matter of time before breaches as sophisticated as the SolarWinds attack are carried out by ransomware criminal groups to plant their own malware.

In short, the SolarWinds breach shows us that legitimate, friendly software providers have become strategic targets of nation-state actors. It is not reasonable to expect that all of the world's friendly suppliers will be able to deploy cybersecurity programs powerful enough to defeat such malware-insertion attacks reliably. Today’s pervasive cyber threat environment is such that every signed, authenticated software and security update, from every legitimate supplier, must now be suspect.

This new kind of risk needs to be communicated to electrical critical infrastructure providers. The US DOE has the knowledge, expertise and reputation to be able to communicate this risk convincingly.

Internet Services Supply Chain Risks

Internet-based cloud and vendor systems are now providing important services to industrial control systems in electrical critical infrastructure sites. The most common services include predictive maintenance, continuous remote support, and optimization services. Turbine vendors for example maintain thousands of VPN connections into steam and gas turbines all over the continent. These VPN connections gather data from the turbines and provide occasional remote control when detailed investigations are needed, or when the turbines need adjustment. Many historian vendors and other control system vendors also maintain up to thousands of VPN connections into critical infrastructure and other control systems to support remote monitoring, optimization, and repair services.

The value proposition for these vendors is powerful: “Send us your data and we will use it to make you more efficient / productive / reliable / etc.. We built these products after all, and so we are the experts on them.” This value is why so many electrical and other critical infrastructure providers use these Internet-based and cloud-based services.

This is a “remote services” supply chain. The risk here is that a threat actor will compromise one of these cloud/vendor providers and use the clients’ own VPN connections to reach back into critical infrastructure control systems and sabotage those systems. It is unlikely that the cost of such a breach is beyond the reach of a nation-state actor, and it may well be within the reach of today's ransomware groups.

Like the software supply chain breach, it seems unreasonable to require all of the world's cloud-based providers to deploy security capable of defeating a military-grade cyber assault. And even if such a thing were required of all these providers, it seems unlikely that all providers, large and small, would succeed in defeating such assaults.

This new kind of risk also needs to be communicated to electrical critical infrastructure providers. The US DOE has the knowledge, expertise and reputation to be able to communicate this risk convincingly.

Protecting Critical Sites

The world's most secure sites uniformly use unidirectional gateway technology to protect themselves from these software and services supply chain risks, as well as from many other risks. The US NIST Special Publication 800-82 Revision 2 Guide to Industrial Control System (ICS) Security defines a unidirectional gateway as:

Unidirectional gateways are a combination of hardware and software. The hardware permits data to flow from one network to another, but is physically unable to send any information at all back into the source network. The software replicates databases and emulates protocol servers and devices.

The technology is used routinely in many industries, with conventional power generation and petrochemical pipelines being most relevant to this RFI.

Unidirectional gateway technology defeats the remote-control malware, such as the malware embedded in the SolarWinds Orion software supply chain, by preventing any communication into the malware from Internet-based command and control centers. When the only connection between OT networks and external networks is unidirectional, and when that connection is oriented to send OT data out to IT destinations or the Internet, no remote-control command can pass back into the protected OT network. Unidirectional gateway hardware is by definition unable to send any such malicious commands back into protected networks.

Unidirectional gateway technology defeats compromised cloud or Internet service providers when the gateways are inserted into the communications path between industrial networks and the Internet. Unidirectional gateways are able to send industrial information into the Internet-based service providers, but no malicious command can pass back through the gateway hardware into the unidirectionally-protected control systems.

When service providers need to provide their expertise in the course of correcting a problem that cloud-based systems have discovered, the most common mechanism for such corrections is unidirectional remote screen view, coupled with a telephone call to the service provider.

Conclusion

In short, the pervasive cyber threat environment has evolved to the point where remote-control malware has been embedded in otherwise trusted software suppliers' security updates. In addition, the pervasive use of very popular Internet-based diagnostic and management systems has created an opportunity for threat actors to distribute remote-control malware or carry out other attacks via encrypted connections from control systems into cloud systems. While these types of attacks currently represent a significant investment from threat actors, the return is enormous: access to up to thousands of critical infrastructure and other industrial victims simultaneously. Furthermore, the cost of such attacks is likely to diminish as the threat actors build up new tools and automation to assist them in their attacks.

Unidirectional gateways deployed at critical industrial infrastructures make industrial data available to IT-based and cloud-based consumers for management, diagnostic and optimization applications to increase efficiency and reliability. The gateways do this while physically preventing any attack information from flowing from compromised clouds or Internet-based command-and-control centers back into industrial operations.

The protections that unidirectional gateways provide cannot be changed by a remote cyber assault, no matter how sophisticated the attack. Unidirectional gateway hardware is physically able to send information in only one direction – no kind of cyber assault can change that. While classic, software-based protections do have a role in unidirectionally-protected networks, unidirectionally protected sites generally view their unidirectional gateways as the foundation of their cybersecurity programs.

Again, Waterfall Security Solutions recommends that the US Department of Energy will provide clear information to critical infrastructure providers as to the software and

services supply chain risks those providers now face and will provide clear advice as to the value of unidirectional protections in critical infrastructure cybersecurity designs.

Note:

To anyone not familiar with unidirectional technologies, the concept can seem confusing. Please rest assured that the use of unidirectional gateways does not place undue burdens on the businesses using the technology. Many power plants and pipeline operators already use the technology completely voluntarily, with great success. The unidirectional approach clearly works. For practitioners not yet familiar with the technology, I recommend my 2019 book Secure Operations Technology – a text that Waterfall Security Solutions continues to provide at no cost, as a public service to OT security practitioners and stakeholders. Please see https://waterfall-security.com/sec-ot to request your copy.

Thank you for the opportunity to provide information and recommendations into this process. Please feel free to reach out to me or to Waterfall if there are other ways we can be of service.

Respectfully submitted,

Andrew Ginter
VP Industrial Security
Waterfall Security Solutions