Geometric illustration of oil and gas pipeline. Royalty-free stock vector ID: 1606949662.

Jul 28, 2021 12:08 BST

News spotlight: Oil and gas pipelines a target for hackers – part one

Last week saw substantial cyber security developments for the oil and gas industries in the US, including an advisory issued by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) on a spear phishing and intrusion campaign carried out on 23 US oil and natural gas pipeline operators between 2011 to 2013 by Chinese state-sponsored hackers.

Here, Damon Small, technical director at NCC Group reacts to this news and delves into the hackers' tactics, techniques, and procedures (TTPs).

According to the advisory, hackers had a specific goal of 'holding US pipeline infrastructure at risk', gaining the ability to physically damage or disrupt compromised pipelines. Of the 23 known targets, 13 were confirmed compromises, three were near misses, and eight had an unknown depth of intrusion.

How big of a threat is spear phishing and social engineering attacks to the oil and gas industry?
“It’s not only oil and gas. Spear phishing and social engineering remain successful techniques across all industries because they prey on the most vulnerable part of the technology stack – we humans that use that technology – or the 'chair-keyboard interface', as I like to call it.

“Our adversary in these cases are criminals, but unfortunately, they are also very clever. The best way to defeat a technical control is to trick the user to doing something unwise such as entering their username and password into a malicious website or to run malicious software.The best firewalls, anti-virus, patch management, and vulnerability assessment programs in the world won’t stop a miscreant if you invite them in.”

Are the TTPs used in these attacks sophisticated?
“The TTPs were sophisticated in the sense that some of them involved malicious software that would have been advanced at the time, and also infrastructures to support the phishing campaigns and command and control (C2) systems that allowed for unauthorised access once the victim had been compromised.The technology supporting the attacks was sophisticated, but at the end of the day, what allowed these attacks to happen was coercing a person to click a URL, file, or to verbally give away sensitive information over the phone.

“If anything is noteworthy it is that, even back then, technical controls to prevent phishing emails from having been received and to have prevented malicious software from executing properly already existed. The fact that the attacks were so widely successful suggests that those controls were not implemented at all, not implemented properly, or were defeated by the criminals. If the latter, then this further supports the notion of 'defense-in-depth'.

“That is to say, we cannot depend on any single defensive mechanism and all organizations should implement many layers to protect sensitive information

assets in the event that one layer is circumvented."

Do you agree or disagree with the mitigations proposed in the advisory?
"The mitigations suggested cover the necessary ground and are what I would recommend to a client. This includes replacing end-of-life software and hardware, restricting and managing remote access software, implementing and ensuring robust network segmentation between IT and ICS networks. What is missing, but likely out-of-scope for such a publication, is how companies should implement them.

"The specifics around how to do all of these important things will vary from business to business. After all, if this was easy, we'd all be doing it already. Beyond reading the advisory, critical infrastructure operators need to work with internal subject matter experts and trusted third parties to plan on how to implement it."

Is there anything that these recommendations miss out that oil and gas companies need to be doing now?
"Asset management. Asset inventory is mentioned several times in the mitigations section of the advisory but it is a bit buried in that lengthy section of the document.Before an organisation does anything though, they should take on asset management and inventory first. You cannot protect what you cannot see, and none of the recommendations will begin to approach 100% efficacy if there are blind spots within the network.

"As the saying goes, 'you cannot manage what you cannot measure,' and having an up-to-date and accurate inventory is the only way to begin to measure a threat landscape."

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and

manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750