BLUF

The cyber-threat actor known as The Ringleaders, locked Worldwide Industrial Management's (WIM) pipeline industrial control systems (ICS) under a $250 million dollar ransomware attack 12 hours ago. WIM operates in the US, Canada, and Europe with its Keystone Oil, Rockies Express Gas, and Druzhba Oil pipelines. WIM merged with Nordsk Pipelines 3 months ago during which a Log4Shell attack on Nordsk's Supervisory Control and Data Acquisition (SCADA) servers likely left a command and control backdoor. The attackers are motivated by financial gains using environmental leverage against WIM Global Enterprises and the affected governments. The Ringleaders threaten to pressurize the pipelines if their demands are not met within the next 12 hours. In accordance with the DHS NCIRP Annex B, this is a Level 5 Emergency and poses an imminent threat to critical infrastructure and U.S. citizens. We advise action to identify, contain, and restore infected systems by coordinating with federal agencies, state, local and foreign governments.

TASKS AND PRIORITIES FOR KEY FEDERAL AGENCIES

The primary COA employs the FBI, NSA, CISA, DoD into a task force in partnership with private contractors and EC3.

The FBI will identify compromised systems, files and track the intruding source.

The NSA will conduct counter-cyber exercises alongside the FBI's investigation to locate and disable The Ringleader's systems. Collaboration with EC3 will be key to the capture and neutralization of the adversary and its infrastructure at a global level. The NSA will also seek to employ its vast cryptological and reverse-engineering capabilities to identify a method to disable the ransomware.

On another hand, we delegate CISA the responsibility of protecting WIM systems from additional compromise, which will culminate defense standards to the threat landscape. In accordance with Operational Directive 22-01, CISA is tasked with reducing the significant risk of known exploited vulnerabilities. We advise the CISA to track and decrypt the malware actively controlling the ICS. They will engage with state and local governments to provide expertise and maintain information flow to continue threat mitigation. CISA will also immediately engage key private industrial contractors and stakeholders to enhance our national response.

The DoD will establish network segmentation to mitigate malware proliferation towards unaffected critical infrastructure systems. Malicious websites and servers acting as a vector for infection will be logged and provided to ISPs and operators of internet infrastructure to blacklist intruders and prevent further network disruption.

Key contractors such as Mandiant and Cynet will sweep SCADA and ICS to understand how far hackers probed WIM networks and secure system controls. Identifying the attack vector is integral to determining a solution to further isolate the current and future attacks. A post-mortem of the

prior-SCADA infection may provide forensic teams clues about the adversary's infrastructure and used to our advantage.

The FBI must prioritize working with EC3 to analyze associated systems for WIM's recently purchased Druzhba Oil Pipeline crossing through Poland, Hungary, Slovakia, the Czech Republic, Austria and Germany. All information we ascertain about mitigating the hack will be provided to EC3 as we expect EC3 will offer a different perspective. We also should provide our expertise with non-EU entities such as the governments of Ukraine, Russia, and Belarus. Even amidst the current Russo-Ukrainian crisis, we must secure critical global infrastructure and establish a coalition to prevent future implications, particularly the cascading effects to the global oil supply chain. .

RELIEF

We advise the President to authorize the Governors of Colorado, Illinois, Indiana, Kansas, Missouri, Montana, Nebraska, Ohio, Oklahoma, Texas, Wyoming, North Dakota, and South Dakota to mobilize the Army National Guard under U.S.C. Title 32. The DOT and DOE should coordinate with NorthCOM to manage civil support objectives in the event of catastrophic environmental damage. We request state and local governments provide emergency personnel assistance to evacuation zones. Pending the security and containment of the Keystone Oil and Rockies Express Gas pipelines, the United States will consider sending foreign aid, upon their request, through title 10 authorities if EC3 is unable to contain the Druzhba Oil Pipeline's breach and subsequent exploitation.

ALTERNATIVE COA

If all resources are exhausted and our 12 hour window is closing, we advise authorization of the $250 million dollar Bitcoin payment. The relief plan from the primary COA is also in effect here, and we expect evacuations to be carried out accordingly. We recognize our primary goal of ensuring the safety and security of the nation by conducting this payment. We cannot allow our critical infrastructure to be destroyed.The payment will be conducted with the following stringent guidelines. Any money or assets sent to The Ringleaders must be traced by the FBI. Cryptocurrency exchanges will be updated with a blacklist of addresses, coins, etc…, to prevent the offramping of the cryptocurrency to fiat. In the event the adversaries try to launder the money through Monero, CipherTrace claims to have the ability to track Monero, and we will employ their services. A successful trace will allow us to locate the threat actor and recover the ransomed money. Meanwhile, CISA will oversee the decryption process, and engage in enhanced infrastructure surveillance for any sign of persistent threat. They will conduct software vulnerability remediation and hardening upon successful decryption of WIM ICS.

We advise to mobilize as many available national assets to image, restore, and replace critical infrastructure as a precautionary measure if the encryption key is not released after the ransom is paid, or the key initializes another malicious event such as a disk wipe. Pipeline operators and managers must be on site to provide immediate technical expertise in such an effort. The DOT will distribute temporary waivers to expand the ability of railway and motorway operators to

move gas in a safe capacity. Critical civil and defense infrastructure will be prioritized, and gas rationing will be implemented by state and local governments as determined by their ability to get gas. We request unaffected states to distribute their fuel to the states under a declaration of emergency in conjunction with the DOT's guidance.

Internal and External Messaging:

The outlined COA requires active deliberation, briefing, and professionalism as operating time narrows. We recommend the FBI lead internal discussions between directors of associated entities by disseminating information and transitioning between COA stages with ease.

We also recommend the DOE to conduct a transparent press conference because U.S. persons across several states are at serious environmental risk. The DOE must stress the importance of remaining calm to the people as at this point, relief forces are deployed to aid affected communities.

Options to Respond against the threat actors and to prevent future incidents:

Options to prevent future incidents are limited as The Ringleaders exploited a zero-day vulnerability. As markets blend together in the cyber-world, a fortified national security requires swift collaboration with the private sector to protect network integrity. We propose drafting a Business Continuity and Disaster Recovery (BCDR) joint manual to safeguard our nation's enterprises from future cyber attacks. An inter-agency manual will further guide training exercises as ICS and SCADA continue to highlight major weaknesses in American cyber-defense.

Conclusion

The JCTF recommends a course of action to identify, contain, and restore infected WIM Global Enterprise systems by coordinating with the FBI, NSA, CISA, DoD, EC3, foreign governments and private cyber-security companies. We propose a relief exercise by activating the ANG in several states under the U.S.C. Title 32 in partnership with the DOE, DOT, and NorthCOM. The alternative Course Of Action outlines options after the 12 hour window closes and ransom payment has been distributed. Our top priority is to protect and serve the American people by securing our nation's critical infrastructure systems. Thank you.