PNDC
UNIVERSITY of STRATHCLYDE

PNDC

Case Study – Evaluation of Lupovis Cyber Security Deception Solution in Power Networks

Exploring Cyber Deception Solutions in Utility Networks to Mitigate Rising Threats Due to Digital Transformation for Net Zero Attainment.

Delivered in Collaboration with:

Project Overview

The project, funded through the core research fund, comprises a partnership between PNDC, Lupovis Ltd and the PNDC's key DNO members UKPN, SPEN and SSEN and is delivered in collaboration with UK Power Networks and Lupovis.

Background

According to the Ponemon Institute, 90% of Critical Infrastructures (CIs) have experienced successful cyber-attacks ranging from ransomware to persistent threats affecting operational processes. Over the recent past, hackers have become more advanced in techniques and strategies increasing the probability of a successful breach and resulting in systematic and persistent disruption. Each year, the consequences of breaches are becoming more damaging and in 2021, the costs owing to global cybercrime exceeded $6Trillion.

Current cyber-security protection systems still do not prevent successful and undetected attacks. The average time to identify and contain a cyber-breach is >300 days, a significant exposure demanding the detection and mitigation of successful attacks as early as possible. Early detection is challenging as attackers constantly adapt techniques to evade embedded protection measures. Furthermore, a 15.1% increase in successful cyber-attacks has occurred over the last year despite the plethora of solutions and tools on offer. Security Operation Centres (SOCs) report that current solutions generate between 72% and 80% False Positive (FP) alerts, resulting in increasing pressures on the Security Operations Centre personnel.

In relation to the energy sector, the potential damage and associated costs of a successful cyber-attack is exemplified by the attack on the Ukrainian Power System in 2015. The breach took the attackers 10 months from reconnaissance to execution, the goal of the attack was to cause physical damage to a transmission station. The associated costs can be segmented as 'consequential' and 'reputational':

- the breach resulted in 225k customers without access to power and an estimated £27m revenue loss; the average network downtime costs were £240k per hour
- the estimated reputational damage cost was £1.2m and the investigation lasted for four years

A recent report states that the potential GDP losses for the UK from a similar-sized attack may range from ~£21m for a four-substation electricity event to ~£111m for a 14-substation incident.

Thus, the project is motivated by the PNDC's Distribution Network Operators (DNOs) members need to improve current defences to prevent the continually growing cyber security threats against critical national infrastructure like the energy sector. Furthermore, given the critical service providers compliance order in the updated UK's Network and Information System (NIS) regulations mandating utilities to implement adequate threat detection and reporting of attack incidents to the UK regulators such as the Office of Communications (Ofcom), Office of Gas and Electricity Market (Ofgem) and the Information Commissioner's Office (ICO), the energy sector needs innovative tools for active vulnerability identification and reporting of high-risk incidents to demonstrate robust cyber security resilience and obviate potential fines of up to £17 million for non-compliance.

Over the recent past, there has been a re-emergence of honeypot technologies which have been used to trap malicious users in order to identify early signs of attacks. While effective in luring inexperienced attackers, current solutions are ineffective against more sophisticated intruders given that their (static) non-dynamic nature permits easy identification. Lupovis has re-purposed the utility of honeypots to provision dynamic deception environments that establish a pro-active and offence-centric deception strategy adapted to each adversary regardless of skill level. The solution provides contextual threat intelligence when deployed outside of networks and manages attackers that have penetrated the network through a rich engagement environment, guiding their evolution paths through the decoy infrastructure using adaptive manipulation techniques. The solution deployed inside of the network extends the time window for Security Operation Centre (SOC) operators to respond with the most effective countermeasures to arrest the breach whilst maintaining operational integrity and business continuity. Furthermore, each interaction is recorded and stored providing the environment for the Lupovis cloud analytics engine to mine actionable information, matched against all other interactions captured within the Lupovis data lake, allowing; identify and classify attacker tactics, techniques and procedures and lead them away from critical network resources; autonomously improve deception assets and narratives over time; identify unknown adversary attack patterns using big data and AI; identify adversaries present in single sector e.g., Finance or Country e.g., Belgium, Region e.g., Baltics or attackers that focus on specific cloud providers e.g., AWS. The decoy-to-cloud telemetry implemented by Lupovis is unique.

Objectives

The project centres on the definition, prototyping and demonstration of a Lupovis cloud-based deception implementation that enhances the cyber security resilience of energy infrastructures. The solution can be deployed into any segment/zone of the overall infrastructure, immediately enticing adversaries into deception narratives, gathering contextual threat intelligence through mis-leading the breach away from operational systems, classifying the type of threat and skill of the attacker, maintaining the trustworthiness and operational continuity of energy services. The proposed development plan assumes a close partnership with the appropriate technical assets and evaluation environments within UKPN/PNDC, principally for the capture of product requirements and agreement on the most compelling validation methodology of the features of the deception functionality. Given the stage of engagement and the objectives of the project, largely centred on the definition and validation of the solution in the selected OT environment, access to a representative non-operational infrastructure will be selected through the collaboration.

The objectives are;

- the co-development of a deception-enabled cyber security solution that enhances the protection of critical infrastructures for the power network, but also applicable to other utilities
- showcase the benefits of cyber security deception, informing cyber security operators tasked with the protection of both the corporate (IT) and OT networks
- provide evidence on the benefits of cyber security deception for the sector
- the insights arising out of the project results will be disseminated to all DNOs and other utility infrastructures

Methodology

The development will create an energy-specific cluster of collaborating decoys that will implement a narrative that entices and locks an attacker on a path away from critical operational assets. The decoy cluster will co-operate to demonstrate the ability of deception-based cyber security to identify evolving threats placed into a global context, initially outside IT utility networks, enhancing the cyber security resilience on the backdrop of ever-increasing levels of sophisticated campaigns of attacks. Lupovis's deception will generate Technique, Tactics, and Procedure (TTP) from the data acquired, real-time from a cluster of decoys deployed within a representative DNO environment (Figure 1). The characterisation of the showcase deployment will ascertain the additional benefits of deception to enhance current cyber security practices in operational technology networks. The recommendations on the most appropriate deception solution and the route to deployment within utility infrastructures are insights that inform decisions on the value of deception for the sector.

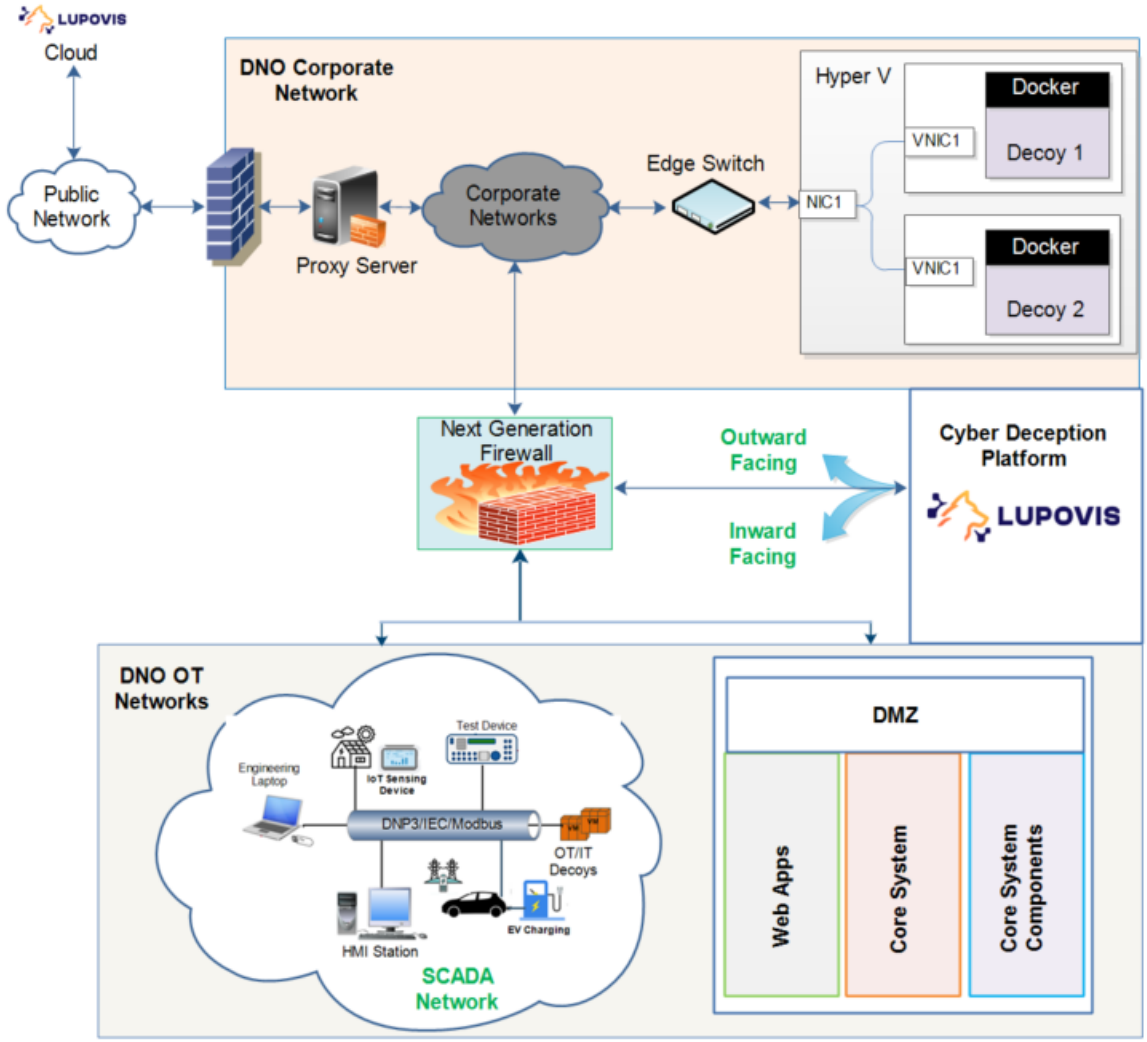


Figure 1: Lupovis deception deployment in a representative segment of an utility infrastructure.

The stages of the development are as follows;

- narratives representative of attack paths in utility infrastructure will be created in consultation with DNOs
- energy-specific decoys will be created, and evaluation metrics for cyber deception agreed in consultation with DNOs
    - breadcrumbs will be utilised to maintain a strong engagement with the attacker
- the Lupovis Deception-as-a-Service platform (SNARE) will serve the energy-specific decoys within a representative network
- the Lupovis contextual threat intelligence platform (PROWL) will be employed to generate Internet-based attacks
- performance will be referenced through simulated attacks against Apache Server, SSH Server, SMB, and Postgres DB and validated with indicators of intelligence (attack detection and alert) via the Lupovis platform

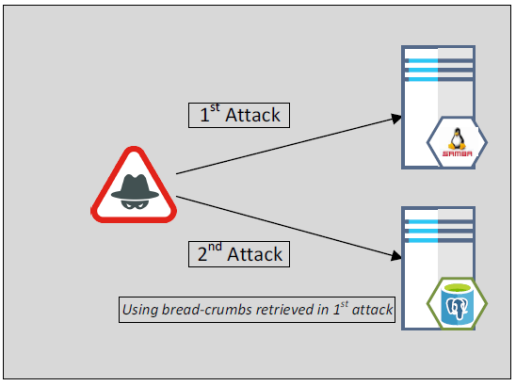
Delivery and Outcomes

The output of the project will inform power utilities and other critical infrastructure organisations on the benefits of decoy-enabled deception as an enhancement to current cyber security provisions. The goals are:

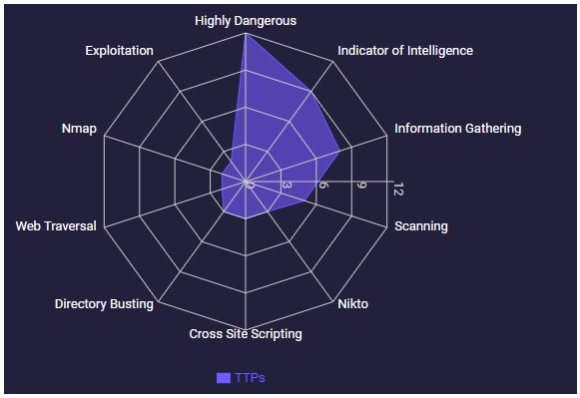
- to identify potential access nodes in utility networks for cyber-attacks informing on the optimum placement of decoy types (services, files, objects) across the network infrastructure to achieve acceptable protection coverage.
- determine the types and the percentage of decoys required to protect a representative utility infrastructure i.e., the ratio of real and deceptive assets in the network without significant additional resources, operational challenges and system infidelity. Ideally, cyber deception coverage within a critical infrastructure like utilities is expected to cover 20% to 100% of the real network assets for increased deception performance, often dependent on the network architecture, existing security solutions and policies of the utilities.
- minimise false positives from decoys configured within a DNO's narrative as data from every interaction data from the deceptive decoys enriches the context and accuracy of the threat intelligence of the attacker's activities and progression.

Lupovis Trial Summary

- Within the Snare platform, the interactions logs concerning the deployed decoys and attacking IP within the selected organisation can be refined to gain other information like attacking IP address and any intelligence within the attack. Each interaction with the decoy receives a severity rating, categorised as 'informational', 'warning', or 'critical', following an analysis of the interaction.
- Analytics are applied to assess the interactions between the attacker and decoy, determining whether the connection should be identified as an attack. Each attack is assigned a threat score on a scale of 0 to 100. Interactions originating from a private IP address default to a threat score of 50, as this implies that the attacker may be within the network. Threat scores are routinely reassessed as interactions evolve.



Attack Simulation Scenario: Attempts to attack the different decoy Narratives deployed in the network.



Attack Simulation TTPs Faced in a month

- To strategically aligns decoy placement with the goal of detecting and responding to potential threats across different segments of the DNO's environment, deception decoys can be placed at the Corporate Perimeter Network to monitor and detect external threats from the Internet, SCADA Perimeter Network to provides insight into threats targeting the OT environment, Proxy DMZ to detect network access and signalling scanning activities from potential threats at the substation network, and at the Corporate Internal Network to identify internal related threats

Quotes

from Lupovis.

Xavier Bellekens, co-founder and CEO of Lupovis "*observes that the Lupovis solution has already been demonstrated to deliver value to customers in the manufacturing, education and finance sectors, furnishing periodic reports to these industries encapsulating prominent Common Vulnerabilities and Exposures (CVEs) observed within a given sector and predominant Tactics, Techniques, and Procedures (TTPs) leveraged by adversaries, allowing end users to discern vulnerabilities, strategies countermeasures, and implement timely remediation. However, Xavier stresses that entry into new sectors/infrastructures necessitates an initial development phase, in particular a deeper understanding of the challenges and needs faced by a particular sector which then informs the creation of the range of decoys that are accurate representations of the infrastructure to be protected. Thus, the opportunity to co-create with DNOs in partnership with the PNDC lowers the barrier to developing products appropriate to utilities".*

Quotes

from UKPN.

Matthew Bates, OT Cyber Security Lead at UKPN *"Lupovis brings a new perspective to traditional honeypots, by providing a customised narrative that is unique to the environment, allowing a deployment of strategically placed decoys that provide breadcrumbs to entice and detect intelligent cyber-attack tactics. It's all about detecting intelligent movement, an early warning system, allowing for the defender to detect and remediate any weakness in its defences to any potential or further attempt at a cyber breach. A simple solution to deploy with full support from Lupovis, a valuable experience".*

Quotes

from PNDC.

Stephen Ugwuanyi, Research and Development Engineer at PNDC, "*As the Operational Technology (OT) domain is constantly evolving, innovative approaches are needed to enhance existing cybersecurity systems in Critical National Infrastructure (CNI). To better understand the routes to cyber deception deployment, network integration, performance, and its operational challenges and benefits in OT networks like Distribution Network Operator (DNO), Lupovis cyber deception solution through collaborating honeypots (decoys - 'Snare and Prowl') and Breadcrumbs proved to be an innovative approach to early detection of threats, the subsequent monitoring of its progression and attack characterisation". Other use case trials would potentially allow for the identification of more Common Vulnerabilities and Exposures (CVEs) specific to Distribution Network Operators (DNO), attack Techniques, Tactics, and Procedures (TTPs) leveraged by adversaries, and strategic locations within the DNO network for optimal deception deployment.*

Next Steps

The findings of the trial will inform UKPN and PNDC on cyber security practices that mitigate future risks from an evolving range of new cyber attacks. It will also help in assessing the strategic locations within DNOs environment that are most suitable for deploying cyber deception solution and the deployment requirements.

There is an open collaboration opportunity call to further demonstrate the technology with other organisations through specific use cases and scenarios that help to meet NIS regulations and directives from the National Cyber Security Centre (NCSC). Utilities will be integral to the selection of the suite of most appropriate decoys for the sector e.g., PLC, CCTV, HMI with custom configurations, decoy concealment, and to define optimum routes for the integration of the digital intelligence generated by deception within SIEM products and Supervisory Control and Data Acquisition (SCADA) systems.

Get in touch

PNDC Project Leads: Dr Stephen Ugwuanyi and Dr Kinan Ghanem