Radiflow Security Brief

# Insights into the Norsk Hydro Cyberattack: Using AD in IT/OT Networks

March 2019

radiflow
Secure Your Assets

## OVERVIEW

One of the world's biggest aluminum producers, multinational manufacturer Norsk Hydro, announced it had been hit by a ransomware attack of unknown origin, with hackers demanding a ransom.

The attack caused severe damage to the corporate network by disabling network communications on every computer, encrypting files and changing local user accounts to prevent recovery procedures.

Norsk Hydro's incident response team isolated part of the production facilities moved some plants to manual or semi-manual operations and brought external IT and cyber security experts in to assist in investigation and recovery operations.

The analysis of the malware pointed to a rare seen ransomware named LockerGoga which was previously reported as being used in attack on French global engineering and consulting firm Altran in February 2019.

Even though most of cyber security community agrees that the Norsk incident response process was conducted professionally, the attack definitely affected manufacturing activities and caused overall business interruption and operational loss that is yet to be determined.

As part of the incident response process Norsk informed Norway CERT which later mentioned that the attack on Hydro was combined with an attack against its Active Directory (AD).

Also, LockerGoga malware which is reported to infect the Norsk Hydro network does not have the capability to spread in an automatic way so we can only wonder if some network built-in mechanism was exploited by the attackers.

Although the exact incident details are still unclear, we will focus our analysis on this architectural issue.

## ACTIVE DIRECTORY – SECURITY CONSIDERATIONS

Using Active Directory (AD) to manage user credentials is one of the most well-known practices in corporate IT operations. All user credentials are maintained in a central secure location and all accesses to the network assets are authenticated and monitored.

However, we also witness numerous incidents in which threat actors leverage central user management and its built-in mechanisms for delivering malicious payloads, leaving backdoors for continuous access and more.

AD uses multiple ports to support both user and computer authentication- TCP/UDP 445 for SMB, 389 for LDAP communications and 88 for Kerberos protocol, for example. In Microsoft-based networks one should leave open NetBIOS ports (137-139) and Microsoft RPC port (135).

In networks with more than one Domain Controller (DC) (e.g. different geolocations) network administrators activate replication mechanisms between the DCs, which requires leaving these ports open in the cross-site firewall for this replication process.

There are additional security issues in Microsoft AD networks which need to be addressed by the cyber security personnel – usage of local workstation administrator account, management of multiple groups in AD with high privileges, storage of domain administrator account credentials, etc.

Such networks with AD implementation flaws and selective security monitoring is easily becoming the attractive and easy to exploit target for hackers. These hackers can apply multiple techniques to acquire privileged access or even Domain Admin credentials – performing "Pass-the-Hash" attacks, leveraging Mimikatz utility to extract passwords and authentication tokens from memory and more.

After acquiring these high-privilege credentials, hackers

can deploy various techniques to spread out malware in the network such as GPO mechanisms, scheduled tasks, etc.

Unfortunately, in industrial corporates with manufacturing networks the risk derived from using AD is even higher. Networks in this kind of enterprises are usually built from at least two segments – the corporate IT network and the production OT network.

Industry best practices suggest physical isolation or at least firewall-based segmentation between the IT and OT networks. Having said that the recent trends of digital transformation in the production floor undermine these boundaries, such as using Active Directory in the OT network.

From the usability point of view, the network administrator would like that all users have the same credentials, whether they are connecting to a PC in their office or to the HMI machine in the ICS network. However, from security point of view, it means that either:

a) Hosts in the ICS network will have access to the domain controller in the corporate network (with all ports open and all security implementation flaws that could take place in it); or,

b) Network admin will deploy a separate Active Directory server in the ICS network and will activate an automatic synchronization between the two Domain Controllers – the one in the industrial network and the one in the corporate network.

Both implementations will open the ICS network to external communication and allow additional attack vectors. Using the same user database for both networks means that the isolation between the industrial and the corporate network is breached and that the cyber threat to the production floor and business disruption will increase dramatically.

Furthermore, the computers in ICS networks usually use older versions of Windows which contain more vulnerabilities such as utilization of the unsecure NTLM-based authentication, instead of the more secure Kerberos protocol which result in very easy vulnerability exploitation and smooth lateral movement.

## CYBER RISK ASSESSMENT

From the partial information that it is available, it is clear that the network in Norsk Hydro may have had a 'wide attack surface'. Attack surface is the sum of the different network points in which an unauthorized user can try to exploit the network and to launch the malware or to exfiltrate sensitive information from an environment. Keeping the attack surface as minimal as possible is a basic security measure.

For example, in the Norsk Hydro network, an industrial network risk assessment methodology would have been able to identify the following cases related to the usage of Active Directory:

1. An Active Directory server which is located in a different network.
2. An Active Directory server which has some synchronization mechanism with a server outside of the industrial network.
3. Usage of less secure AD protocols (i.e. NTLM vs Kerberos).

Such a risk assessment methodology that relates to the business processes would have probably highlighted such high-risk attack vectors from the IT network to the critical ICS environment.

## RECOMMENDATIONS

Recommendations can be divided into two categories:

1. People and processes

a) The enterprise should develop cyber security awareness program and constantly train its employees to be aware of and recognize cyber threats.

For example, in majority of known cyber incidents in manufacturing industry the first foothold was established via a spear-phishing e-mail to employees that clicked on malicious links or opened a weaponized document.

b) Another recommendation should be in regard to planning and applying a business continuity program (BCP) in the case of a cyber incident.

In the Norsk Hydro case, one can see from the public announcements that the "good backup solutions and routines are in place" and "it is switching to manual operations where possible".

c) In order to be able to define cyber security policy and conduct proper cyber operations, the enterprise should be aware of its security posture preferably based on a professional risk assessment.

While this is a common practice in IT networks, in ICS networks it is still uncommon, mainly due to a lack of awareness but also due to the lack of tools which are optimized for such assessment of ICS networks.

2. Technological. To this category we can associate several recommendations. Among them:

a) Secure design of the network architecture of whole parts of the enterprise - both IT and OT. It includes proper network segmentation and segregation – first of all between the IT network and production floor, hardening the IT infrastructure, authentication and access control, establishment security patching policy and more.

In this article we stressed the importance of separate user management systems based on Active Directory implementations in IT corporate network and ICS production environment and hardening the network architecture.

b) ICS assets visibility and production network security monitoring. ICS cyber experts together with process owners should define the critical business processes and at which points the enterprise should control and monitor traffic.

Strict monitoring architecture with behavior anomaly detection of the production floor can minimize the time of breach discovery and allow fast incident esponse which will minimize the impact.

c) Use Automatic Industrial Risk Assessment and Analytics System – analyzing the risk and the attack surface in large networks is very complicated. Manual analysis is time consuming process and also prone to errors.

Automatic risk analytics systems with reference to the ICS business processes can prioritize your corrective measures.

All these can assist to reducing business loss and speed up recovery.

## ABOUT RADIFLOW

Radiflow is a leading provider of cyber security solutions for critical industrial automation (ICS/SCADA) networks, non-intrusive IDS (Intrusion Detection System) and in-line security gateways.

Founded in 2009, Radiflow's leadership team consists of renowned cybersecurity experts as well as industrial automation professionals from global automation vendors and operators. More at www.radiflow.com.

**US and Canada:**
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

**EMEA:**
Tel: +972 (77) 501-2702
sales@radiflow.com

**UK:**
Tel: +44 (0) 800 246-1963
sales_UK@radiflow.com

**France:**
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com