# Russian-made Remote Desktop Software Installed on Critical Infrastructure

**Industry:** State, Local Government & Education

## Attacker Objective

Attack and compromise of critical infrastructure

## Background

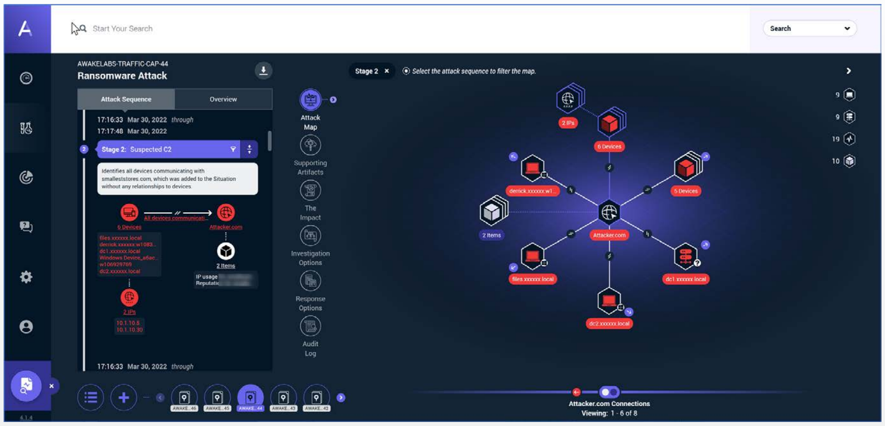
Arista NDR found Russian-made remote desktop protocol (RDP) software on the control server for a municipality's water treatment plant. The software was regularly communicating to its home base in Russia, enabling full outsider access to the chemical processes necessary to treat the water supply for a city of close to 100,000 people.  An outsider could thus easily act maliciously and sabotage the water supply.

## Arista NDR uncovered this threat by:

- Detecting unusual communications to and from an external foreign entity and a critical infrastructure system.
- Automatically identifying Russian-made software on the equipment.
- Identifying the outdated software on this system that prevented the security team from monitoring, patching, and managing it.

## Why Arista NDR?

**The FBI and Department of Homeland Security have issued multiple warnings about Russian actors targeting government entities and critical infrastructure sectors. Arista NDR alerted the city's security team to the presence of the software, which allowed them to remediate the situation rapidly.**



AWAKELABS-TRAFFIC-CAP-44
Ransomware Attack

17:16:33 Mar 30, 2022 *through*
17:17:48 Mar 30, 2022

Stage 2: Suspected C2

Identifies all devices communicating with smalleststores.com, which was added to the Situation without any relationships to devices

6 Devices: files.xxxxxx.local, derrick.xxxxxx.w1083..., dc1.xxxxxx.local, Windows Device_a6ac..., w106929769, dc2.xxxxxx.local

2 IPs: 10.1.10.5, 10.1.10.30

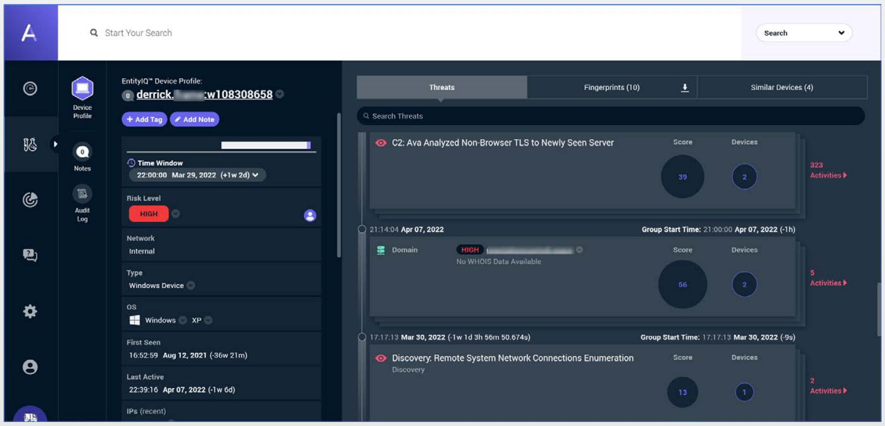
IP usage [redacted]
Reputati[redacted]

17:16:33 Mar 30, 2022 *through*

Stage 2 ×  Select the attack sequence to filter the map.

Attacker.com Connections
Viewing: 1 - 6 of 8

*Fig 1: Arista NDR identified an unpatched device used to control the water treatment plant with remote access from a foreign location.*



EntityIQ™ Device Profile:
derrick.[redacted]:w108308658

Time Window: 22:00:00 Mar 29, 2022 (+1w 2d)
Risk Level: HIGH
Network: Internal
Type: Windows Device
OS: Windows XP
First Seen: 16:52:59 Aug 12, 2021 (-36w 21m)
Last Active: 22:39:16 Apr 07, 2022 (-1w 6d)
IPs (recent)

C2: Ava Analyzed Non-Browser TLS to Newly Seen Server — Score 39, Devices 2, 323 Activities

21:14:04 Apr 07, 2022 — Group Start Time: 21:00:00 Apr 07, 2022 (-1h)

Domain HIGH [redacted] — No WHOIS Data Available — Score 56, Devices 2, 5 Activities

17:17:13 Mar 30, 2022 (-1w 1d 3h 56m 50.674s) — Group Start Time: 17:17:13 Mar 30, 2022 (-9s)

Discovery: Remote System Network Connections Enumeration — Discovery — Score 13, Devices 1, 2 Activities

*Fig 2: Arista NDR's EntityIQTM tracked down an unpatched device being used to control the water treatment plant*

Arista NDR automatically discovered the software since it triggered a couple of adversarial models, including one for data exfiltration and another for extended remote access. Using Arista's AVA AI capabilities, Arista NDR autonomously triaged anomalous behaviors of a critical server and isolated the system behaving erroneously, confirming remote access from a foreign location.

Arista NDR also identified that this system was running an unpatched and unsupported version of Microsoft Windows 2003.

May 31, 2022