Russian-made Remote Desktop Software Installed on Critical Infrastructure

Industry
State, Local Government & Education

Attacker Objective
Attack and compromise of critical infrastructure

Awake detected this threat by:

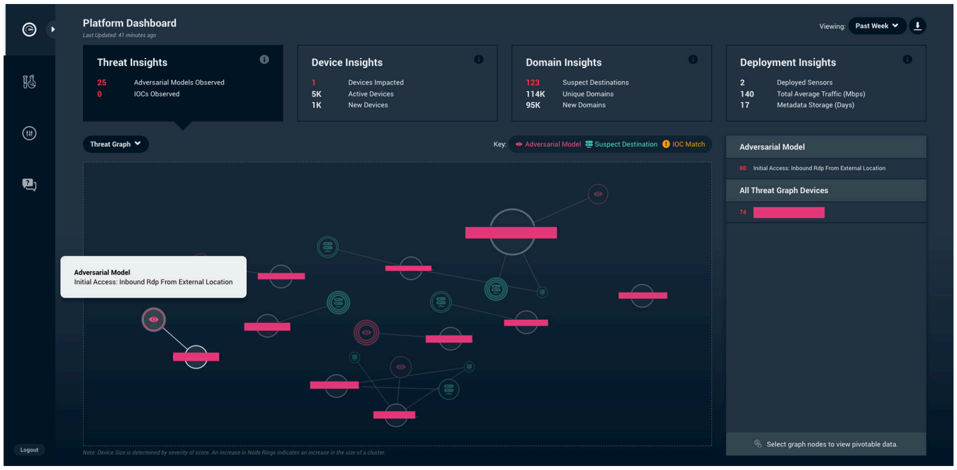
- ✓ Detecting unusual communications to and from an external foreign entity and a critical infrastructure system
- ✓ Automatically identifying Russian-made software on the equipment.
- ✓ Highlighting the outdated software on this system that prevented it from being monitored, patched and managed by the security team.

Awake Security found Russian-made remote desktop protocol (RDP) software on the control server for a municipality's water treatment plant. The software which was communicating to its home base in Russia on a regular basis, enabled full outsider access to the chemical processes necessary to treat the water supply for a city of close to 100,000 people. In effect, an outsider could act with malicious intent and sabotage the water supply.

Awake automatically discovered the software since it triggered a couple of adversarial models, including one for data exfiltration and another for extended remote access. Awake's security expert system, Ava, concluded through autonomous triage that the behaviors were not normal for a critical server.

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

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



Platform Dashboard

Last Updated: 41 minutes ago

Viewing: Past Week

Threat Insights		Device Insights		Domain Insights		Deployment Insights	
25	Adversarial Models Observed	1	Devices Impacted	123	Suspect Destinations	2	Deployed Sensors
0	IOCs Observed	5K	Active Devices	114K	Unique Domains	140	Total Average Traffic (Mbps)
		1K	New Devices	95K	New Domains	17	Metadata Storage (Days)

Threat Graph

Key: Adversarial Model · Suspect Destination · IOC Match

Note: Device Size is determined by severity of score. An increase in Node Rings indicates an increase in the size of a cluster.

Adversarial Model

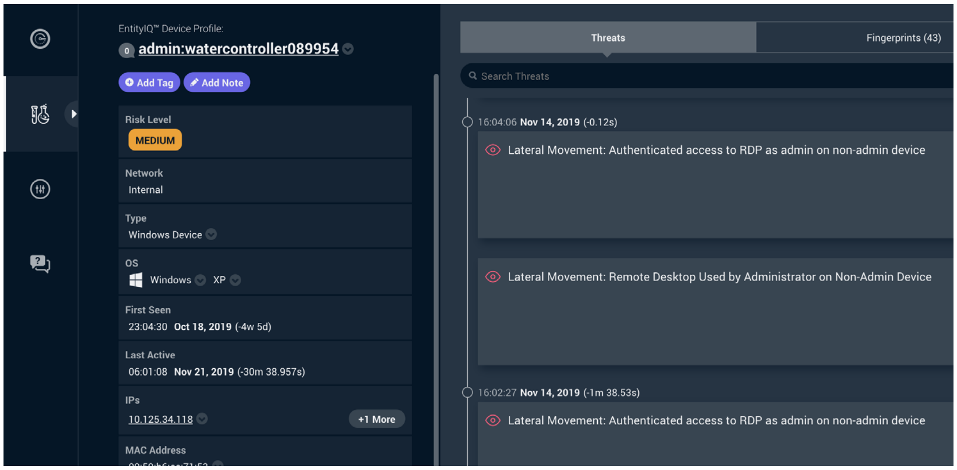
80 Initial Access: Inbound Rdp From External Location

All Threat Graph Devices

74 [redacted]

Select graph nodes to view pivotable data.

Awake identified an unpatched device being used to control the water treatment plant with remote access from a foreign location.



EntityIQ™ Device Profile:

0 admin:watercontroller089954

Risk Level: MEDIUM

Network: Internal

Type: Windows Device

OS: Windows XP

First Seen: 23:04:30 Oct 18, 2019 (-4w 5d)

Last Active: 06:01:08 Nov 21, 2019 (-30m 38.957s)

IPs: 10.125.34.118

MAC Address

16:04:06 Nov 14, 2019 (-0.12s)

Lateral Movement: Authenticated access to RDP as admin on non-admin device

Lateral Movement: Remote Desktop Used by Administrator on Non-Admin Device

16:02:27 Nov 14, 2019 (-1m 38.53s)

Lateral Movement: Authenticated access to RDP as admin on non-admin device

Awake's EntityIQ™ tracked down an unpatched device being used to control the water treatment plant, and an adversarial model in combination with Ava™ confirmed remote access from a foreign location.

For additional information about Awake please visit awakesecurity.com

AWAKE