Ransomware Attack Unfolds

Industry: Manufacturing

Attacker Objective

Profit from holding files for ransom

Background

Arista NDR was engaged in a Proof of Value trial with a manufacturing company at their Dallas, TX location.

While the customer was evaluating the Arista NDR platform, a company facility in Atlanta, GA, was hit by a ransomware attack. The Sodinokibi ransomware executed and encrypted more than 2,500 files, effectively shutting down four of the company's critical servers. Additionally, the attacker demanded a $750,000 ransom for the files.

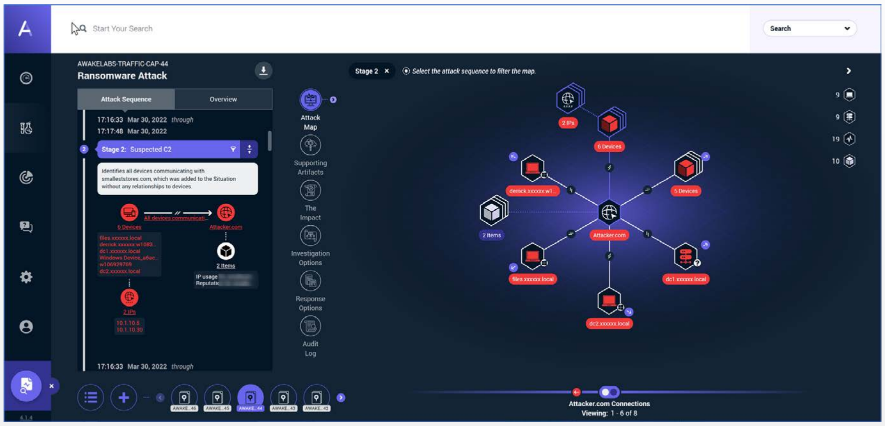
While this attack was unfolding in Atlanta, Arista NDR identified suspicious activity from a legitimate (but what appeared to be a compromised) device.

Arista NDR detected this threat by:

- Isolating early warning signs of ransomware like credential abuse, privilege escalation, and network discovery.
- Identifying security measures such as using non-browser encrypted communications.
- Uncovering the use of a malicious domain for ransomware download and distribution.

Why Arista NDR?

Arista NDR's identification of the tactics, techniques, and procedures (TTPs), such as encrypted attacks, privilege escalation, and lateral movement used by ransomware threat actors, prevented the attack from spreading to the Dallas location. The whole attack was thus stopped in its tracks, and the damage was minimized to just the unmonitored Atlanta location.



Start Your Search

AWAKELABS-TRAFFIC-CAP-44
Ransomware Attack

Attack Sequence | Overview

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

All devices communicati... → Attacker.com

2 Items

IP usage [redacted]
Reputatio [redacted]

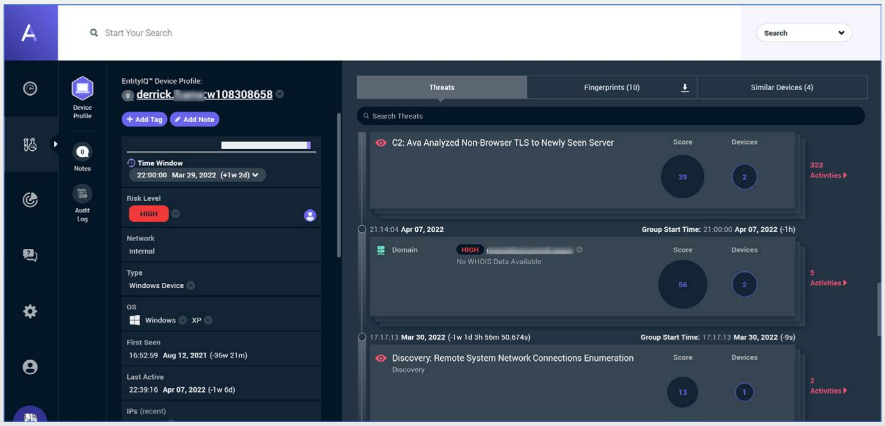
2 IPs: 10.1.10.5, 10.1.10.30

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's Situations dashboard highlights the attempts to spread the ransomware.



Start Your Search

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)

Threats | Fingerprints (10) | Similar Devices (4)

Search Threats

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 highlights the threat timeline as the ransomware attempted to spread to the environment in Dallas.

Purely through network traffic analysis, Arista NDR notified the security team that the attacker was using a non-browser based, encrypted channel for communication. The Arista NDR platform also identified devices connecting to a malicious web site which appeared to be an attempt to download the next stage of the ransomware. Finally, Arista NDR identified network discovery traffic attempts from the infected devices in Atlanta to the Dallas location being monitored by Arista NDR.

June 28, 2022