ARISTA

Case Study

Unauthorized VPN Used to Hide Data Exfiltration

Industry: High-Tech

Attacker Objective

Stealthily exfiltrate corporate data via a senior executive's device

Background

A senior company executive at a technology firm used a personal laptop computer to access the corporate network. Arista NDR identified the compromised laptop using "free" virtual private network (VPN) software. A VPN is typically used to create a secure, encrypted connection to a network. In this case, the free software set up a peer-to-peer network that multiple threat actors used as a vector for command and control, remote execution, and data exfiltration. As a result, the executive unwittingly turned their computer into an "exit node" that an attacker could access. What's more, this circumvented many of the company's security practices in the process.

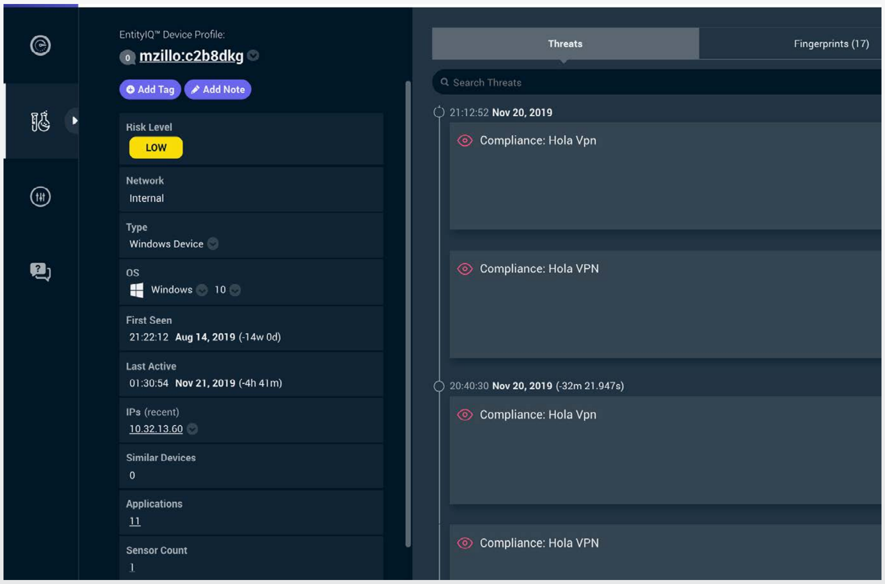
Arista NDR detected this threat as:

- Risky due to the VPN software's reputation for nefarious activities.
- Introducing unusual traffic from external sources.
- Unique to a particular device or person when compared to other similar devices or people, such as those in similar job functions.

Why Arista NDR?

Arista NDR discovered this situation through an adversarial model looking for VPNs and other remote access tools. The security team, once notified, was able to remove the software from the laptop.

Traditional security tools might have missed this software because it was on an unmanaged personal device. However, Arista NDR's network detection and response capabilities allowed this organization to identify the use of risky software because of the deep analysis of all traffic crossing the organization's network.



EntityIQ™ Device Profile:
mzillo:c2b8dkg

Risk Level
LOW

Network
Internal

Type
Windows Device

OS
Windows 10

First Seen
21:22:12 Aug 14, 2019 (-14w 0d)

Last Active
01:30:54 Nov 21, 2019 (-4h 41m)

IPs (recent)
10.32.13.60

Similar Devices
0

Applications
11

Sensor Count
1

21:12:52 Nov 20, 2019

Compliance: Hola Vpn

Compliance: Hola VPN

20:40:30 Nov 20, 2019 (-32m 21.947s)

Compliance: Hola Vpn

Compliance: Hola VPN

Figure 1: Arista NDR's EntityIQTM identifies the personal device and displays the timeline detailing the repeated use of the Hola VPN software.

Arista NDR highlighted that anyone else on the P2P network could use the processing power of this laptop, and any illicit activity would appear to have originated from the laptop owner and the company. This specific tool was used for nefarious purposes such as human trafficking and distribution of child pornography. If an investigation were to occur, such activities could be attributed back to the executive and the company as well.

Copyright © 2022 Arista Networks, Inc. All rights reserved. CloudVision, EOS and NetDL are registered trademarks and Arista Networks is a trademark of Arista Networks, Inc. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. June 23, 2022