Malicious Browser Extensions

Industry: Multiple

Attacker Objective

Intercept and manipulate browser-based traffic

Background

As people and businesses do more things online, browsers have become a critical means to access applications and data. Add-ons to Chrome, Edge,Firefox, and other browsers are primarily intended to be helpful extensions for activities such as converting documents to PDF or comparing prices on websites. Increasingly however, browser extensions are becoming a popular means for malicious actors to gain access to all of a user's online activities.

When a browser extension is installed, it has access to everything the browser and the user within the browser does: every search on Google, every transaction on a banking website, every customer record in Salesforce, every file in Dropbox, etc. Attackers see this as an easy vector to steal sensitive information, and browser extensions are becoming the new "rootkit," except with none of the complexity involved in developing and deploying traditional malware. In particular, Arista NDR has observed Russian, and other nation-state threat actors actively use this Man-in-the-Browser technique to intercept TLS-encrypted communications.

Why Arista NDR?

This threat vector will continue to grow due to the low barrier to entry. The only way to determine if a browser plug-in is malicious is to understand its actions and communications. Arista NDR analyzes these behaviors automatically to determine risk levels.

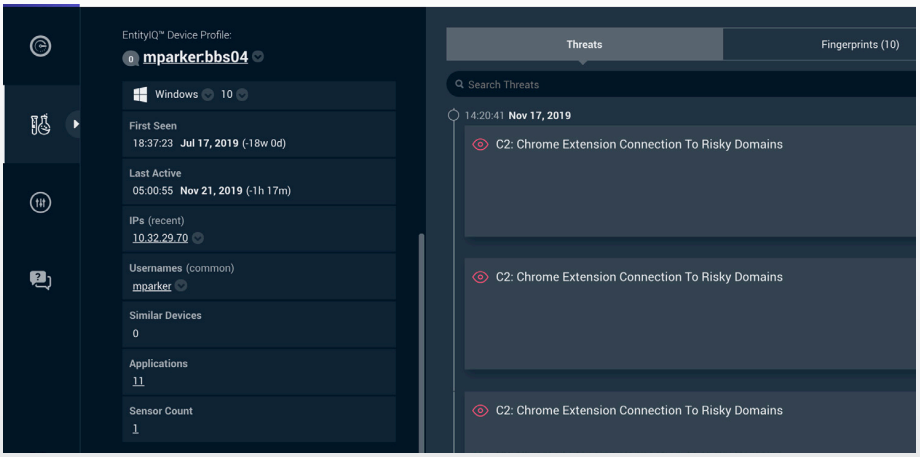

Fig 1: An adversarial model identified an unregistered Google Chrome extension used for command and control and data exfiltration.

Arista NDR detected this threat by:

- Detecting browser extensions with suspicious communication patterns.
- Identifying theft of browser-based credentials via a browser extension.
- Automatically determining if an add-on software is a legitimate part of the browser ecosystem.

Endpoint security solutions typically don't report browser add-ons as a threat because they aren't traditional malware. Arista NDR autonomously identifies risky browser plug-ins based on where they communicate and whether they are legitimate extensions. For instance, Arista NDR automatically detects extensions not registered in the Chrome Web Store. Arista NDR has also identified attempts to steal browser-based credentials for cloud services such as AWS and upload these credentials to an attacker-controlled location.

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 28, 2022