UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00022

DURI HTML SMUGGLING CAMPAIGN

DATE ISSUED: 18th August 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	LOW	MEDIUM	HIGH

OVERVIEW

First detected in July and remaining active today, Duri bypasses network security allows HTML smuggling to deliver malware, circumventing solutions such as sandboxes, legacy proxies, and firewalls. This type of attacks exploits legitimate HTTP protocols, JavaScript APIs and HTML5 APIs.

BREAKDOWN

Users clicking a malicious link are redirected to a malicious site duckdns,org, which activates a JavaScript blob (Binary Large Object) whereby malicious files ma be smuggled onto the endpoint device via their browser using HTML. The construction of the payload occurs on the client side, meaning that no objects are inspected by security solutions, as there are effectively none being transferred over the wire. The zipped folder that the user must then open and run is disguised as a Microsoft Windows Installer (MSI).

REMEDIATION STEPS

- Be wary of any file downloads from HTTP site duckdns.org, do not unzip or run any unknown files or executable MSIs
- Ensure you are running the latest version of your web browser, with latest security patches installed
- Block all URL Indicators of Compromise as listed on Rewterz using web filtering, scan network for IoC detections

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/active-malware-campaign-html-smuggling/158439/
Dark Reading https://www.darkreading.com/attacks-breaches/new-duri-campaign-uses-html-smuggling-to-deliver-malware/d/d-id/1338691
Bleeping Computer: https://www.bleepingcomputer.com/news/security/duri-campaign-smuggles-malware-via-html-and-javascript/
Rewterz: https://www.rewterz.com/rewterz-news/rewterz-threat-alert-new-duri-campaign-uses-html-smuggling-to-deliver-malware