Abuse of Windows Search to Redirect to Malware

Date: June 16th 2024 | Severity: High

Summary

This complex malware campaign uses the HTML Windows search to spread malware. The attack is initiated through an email with a zipped archive that embeds a malicious HTML file, which looks like any other normal document used daily as its disguise strategy.

Attack Vectors

- The campaign starts with a suspicious email containing an HTML attachment disguised as a routine document, like an invoice. The threat actor encloses the HTML file within a ZIP archive to enhance deception and evade email security scanners.
- The HTML attachment in this campaign, while simple, is crafted to launch a sophisticated attack. Once opened, this HTML file abuses standard web protocols to exploit Windows system functionalities.
- This attribute instructs the browser to automatically reload the page and redirect to a new URL, with a delay specified by the content attribute. In this scenario, the delay is set to zero, meaning the redirection occurs instantly as the page loads, giving the user no time to react or notice anything suspicious.
- When the HTML loads, browsers typically prompt the user to allow the search action. This security measure prevents unauthorized commands from executing potentially harmful operations without the user's consent. The redirection URL utilizes the search: protocol, a powerful but potentially risky feature that allows applications to interact directly with Windows Explorer's search function.
- The attack moves to its next phase after the user permits the search action. The search function retrieves invoice-named files from a remote server. Only one item, particularly a shortcut (LNK) file, appears in the search results. This LNK file points to a batch script (BAT) hosted on the same server, which, upon user click, could potentially trigger additional malicious operations.
- At the time of our analysis, the payload (BAT) could not be retrieved as the server appeared to be down. Nonetheless, the attack shows a sophisticated understanding of system vulnerabilities and user behaviors.

Indicator of compromise

INDICATOR TYPE	INDICATORS
SHA Hash Value	• md5 f77a4a27f749703165e2021fecd73db9 • sha1 cbc3a8e762e0f2eda9e8a9bde348d04d1d7ce17e • sha256 d136dcfc355885c502ff2c3be229791538541b748b6c07df3ced95f9a7eb2f30
URLs	• associate[.]trycloudflare[.]com@SSL\DavWWWRoot\google\INVOICE

Recommendation

- Block all threat indicators at your respective controls.
- Maintain cyber hygiene by updating your anti-virus software and implementing a patch management lifecycle.
- Deploy WAF so that helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.
- Ensure any communication towards public facing network is happening via SSL and TLS (Secure Socket Layer and Transport layer security latest version).

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Link

- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/search-spoof-abuse-of-windows-search-to-redirect-to-malware/?&web_view=true