AL2024_09 Phishing Campaign Abuses Windows Search Protocol to Deliver Malware (14th June 2024)

Description

A new phishing campaign has emerged, exploiting the Windows search protocol (search-ms URI) to distribute malicious scripts. This method leverages HTML attachments in emails to initiate Windows searches that connect to remote servers hosting harmful batch files. This sophisticated approach bypasses many security measures, posing significant risks to users.

Details

The Windows search protocol allows applications to open Windows Explorer and conduct searches based on specified parameters. While typically used to search local device indexes, it can be configured to query remote file shares and use custom titles for search windows.

The attackers exploit this functionality by embedding HTML attachments in phishing emails. These attachments trigger Windows searches on remote servers when opened, facilitating the download of malware. The attack chain follows these steps:

- **Email Attachment:** The phishing email contains an HTML attachment disguised as an invoice, compressed within a ZIP file to evade security scanners.
- **HTML Redirection:** The HTML file uses the <meta http-equiv="refresh"> tag to automatically redirect the browser to a malicious URL upon opening.
- **Fallback Mechanism**: If the meta refresh fails due to browser settings blocking redirects, an anchor tag serves as a clickable fallback link to the malicious URL, requiring user interaction.

- **Malicious Shortcut:** The search result displays a shortcut (LNK) file named as an invoice. Clicking this file triggers a batch script (BAT) hosted on the remote server.
- **Search Parameters**: The URL uses the Windows Search protocol to perform a search on a remote host with the following parameters:
    - Query: Searches for items labelled "INVOICE."
    - Crumb: Defines the search scope, pointing to a malicious server via Cloudflare.
    - Display name: Renames the search display to "Downloads" to mimic a legitimate interface.
    - Location: Utilizes Cloudflare's tunnelling service to mask the server, presenting remote resources as local files.

Indicators of Compromise (IOCs)

- **Email Characteristics**: Emails with subject lines or body text referring to invoices or other financial documents, containing ZIP files with HTML attachments.
- **HTML Attachments:** Files with <meta http-equiv="refresh"> tags or anchor tags redirecting to suspicious URLs.
- **Suspicious URLs:** URLs using the Windows Search protocol pointing to unfamiliar or suspicious domains, often masked by services like Cloudflare.
- **Registry Entries**: Unusual modifications or new entries under HKEY_CLASSES_ROOT\search or HKEY_CLASSES_ROOT\search-ms.

Recommendations

To defend against this threat, the Guyana National CIRT recommends considering the following measures:

- **User Awareness and Training:** Educate users about phishing tactics and the importance of scrutinizing email attachments, even if they appear legitimate.
- **Email Filtering:** Enhance email filtering mechanisms to detect and quarantine emails with suspicious attachments, especially ZIP files documents.
- **Registry Protection:** Delete registry entries associated with the search-ms/search URI protocol using the following commands. Note that this will disable legitimate applications relying on this protocol:

```
reg delete HKEY_CLASSES_ROOT\search /f

reg delete HKEY_CLASSES_ROOT\search-ms /f
```

- **Endpoint Protection**: Implement advanced endpoint protection solutions capable of detecting and blocking malicious scripts and batch files.
- **Network Monitoring:** Monitor network traffic for unusual activities, such as connections to remote servers using the Windows Search protocol.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Toulas, B. (2024, June 12). Phishing emails abuse Windows search protocol to push malicious scripts. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/phishing-emails-abuse-windows-search-protocol-to-push-malicious-scripts/