ultraviolet

CONFIDENTIAL

THREAT REPORT:

WarmCookie: You Don’t Want This Cookie

Services Performed By:
UltraViolet Cyber
Meredith Glass
(443) 351-7630
info@uvcyber.com

Published Date:
6/5/2024

Doc ID: ECORP_SUM_07032023_v1.1

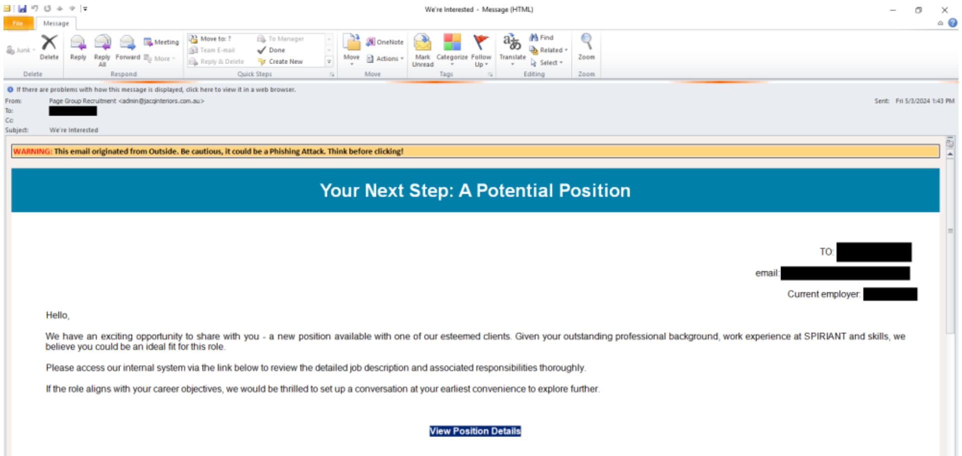
Contents

1 Executive Summary

A backdoor specific to Windows devices has been discovered, delivered via recruitment-themed phishing campaigns. Elastic Security Labs has dubbed the backdoor 'WARMCOOKIE' due to data transfer across the HTTP cookie parameter. The phishing campaign delivering the malware utilizes specifically individualized emails that pull information about a target's employers, current and potentially past, to tailor the bait to suit an individual's specific interests and skillset. The potential for compromise and further exploitation involved in this backdoor represents a significant threat, especially given the relatively simple nature of the malware, its targeted delivery method and further capability to allow additional actions on objectives.

2 Technical Analysis

WARMCOOKIE, as mentioned, uses specific information to target individuals with 'opportunities' that would presumably be enticing given the individual's employment history. Following are screenshots shared by Elastic Security Labs that provide samples for an initial phishing email that could be used in this campaign as well as the landing page that follows after clicking the malicious link within the email. It's important to note that these are only samples and the actual email and landing page appearances could vary as the campaign progresses.



We're Interested - Message (HTML)

If there are problems with how this message is displayed, click here to view it in a web browser.

From: Page Group Recruitment <admin@jacqinteriors.com.au>
To: [redacted]
Cc:
Subject: We're Interested

Sent: Fri 5/3/2024 1:43 PM

WARNING: This email originated from Outside. Be cautious, it could be a Phishing Attack. Think before clicking!

Your Next Step: A Potential Position

TO: [redacted]
email: [redacted]
Current employer: [redacted]

Hello,

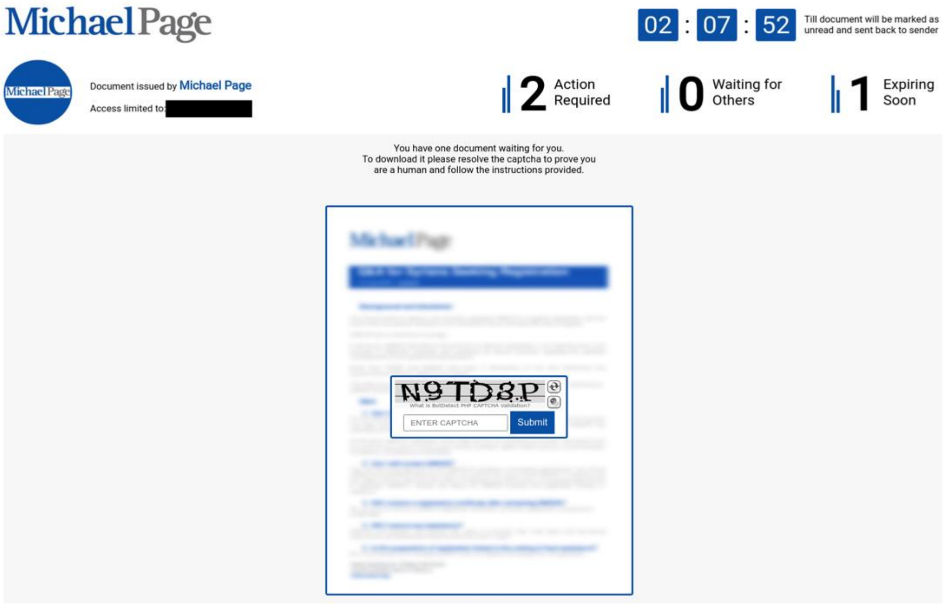
We have an exciting opportunity to share with you - a new position available with one of our esteemed clients. Given your outstanding professional background, work experience at SPIRIANT and skills, we believe you could be an ideal fit for this role.

Please access our internal system via the link below to review the detailed job description and associated responsibilities thoroughly.

If the role aligns with your career objectives, we would be thrilled to set up a conversation at your earliest convenience to explore further.

View Position Details

Phishing Email Sample



Michael Page

02 : 07 : 52 Till document will be marked as unread and sent back to sender

Document issued by Michael Page

Access limited to: [redacted]

2 Action Required

0 Waiting for Others

1 Expiring Soon

You have one document waiting for you.
To download it please resolve the captcha to prove you
are a human and follow the instructions provided.

Landing Page Sample

As shown in the landing page sample, a given target is prompted for a CAPTCHA solve and once this is entered, download of an obfuscated JavaScript file follows, with Elastic Security Labs indicating the sample obtained during their investigation was named ‘Update_23_04_2024_5689382.js’, and while other sample names collected differed, they followed a similar naming convention.

A PowerShell script is ran following the download of the malicious JS file, which downloads WARMCOOKIE and runs the dynamic link library involved as a backgrounded, autostart executable (using BITS, Background Intelligent Transfer Service). The malware runs with System privileges as a scheduled task to maintain persistence. Static analysis is confounded due to dynamic API loading and targets and identifying strings are protected via encryption.

The host compromised by this malware is fingerprinted, then connection is established with the C2 server, passing values through the HTTP cookie parameter. 7 command handlers are included to allow for command line execution, screenshotting of the target device, file reads and writes and deletion of persistence as necessary, along with several other commands.

This functionality boils down to a simple, lightweight backdoor capable of loading additional malware, ransomware and the like.

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber regularly updates our IOC database to ensure alerting is up to date
- Active threat hunting is pursued across customer environments to determine potential for and evidence of possible compromise
- Monitoring network logs for traffic to known malicious sites (in this specific case, samples noted attackers to be generating landing pages on IP address 45[.]9[.]74[.]135 with a variety of domains to match keywords associated with industry specific job searches)
- Investigating suspicious emails sent to users to determine potential for this campaign being executed in customer environments

4 What Customers Can Do

- Continue to educate employees about phishing campaigns, utilizing best practices and phishing simulations that allow for employees to learn and improve their awareness and circumspection
- Ensure emails originating from outside the organization are marked as such and appropriately filtered to avoid inadvertent interaction with potentially malicious messages

5 References

Meskauskas, Tomas. “Warmcookie Backdoor Malware.” *Www.pcrisk.com*, 12 June 2024, www.pcrisk.com/removal-guides/30211-warmcookie-backdoor-malware. Accessed 12 June 2024.

Montalbano, Elizabeth. “WarmCookie Gives Cyberattackers New Backdoor for Initial Access.” *Www.darkreading.com*, 11 June 2024, www.darkreading.com/cyberattacks-data-breaches/warmcookie-cyberattackers-backdoor-initial-access. Accessed 12 June 2024.

Stepanic, Daniel. “Dipping into Danger: The WARMCOOKIE Backdoor — Elastic Security Labs.” *Www.elastic.co*, 12 June 2024, www.elastic.co/security-labs/dipping-into-danger. Accessed 12 June 2024.