Understanding the WarmCookie Backdoor Threat

By Justin Torres

Published: 2024-07-26 · Archived: 2026-04-05 19:12:15 UTC

What is WarmCookie malware?

WarmCookie, also known as BadSpace [2], is a two-stage backdoor tool that provides functionality for threat actors to retrieve victim information and launch additional payloads. The malware is primarily distributed via phishing campaigns according to multiple open-source intelligence (OSINT) providers.

Backdoor malware: A backdoor tool is a piece of software used by attackers to gain and maintain unauthorized access to a system. It bypasses standard authentication and security mechanisms, allowing the attacker to control the system remotely.

Two-stage backdoor malware: This means the backdoor operates in two distinct phases:

1. Initial Stage: The first stage involves the initial infection and establishment of a foothold within the victim's system. This stage is often designed to be small and stealthy to avoid detection.

2. Secondary Stage: Once the initial stage has successfully compromised the system, it retrieves or activates the second stage payload. This stage provides more advanced functionalities for the attacker, such as extensive data exfiltration, deeper system control, or the deployment of additional malicious payloads.

How does WarmCookie malware work?

Reported attack patterns include emails attempting to impersonate recruitment firms such as PageGroup, Michael Page, and Hays. These emails likely represented social engineering tactics, with attackers attempting to manipulate jobseekers into engaging with the emails and following malicious links embedded within [3].

This backdoor tool also adopts stealth and evasion tactics to avoid the detection of traditional security tools. Reported evasion tactics included custom string decryption algorithms, as well as dynamic API loading to prevent researchers from analyzing and identifying the core functionalities of WarmCookie [1].

Before this backdoor makes an outbound network request, it is known to capture details from the target machine, which can be used for fingerprinting and identification [1], this includes:

- Computer name

- Username

- DNS domain of the machine

- Volume serial number

WarmCookie samples investigated by external researchers were observed communicating over HTTP to a hardcoded IP address using a combination of RC4 and Base64 to protect its network traffic [1]. Ultimately, threat actors could use this backdoor to deploy further malicious payloads on targeted networks, such as ransomware.

Darktrace Coverage of WarmCookie

Between April and June 2024, Darktrace's Threat Research team investigated suspicious activity across multiple customer networks indicating that threat actors were utilizing the WarmCookie backdoor tool. Observed cases across customer environments all included the download of unusual executable (.exe) files and suspicious outbound connectivity.

Affected devices were all observed making external HTTP requests to the German-based external IP, 185.49.69[.]41, and the URI, /data/2849d40ade47af8edfd4e08352dd2cc8.

The first investigated instance occurred between April 23 and April 24, when Darktrace detected a a series of unusual file download and outbound connectivity on a customer network, indicating successful WarmCookie exploitation. As mentioned by Elastic labs, "The PowerShell script abuses the Background Intelligent Transfer Service (BITS) to download WarmCookie and run the DLL with the Start export" [1].

Less than a minute later, the same device was observed making HTTP requests to the rare external IP address: 185.49.69[.]41, which had never previously been observed on the network, for the URI /data/b834116823f01aeceed215e592dfcba7. The device then proceeded to download masqueraded executable file from this endpoint. Darktrace recognized that these connections to an unknown endpoint, coupled with the download of a masqueraded file, likely represented malicious activity.

Following this download, the device began beaconing back to the same IP, 185.49.69[.]41, with a large number of external connections observed over port 80. This beaconing related behavior could further indicate malicious software communicating with command-and-control (C2) servers.

Darktrace's model alert coverage included the following details:

[Model Alert: Device / Unusual BITS Activity]

- Associated device type: desktop

- Time of alert: 2024-04-23T14:10:23 UTC

- ASN: AS28753 Leaseweb Deutschland GmbH

- User agent: Microsoft BITS/7.8

[Model Alert: Anomalous File / EXE from Rare External Location]

[Model Alert: Anomalous File / Masqueraded File Transfer]

- Associated device type: desktop

- Time of alert: 2024-04-23T14:11:18 UTC

- Destination IP: 185.49.69[.]41

- Destination port: 80

- Protocol: TCP

- Application protocol: HTTP

- ASN: AS28753 Leaseweb Deutschland GmbH

- User agent: Mozilla / 4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;.NET CLR 1.0.3705)

- Event details: File: http[:]//185.49.69[.]41/data/b834116823f01aeceed215e592dfcba7, total seen size: 144384B, direction: Incoming

- SHA1 file hash: 4ddf0d9c750bfeaebdacc14152319e21305443ff

- MD5 file hash: b09beb0b584deee198ecd66976e96237

[Model Alert: Compromise / Beaconing Activity To External Rare]

- Associated device type: desktop

- Time of alert: 2024-04-23T14:15:24 UTC

- Destination IP: 185.49.69[.]41

- Destination port: 80

- Protocol: TCP

- Application protocol: HTTP

- ASN: AS28753 Leaseweb Deutschland GmbH

- User agent: Mozilla / 4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;.NET CLR 1.0.3705)

Between May 7 and June 4, Darktrace identified a wide range of suspicious external connectivity on another customer’s environment. Darktrace’s Threat Research team further investigated this activity and assessed it was likely indicative of WarmCookie exploitation on customer devices.

Similar to the initial use case, BITS activity was observed on affected devices, which is utilized to download WarmCookie [1]. This initial behavior was observed with the device after triggering the model: Device / Unusual BITS Activity on May 7.

Just moments later, the same device was observed making HTTP requests to the aforementioned German IP address, 185.49.69[.]41 using the same URI /data/2849d40ade47af8edfd4e08352dd2cc8, before downloading a suspicious executable file.

Just like the first use case, this device followed up this suspicious download with a series of beaconing connections to 185.49.69[.]41, again with a large number of connections via port 80.

Similar outgoing connections to 185.49.69[.]41 and model alerts were observed on additional devices during the same timeframe, indicating that numerous customer devices had been compromised.

Darktrace's model alert coverage included the following details:

[Model Alert: Device / Unusual BITS Activity]

- Associated device type: desktop

- Time of alert: 2024-05-07T09:03:23 UTC

- ASN: AS28753 Leaseweb Deutschland GmbH

- User agent: Microsoft BITS/7.8

[Model Alert: Anomalous File / EXE from Rare External Location]

[Model Alert: Anomalous File / Masqueraded File Transfer]

- Associated device type: desktop

- Time of alert: 2024-05-07T09:03:35 UTC

- Destination IP: 185.49.69[.]41

- Protocol: TCP

- ASN: AS28753 Leaseweb Deutschland GmbH

- Event details: File: http[:]//185.49.69[.]41/data/2849d40ade47af8edfd4e08352dd2cc8, total seen size: 72704B, direction: Incoming

- SHA1 file hash: 5b0a35c574ee40c4bccb9b0b942f9a9084216816

- MD5 file hash: aa9a73083184e1309431b3c7a3e44427

[Model Alert: Anomalous Connection / New User Agent to IP Without Hostname]

- Associated device type: desktop

- Time of alert: 2024-05-07T09:04:14 UTC

- Destination IP: 185.49.69[.]41

- Application protocol: HTTP

- URI: /data/2849d40ade47af8edfd4e08352dd2cc8

- User agent: Microsoft BITS/7.8

[Model Alert: Compromise / HTTP Beaconing to New Endpoint]

- Associated device type: desktop

- Time of alert: 2024-05-07T09:08:47 UTC

- Destination IP: 185.49.69[.]41

- Protocol: TCP

- Application protocol: HTTP

- ASN: AS28753 Leaseweb Deutschland GmbH

- URI: /

- User agent: Mozilla / 4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;.NET CLR 1.0.3705) \

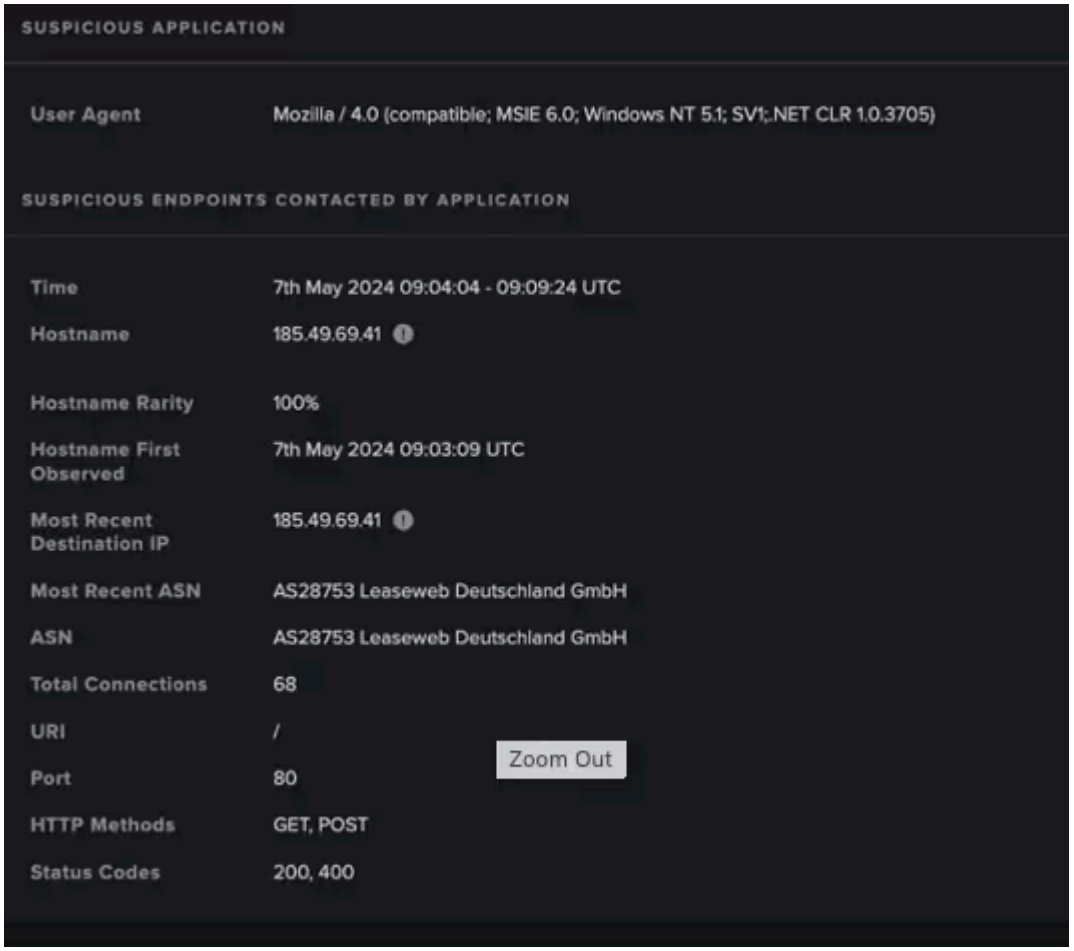

Figure 1: Cyber AI Analyst Coverage Details around the external destination, ‘185.49.69[.]41’.

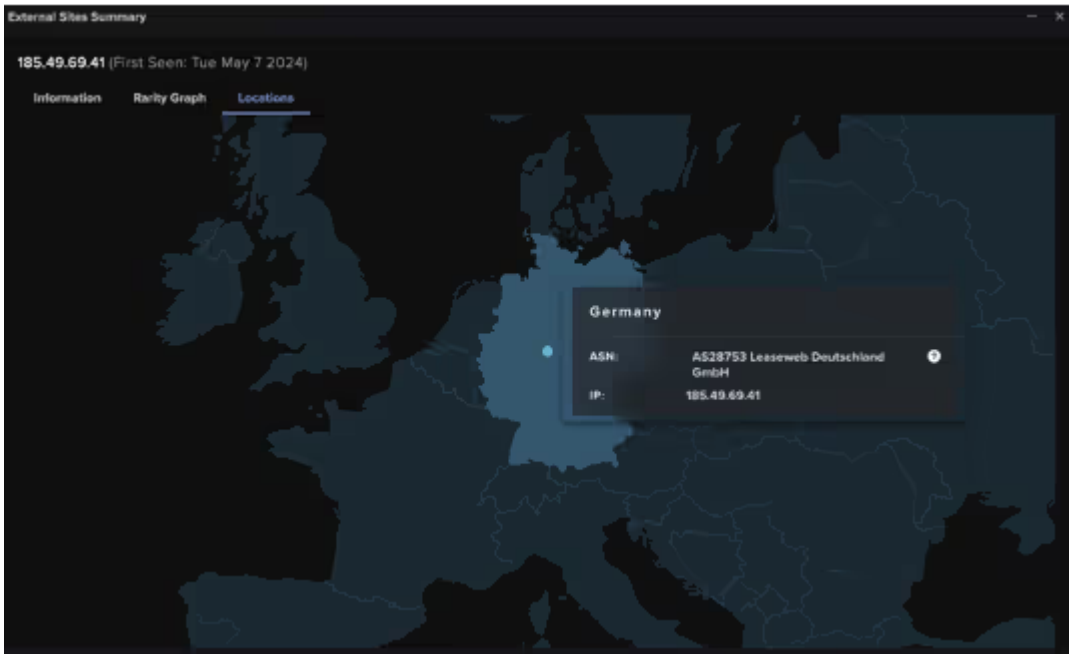

Figure 2: External Sites Summary verifying the geographical location of the external IP, 185.49.69[.]41’.

Fortunately, this particular customer was subscribed to Darktrace’s Proactive Threat Notification (PTN) service and the Darktrace Security Operation Center (SOC) promptly investigated the activity and alerted the customer. This allowed their security team to address the activity and begin their own remediation process.

In this instance, Darktrace’s Autonomous Response capability was configured in Human Confirmation mode, meaning any mitigative actions required manual application by the customer’s security team.

Despite this, Darktrace recommended two actions to contain the activity: blocking connections to the suspicious IP address 185.49.69[.]41 and any IP addresses ending with '69[.]41', as well as the ‘Enforce Pattern of Life’ action. By enforcing a pattern of life, Darktrace can restrict a device (or devices) to its learned behavior, allowing it to continue regular business activities uninterrupted while blocking any deviations from expected activity.

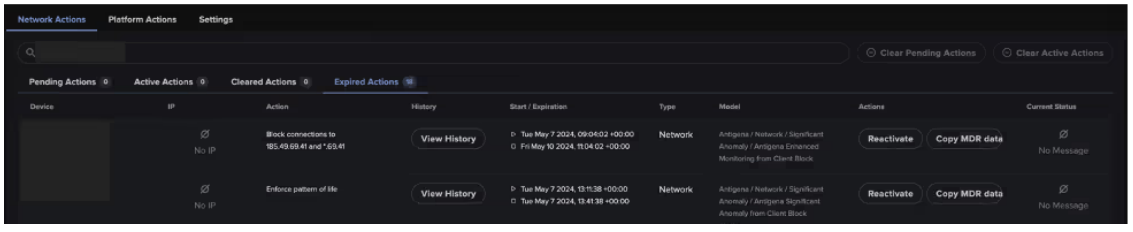

Figure 3: Actions suggested by Darktrace to contain the emerging activity, including blocking connections to the suspicious endpoint and restricting the device to its ‘pattern of life’.

Conclusion

Backdoor tools like WarmCookie enable threat actors to gather and leverage information from target systems to deploy additional malicious payloads, escalating their cyber attacks. Given that WarmCookie’s primary

distribution method seems to be through phishing campaigns masquerading as trusted recruitments firms, it has the potential to affect a large number of organizations.

In the face of such threats, Darktrace's behavioral analysis provides organizations with full visibility over anomalous activity on their digital estates, regardless of whether the threat bypasses by human security teams or email security tools. While threat actors seemingly managed to evade customers' native email security and gain access to their networks in these cases, Darktrace identified the suspicious behavior associated with WarmCookie and swiftly notified customer security teams.

Had Darktrace's Autonomous Response capability been fully enabled in these cases, it could have blocked any suspicious connections and subsequent activity in real-time, without the need of human intervention, effectively containing the attacks in the first instance.

Credit to Justin Torres, Cyber Security Analyst and Dylan Hinz, Senior Cyber Security Analyst

Appendices

Darktrace Model Detections

- Anomalous File / EXE from Rare External Location

- Anomalous File / Masqueraded File Transfer

- Compromise / Beacon to Young Endpoint

- Compromise / Beaconing Activity To External Rare

- Compromise / HTTP Beaconing to New Endpoint

- Compromise / HTTP Beaconing to Rare Destination

- Compromise / High Volume of Connections with Beacon Score

- Compromise / Large Number of Suspicious Successful Connections

- Compromise / Quick and Regular Windows HTTP Beaconing

- Compromise / SSL or HTTP Beacon

- Compromise / Slow Beaconing Activity To External Rare

- Compromise / Sustained SSL or HTTP Increase

- Compromise / Sustained TCP Beaconing Activity To Rare Endpoint

- Anomalous Connection / Multiple Failed Connections to Rare Endpoint

- Anomalous Connection / New User Agent to IP Without Hostname

- Compromise / Sustained SSL or HTTP Increase

AI Analyst Incident Coverage:

- Unusual Repeated Connections

- Possible SSL Command and Control to Multiple Endpoints

- Possible HTTP Command and Control

- Suspicious File Download

Darktrace RESPOND Model Detections:

- Antigena / Network / External Threat / Antigena Suspicious File Block

- Antigena / Network / External Threat / Antigena Suspicious File Pattern of Life Block

List of IoCs

IoC - Type - Description + Confidence

185.49.69[.]41 – IP Address – WarmCookie C2 Endpoint

/data/2849d40ade47af8edfd4e08352dd2cc8 – URI – Likely WarmCookie URI

/data/b834116823f01aeceed215e592dfcba7 – URI – Likely WarmCookie URI

4ddf0d9c750bfeaebdacc14152319e21305443ff - SHA1 Hash – Possible Malicious File

5b0a35c574ee40c4bccb9b0b942f9a9084216816 - SHA1 Hash – Possiblem Malicious File

MITRE ATT&CK Mapping

(Technique Name) – (Tactic) – (ID) – (Sub-Technique of)

Drive-by Compromise - INITIAL ACCESS - T1189

Ingress Tool Transfer - COMMAND AND CONTROL - T1105

Malware - RESOURCE DEVELOPMENT - T1588.001 - T1588

Lateral Tool Transfer - LATERAL MOVEMENT - T1570

Web Protocols - COMMAND AND CONTROL - T1071.001 - T1071

Web Services - RESOURCE DEVELOPMENT - T1583.006 - T1583

Browser Extensions - PERSISTENCE - T1176

Application Layer Protocol - COMMAND AND CONTROL - T1071

Fallback Channels - COMMAND AND CONTROL - T1008

Multi-Stage Channels - COMMAND AND CONTROL - T1104

Non-Standard Port - COMMAND AND CONTROL - T1571

One-Way Communication - COMMAND AND CONTROL - T1102.003 - T1102

Encrypted Channel - COMMAND AND CONTROL - T1573

External Proxy - COMMAND AND CONTROL - T1090.002 - T1090

Non-Application Layer Protocol - COMMAND AND CONTROL - T1095

References

[1] https://www.elastic.co/security-labs/dipping-into-danger

[2] https://www.gdatasoftware.com/blog/2024/06/37947-badspace-backdoor

[3] https://thehackernews.com/2024/06/new-phishing-campaign-deploys.html

---