

# WarmCookie Infrastructure Update: Uncovering New C2 Servers and Threats

Published: 2024-10-17 · Archived: 2026-04-05 22:40:08 UTC

## TABLE OF CONTENTS

[Introduction](#)[Initial Findings and Research](#)[Uncovering Additional Infrastructure](#)[Shared SSH Keys](#)[IPs Sharing SSH Keys](#)[Conclusion](#)[Network Observables](#)

## Introduction

On September 30, [Gen Threat Labs](#) posted a warning on X (formerly Twitter), highlighting a new wave of a FakeUpdate campaign using compromised websites to deliver the **WarmCookie backdoor**. Of note, an updated version of the backdoor adding capabilities was identified, accompanied by indicators of compromise (IoC), including an IP address.

Using this [command-and-control \(C2\) server](#) as a starting point, we identified a small subset of infrastructure sharing characteristics to the IP reported on X. Certificates and HTTP response patterns played a large role in our findings, which we'll discuss below.

## Initial Findings and Research

The IP address **38.180.91[.]117**, identified by Gen Threat Labs as a WarmCookie C2 server, is hosted within the Scalaxy B.V. ASN. Four open ports were observed: 22, 443, 3389, and 8080. By querying this IP in [Hunt](#), we can gain additional insight into its operational context, including details on port configurations and certificate history.

## 38.180.91.117 - Overview

Info Domains 0 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

IOC Hunter: Beware Of Fake Google Chrome Update That Delivers Malware

**38.180.91.117**

Scalaxy B.V.

Dallas, Texas, US

**DNS**

|             |               |
|-------------|---------------|
| Reverse DNS | Unused        |
| Forward DNS | Not available |
| Tag         | Not available |

**ASN**

|         |                |              |
|---------|----------------|--------------|
| AS58061 | 38.180.90.0/23 | Scalaxy B.V. |
|---------|----------------|--------------|

**Open Ports and Software**

| Name     | Port | Product | Version | Extra Info | Last Seen   | First Seen   |  |
|----------|------|---------|---------|------------|-------------|--------------|--|
| SSH      | 22   | -       | -       | -          | 2 weeks ago | 7 months ago |  |
| TLS/HTTP | 443  | -       | -       | -          | 3 weeks ago | 1 month ago  |  |
| TLS      | 3389 | -       | -       | -          | 2 days ago  | 4 months ago |  |
| HTTP     | 8080 | HTTPD   | 2.4.57  | -          | 3 weeks ago |              |  |

Figure 1: Overview of IP address 38.180.91.[.]117 (The IOC Hunter link in the image will take you to the above mentioned X post)

Interestingly, no associated resolving domains were detected for this IP. However, a [range of certificates](#), including both RDP and TLS, which shed light on its operational history. These certificates spanned from mid-June 2024, with the most recent first seen just two days prior to this analysis.

Additionally, HTTP responses helped in connecting other infrastructure to the updated WarmCookie backdoor. Together, these observations hint at a server that might not be static but instead adapting to changing operational requirements.

While the certificate history alone doesn't confirm we are looking at a repurposed server, it does suggest a high probability of regular maintenance or adaptation that could align with the malwares update cycle.

## 38.180.91.117 - Overview

Info Domains History (Beta) Associations **SSL History** SSH History JARM Port History Signals Activity

|         |              |                   |        |         |
|---------|--------------|-------------------|--------|---------|
| ASN     | ASN Name     | Company           | Region | Country |
| AS58061 | Scalaxy B.V. | 3NT SOLUTIONS LLP | Texas  | US      |

| Last Seen                  | First Seen                 | IP            | Ports | SubjectCommonName | IssuerOrganization       |
|----------------------------|----------------------------|---------------|-------|-------------------|--------------------------|
| 2024-10-14<br>2 days ago   | 2024-10-14<br>2 days ago   | 38.180.91.117 | 3389  | WIN-T8507HI73R7   |                          |
| 2024-09-21<br>3 weeks ago  | 2024-09-21<br>3 weeks ago  | 38.180.91.117 | 443   |                   | Internet Widgits Pty Ltd |
| 2024-08-11<br>2 months ago | 2024-08-11<br>2 months ago | 38.180.91.117 | 3389  | DESKTOP-BM56C9C   |                          |
| 2024-06-11<br>4 months ago | 2024-06-11<br>4 months ago | 38.180.91.117 | 3389  | DESKTOP-40OODPJ   |                          |

Figure 2: [SSL History overview for the initial IP linked to WarmCookie](#)

The distinct certificate properties and HTTP responses observed for this server provided key [IOCs](#) for expanding our investigation. Below, we'll discuss the additional IP's likely connected to this new version of WarmCookie.

### Uncovering Additional Infrastructure

Using [Hunt SQL](#), we executed a query primarily based on the certificate attributes, with the HTTP response adding for verification. This resulted in six additional servers sharing characteristics with the IP in the previous section. The IP addresses are listed below:

- 91.222.173[.]91
- 178.209.52[.]166
- 185.49.68[.]139
- 185.161.251[.]26
- 194.71.107[.]41
- 194.87.45[.]138

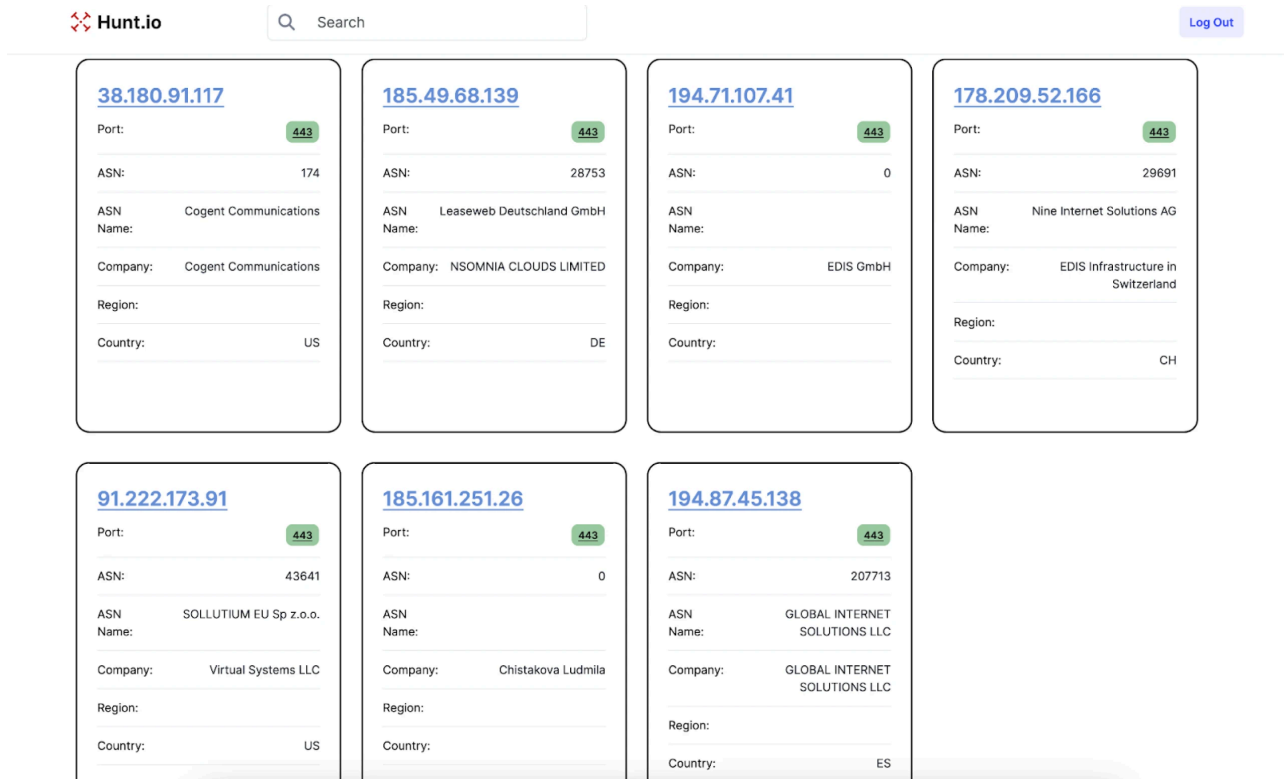


Figure 3: Hunt results for additional infrastructure linked to 38.180.91[.]117

The small number of results strongly suggests that we were indeed tracking relevant infrastructure connected to the updated WarmCookie backdoor.

To further validate our findings, we cross-referenced our results with publicly available sources. Resources such as **VirusTotal** and [ThreatFox](#) proved particularly valuable in this process.

Our scans revealed servers active from late September onward, aligning closely with the IPs listed in ThreatFox, and public reporting.

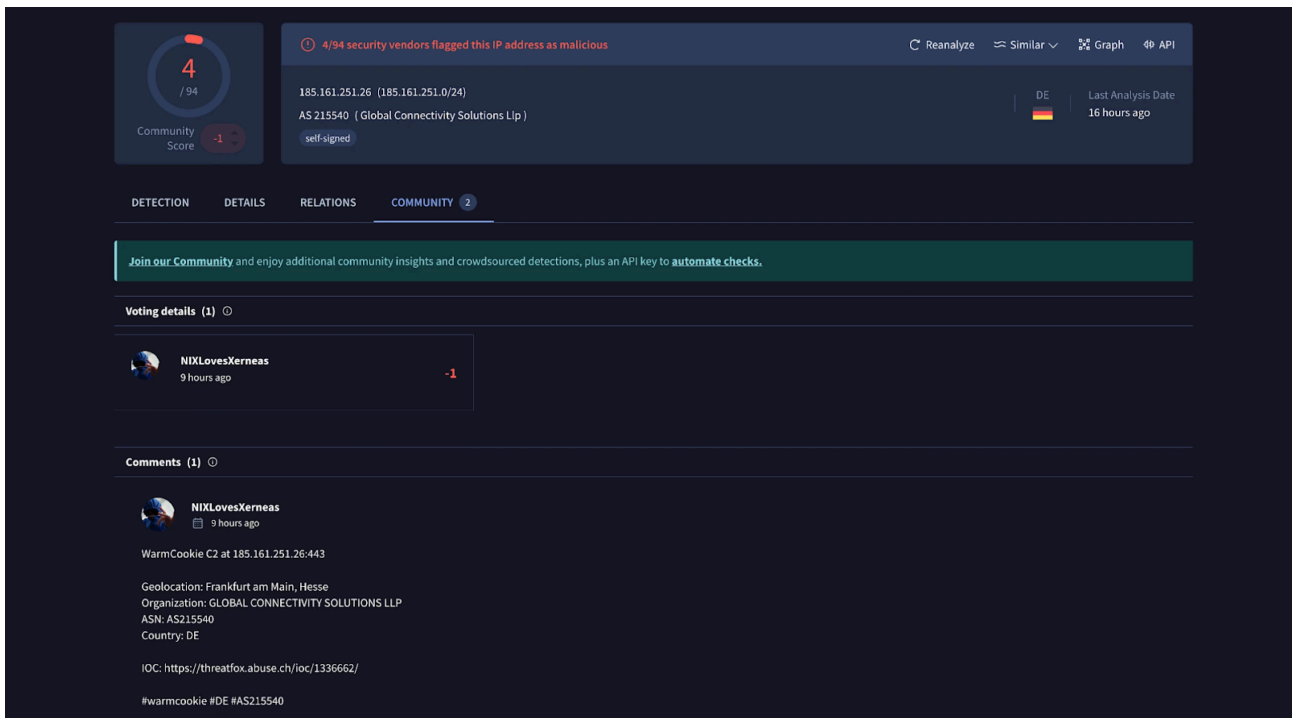


Figure 4: [Community results in VirusTotal for one of the recently found WarmCookie servers](#)

Upon reviewing the IPs returned from our query, we found that most yielded nothing significant to pivot on. That was until we got to **91.222.173[.]91**, which using the Associations tab in Hunt revealed an interesting connection. This server shared an SSH key (fingerprint: **888f05c2856ad60c5ab1e9826b57b87ae697d16303304959930f4b7e149458ac**) with 24 other servers, suggesting a potential network tied to WarmCookie, or use of a standard server image with a pre-configured SSH key that was shared/leaked.

To better understand the associations and the extent of WarmCookies operational reach, we've provided a list of the IPs and any linked domains for defenders to comb through. If you come across something interesting (we did!) let us know.

### IPs Sharing SSH Keys

| IP Address       | ASN                       | Domain(s) |
|------------------|---------------------------|-----------|
| 45.11.59[.]231   | Virtual Systems LLC       | N/A       |
| 45.134.174[.]245 | SOLLUTIUM EU Sp z.o.o.    | N/A       |
| 176.97.124[.]149 | Virtual Systems LLC       | N/A       |
| 195.66.213[.]111 | Leaseweb Deutschland GmbH | N/A       |
| 45.11.59[.]207   | SOLLUTIUM EU Sp z.o.o.    | N/A       |
| 45.134.174[.]18  | SOLLUTIUM EU Sp z.o.o.    | N/A       |

| IP Address        | ASN                    | Domain(s)  |
|-------------------|------------------------|--|
| 45.134.173[.]22   | Virtual Systems LLC    | N/A  |
| 176.97.124[.]203  | Virtual Systems LLC    | N/A  |
| 45.134.174[.]137  | SOLLUTIUM EU Sp z.o.o. | adbs.info.tntseminars[.]com<br>mx1.info.tntseminars[.]com  |
| 91.222.173[.]245  | SOLLUTIUM EU Sp z.o.o. | N/A  |
| 195.66.213[.]160  | SOLLUTIUM EU Sp z.o.o. | N/A  |
| 45.134.174[.]135  | SOLLUTIUM EU Sp z.o.o. | mx1.info.ukshowroom[.]com  |
| 31.42.177[.]38    | SOLLUTIUM EU Sp z.o.o. | N/A  |
| 185.254.198[.]219 | Virtual Systems LLC    | dig-authentic.ipq[.]co<br>Reverse DNS:<br>abrushofchange[.]org                                     |
| 45.134.174[.]254  | SOLLUTIUM EU Sp z.o.o. | Reverse DNS:<br>dedicated.vsys[.]host  |
| 91.222.173[.]140  | SOLLUTIUM EU Sp z.o.o. | N/A  |
| 91.205.2[.]219    | SOLLUTIUM EU Sp z.o.o. | N/A  |
| 45.11.59[.]230    | SOLLUTIUM EU Sp z.o.o. | N/A  |
| 195.66.213[.]243  | SOLLUTIUM EU Sp z.o.o. | N/A  |
| 45.134.174[.]136  | SOLLUTIUM EU Sp z.o.o. | mx1.info.toelicking[.]com<br>Reverse DNS:<br>rrfqm[.]site  |
| 45.134.174[.]134  | SOLLUTIUM EU Sp z.o.o. | adbs.info.ultimacomputers[.]com<br>mx1.info.ultimacomputers[.]com<br>Reverse DNS:<br>savemo[.]shop |
| 45.134.174[.]73   | SOLLUTIUM EU Sp z.o.o. | mx5.mailer.reasonablsh[.]com<br>Reverse DNS:<br>duplified.com[.]co                                 |
| 45.134.173[.]21   | Virtual Systems LLC    | N/A  |

**Table 1:** Shared SSH key IPs & domains.

One of the IPs in the above table, **91.222.173[.]140**, hosted within the SOLLUTIUUM EU Sp z.o.o. ASN, has been flagged as a **DarkGate C2** server with two recent files--Notepad++.exe and upd\_1602649.msix--actively communicating with the IP.

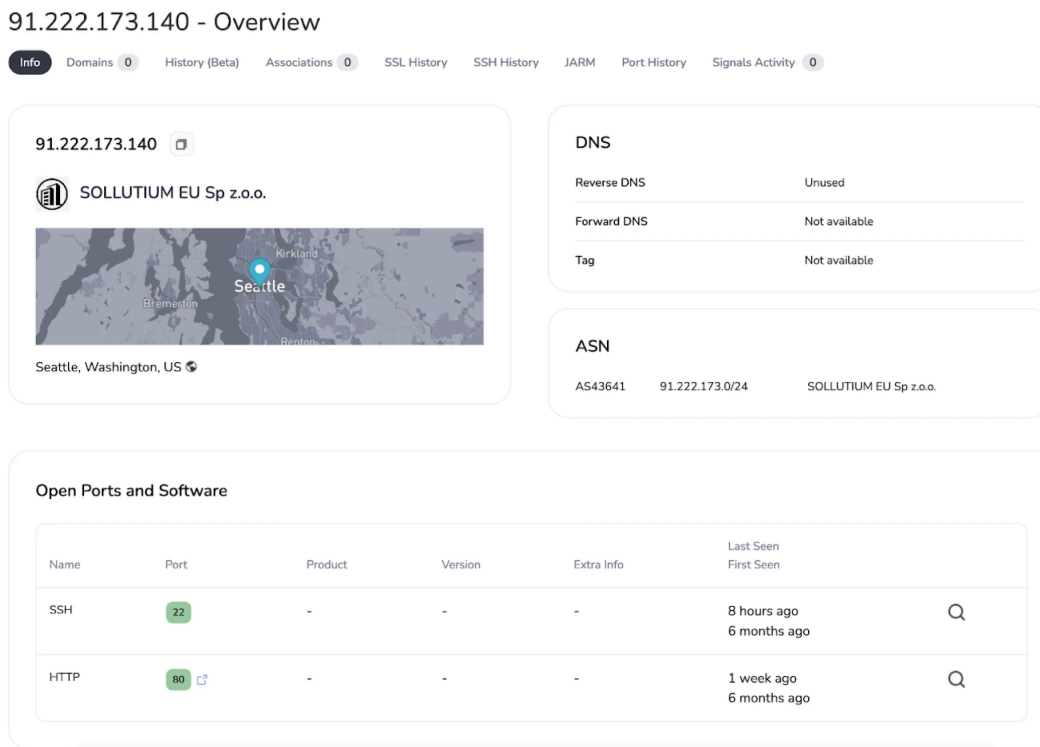


Figure 5: [Overview of the suspected DarkGate C2 IP in Hunt](#)

Given that WarmCookie has been observed in tandem with other [known malware families](#), the presence of a DarkGate C2 within this infrastructure may not be entirely surprising. Still, this finding raises intriguing questions for further investigation, which we leave as an exercise for our readers.

## Conclusion

In conclusion, our analysis of WarmCookie's updated infrastructure has uncovered key indicators, linked servers, and potential overlaps with other malware like DarkGate. While we've shared substantial findings that provide a deeper look into this evolving threat, we're withholding the full detection query to continue monitoring this activity.

While not a major player in the malware landscape, WarmCookie remains worth monitoring for its potential to gain more traction among threat actors.

Thank you for reading, and stay tuned for future updates as we continue tracking this and related threats.

## Network Observables

| IP Address      | ASN                   | Host Country | Last Seen  |
|-----------------|-----------------------|--------------|------------|
| 38.180.91[.]117 | Cogent Communications | US           | 2024-10-03 |

| <b>IP Address</b> | <b>ASN</b>                        | <b>Host Country</b> | <b>Last Seen</b> |
|-------------------|-----------------------------------|---------------------|------------------|
| 91.222.173[.]91   | SOLLUTIUM EU Sp z.o.o.            | US                  | 2024-09-29       |
| 178.209.52[.]166  | Nine Internet Solutions AG        | CH                  | 2024-10-03       |
| 185.49.68[.]139   | Leaseweb Deutschland GmbH         | DE                  | 2024-09-23       |
| 185.161.251[.]26  | GLOBAL CONNECTIVITY SOLUTIONS LLP | DE                  | 2024-09-25       |
| 194.71.107[.]41   | EDIS GmbH                         | BG                  |                  |
| 194.87.45[.]138   | GLOBAL INTERNET SOLUTIONS LLC     | ES                  |                  |

---

Source: <https://hunt.io/blog/from-warm-to-burned-shedding-light-on-updated-warmcookie-infrastructure>