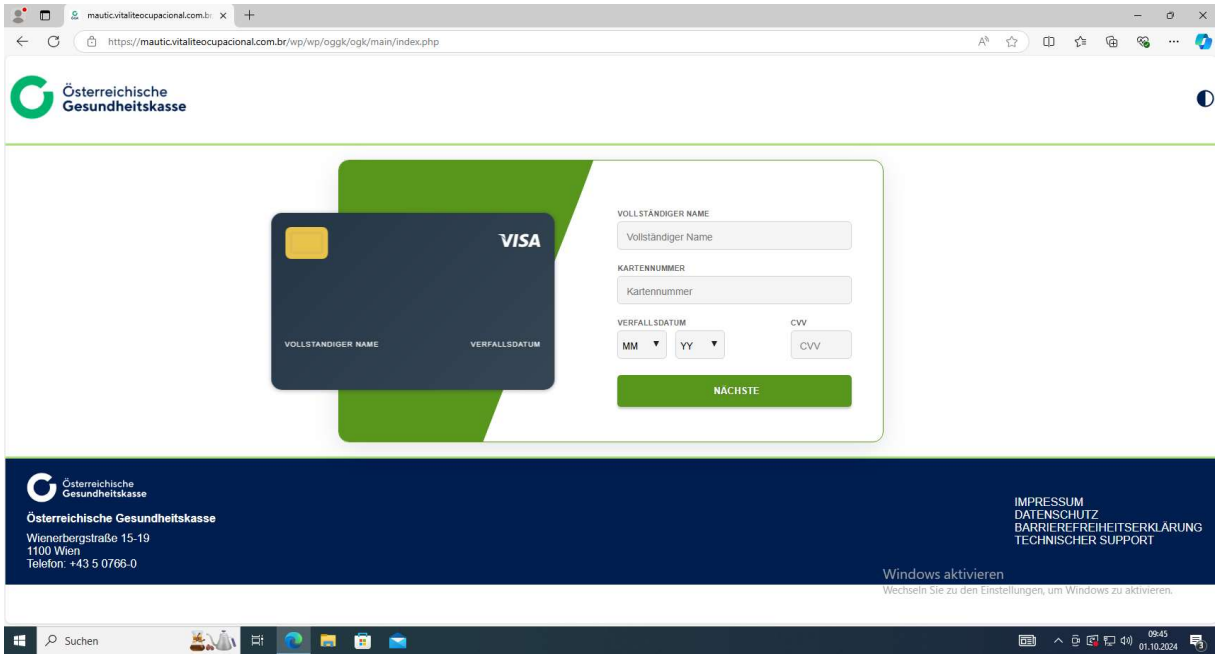
# BlueShield Analyse

Diese Analyse dient zur Darstellung der BlueShield DNS Blocks, die Zugriffe von Kunden auf verdächtige Domains geblockt hat.

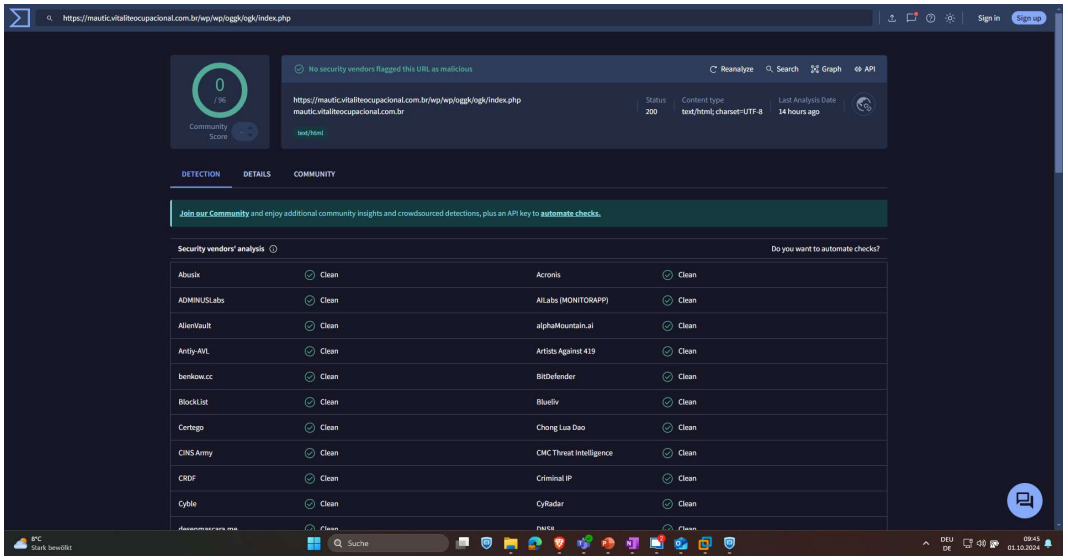
**OEGK Phishing – 30.09.2024 19:00**

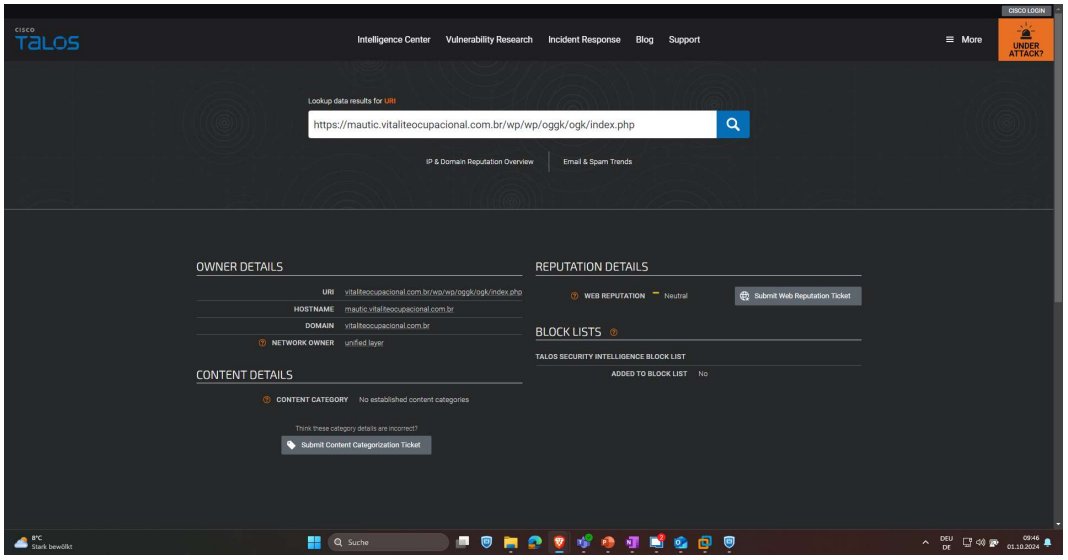
Ist ein OEGK-Phishing, welches Stand 01.10.2024 09:30 bereits 14h 30min bei allen geprüften als nicht „verdächtig“ eingestuft worden ist.

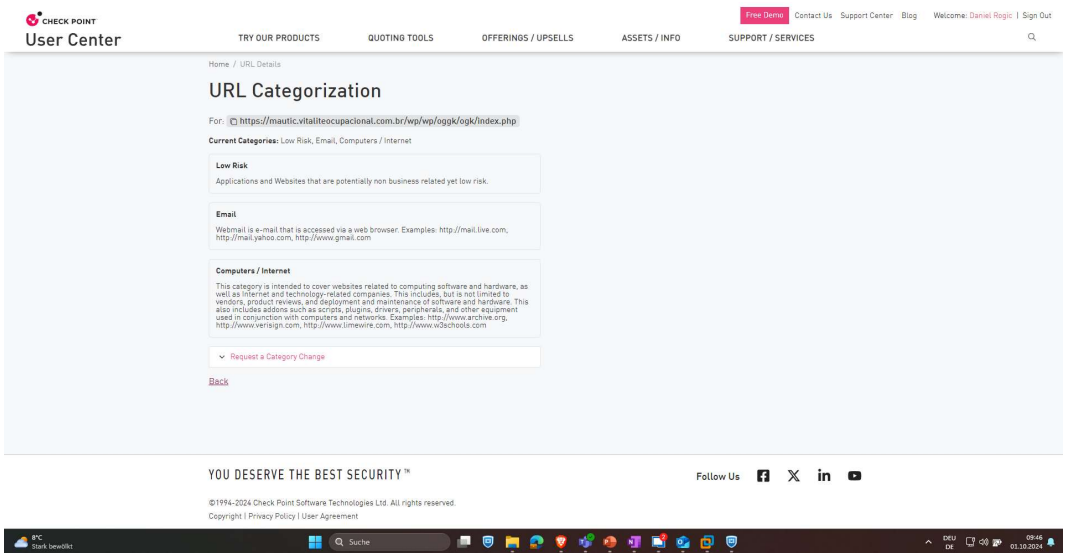


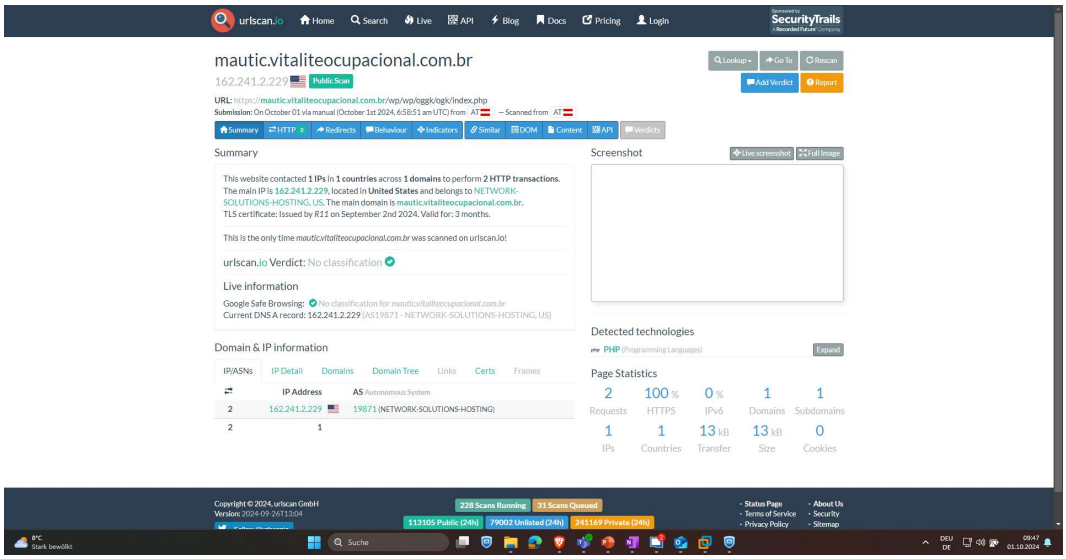

- Microsoft
  - Hat den Link erlaubt – wurde via Microsoft SafeLink geprüft
  - (Stand 01.10.2024 09:30)
- VirusTotal
  - Score 0/96
  - (Stand 01.10.2024 09:30)
- CheckPoint
  - Current Categories: Low Risk, Email, Computers / Internet
  - (Stand 01.10.2024 09:30)
- Cisco Talos
  - Web Reputation: Neutral
  - Added to block list: No
  - (Stand 01.10.2024 09:30)
- Urlscan.io
  - No classification
  - Google Safe Browsing: No classification
- AbuselPDB
  - IP was not found in database

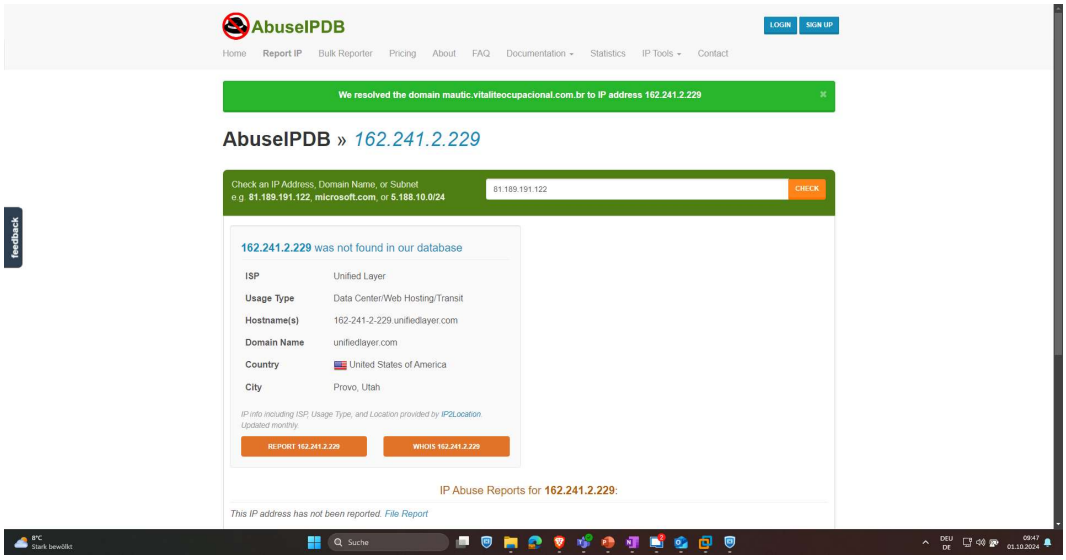
Screenshots:



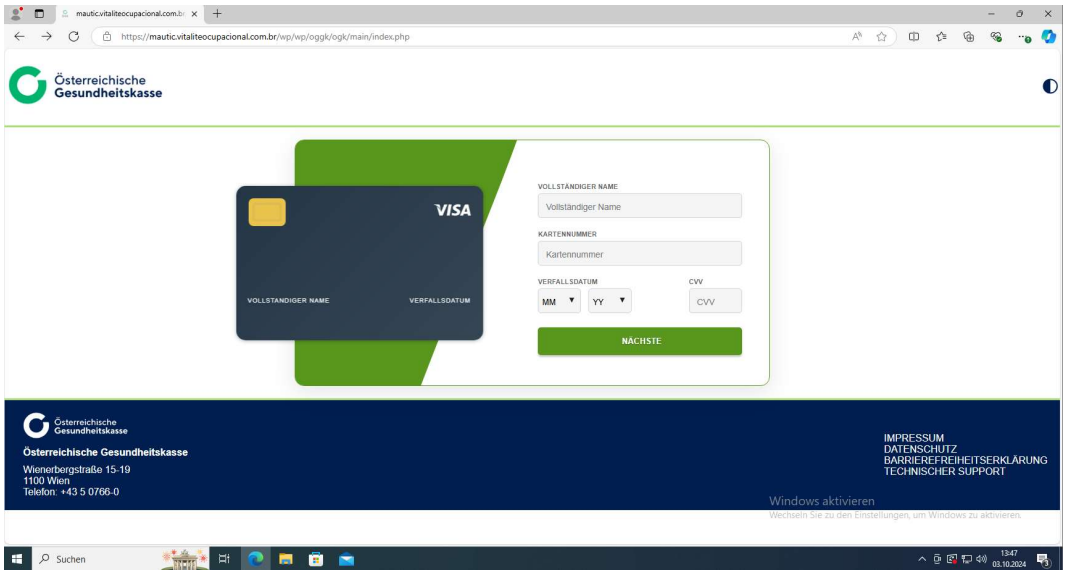

urlscan.io
Home
Search
Live
API
Blog
Docs
Pricing
Login
SecurityTrails
mautic.vitaliteocupacional.com.br
162.241.2.229
Public Scan
URL: https://mautic.vitaliteocupacional.com.br/wp/wp/oggk/ogk/index.php
Submission: On October 01 via manual (October 1st 2024, 6:58:51 am UTC) from AT — Scanned from AT
Lookup
Go To
Rescan
Add Verdict
Report
Summary
HTTP 3
Redirects
Behaviour
Indicators
Similar
DOM
Content
API
Verdicts
Summary
This website contacted 1 IPs in 1 countries across 1 domains to perform 2 HTTP transactions.
The main IP is 162.241.2.229, located in United States and belongs to NETWORK-SOLUTIONS-HOSTING, US. The main domain is mautic.vitaliteocupacional.com.br.
TLS certificate: Issued by R11 on September 2nd 2024. Valid for: 3 months.
This is the only time mautic.vitaliteocupacional.com.br was scanned on urlscan.io!
urlscan.io Verdict: No classification
Live information
Google Safe Browsing: No classification for mautic.vitaliteocupacional.com.br
Current DNS A record: 162.241.2.229 (AS19871 - NETWORK-SOLUTIONS-HOSTING, US)
Domain & IP information
IP/ASNs
IP Detail
Domains
Domain Tree
Links
Certs
Frames
IP Address
AS Autonomous System
2
162.241.2.229
19871 (NETWORK-SOLUTIONS-HOSTING)
2
1
Screenshot
Live screenshot
Full Image
Detected technologies
PHP (Programming Languages)
Expand
Page Statistics
2 Requests
100 % HTTPS
0 % IPv6
1 Domains
1 Subdomains
1 IPs
1 Countries
13 kB Transfer
13 kB Size
0 Cookies
Copyright © 2024, urlscan GmbH
Version: 2024-09-26T13:04
228 Scans Running
31 Scans Queued
113105 Public (24h)
79002 Unlisted (24h)
241169 Privates (24h)
Status Page
Terms of Service
Privacy Policy
About Us
Security
Sitemap
Suche

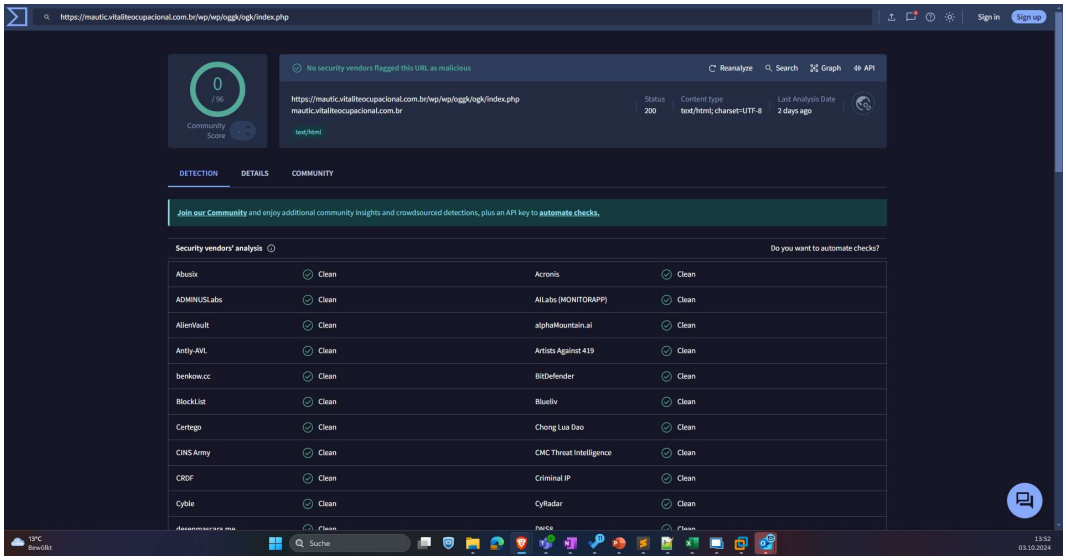

AbuseIPDB
LOGIN
SIGN UP
Home
Report IP
Bulk Reporter
Pricing
About
FAQ
Documentation
Statistics
IP Tools
Contact
We resolved the domain mautic.vitaliteocupacional.com.br to IP address 162.241.2.229
AbuseIPDB » 162.241.2.229
Check an IP Address, Domain Name, or Subnet
e.g. 81.189.191.122, microsoft.com, or 5.188.10.0/24
81.189.191.122
CHECK
feedback
162.241.2.229 was not found in our database
ISP
Unified Layer
Usage Type
Data Center/Web Hosting/Transit
Hostname(s)
162-241-2-229.unifiedlayer.com
Domain Name
unifiedlayer.com
Country
United States of America
City
Provo, Utah
IP info including ISP, Usage Type, and Location provided by IP2Location.
Updated monthly.
REPORT 162.241.2.229
WHOIS 162.241.2.229
IP Abuse Reports for 162.241.2.229:
This IP address has not been reported. File Report
Suche

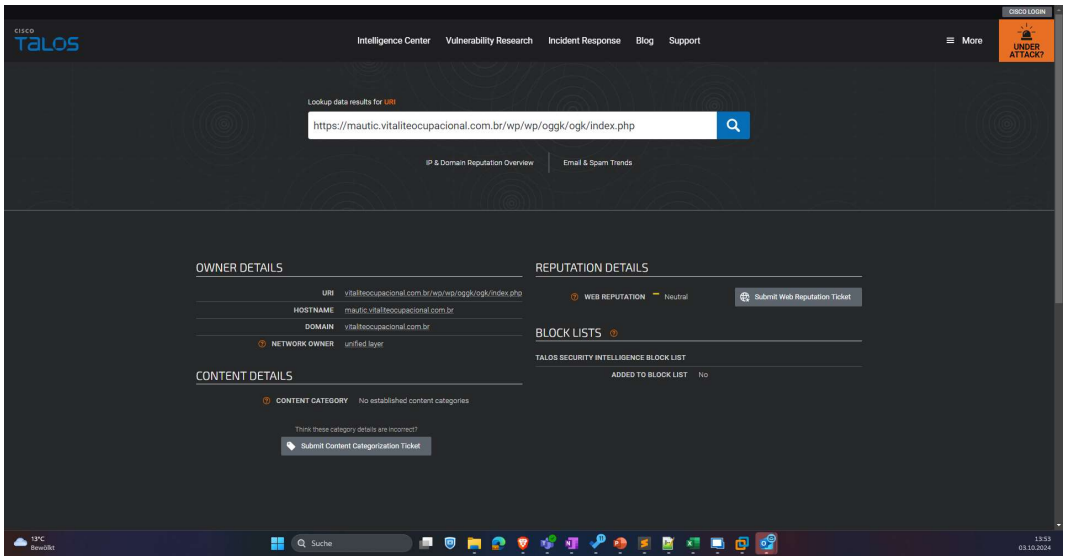
**OEGK Phishing Update – 03.10.2024 13:30**

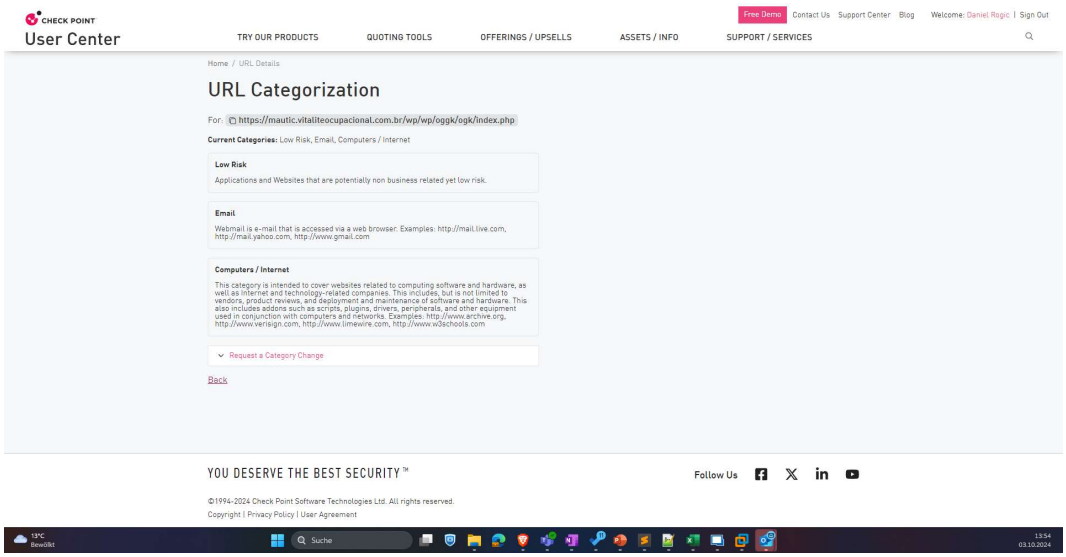
Die Website ist weiterhin erreichbar und wurde nun auch von der Microsoft als "bösartig" eingestuft, sonst hat noch immer niemand der zuvor überprüften Hersteller/Services die Seite blockiert. Die Microsoft hat die Website etwa 2 Tage später blockiert.

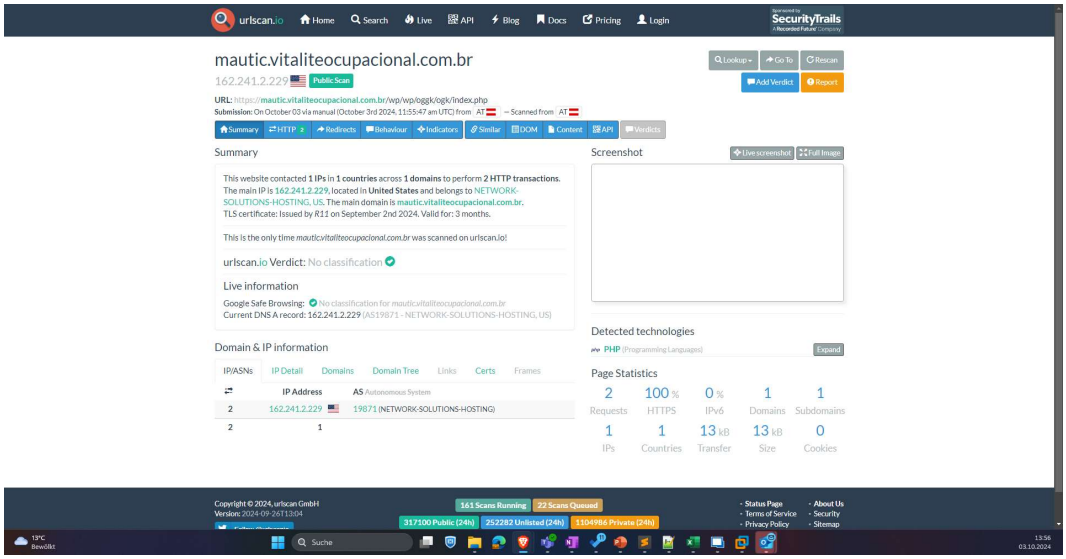
Screenshots:

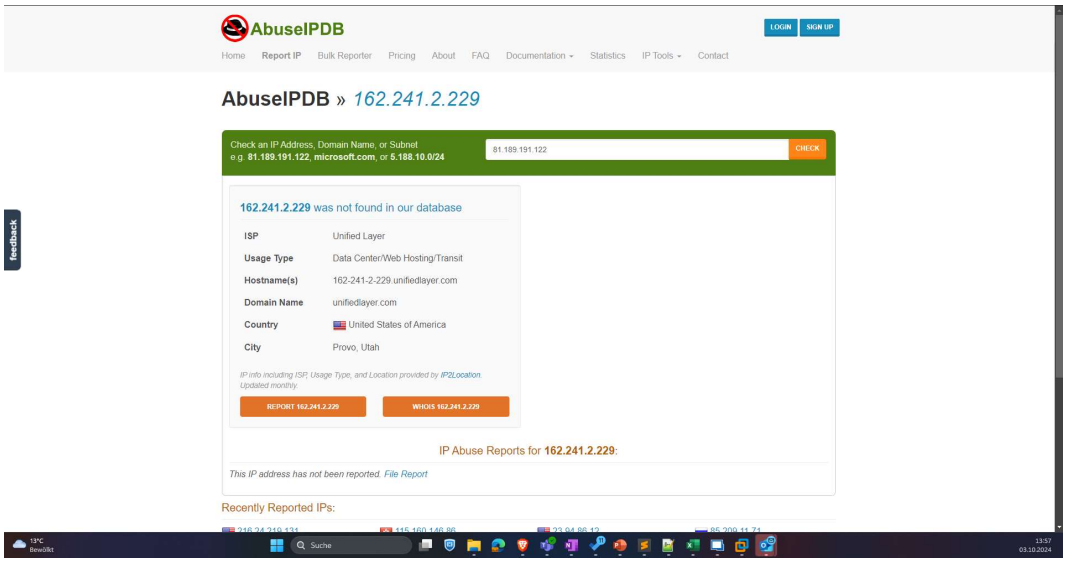


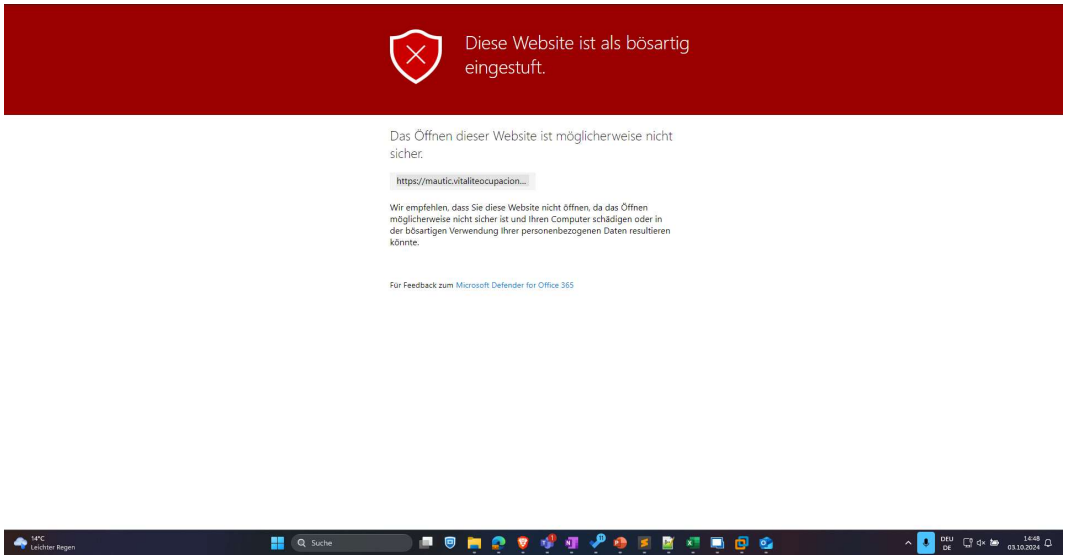




CISCO TALOS
Intelligence Center
Vulnerability Research
Incident Response
Blog
Support
More
UNDER ATTACK?
Lookup data results for URI
https://mautic.vitaliteocupacional.com.br/wp/wp/oggk/ogk/index.php
IP & Domain Reputation Overview
Email & Spam Trends
OWNER DETAILS
URI vitaliteocupacional.com.br/wp/wp/oggk/ogk/index.php
HOSTNAME mautic.vitaliteocupacional.com.br
DOMAIN vitaliteocupacional.com.br
NETWORK OWNER unified layer
CONTENT DETAILS
CONTENT CATEGORY No established content categories
Think these category details are incorrect?
Submit Content Categorization Ticket
REPUTATION DETAILS
WEB REPUTATION Neutral
Submit Web Reputation Ticket
BLOCK LISTS
TALOS SECURITY INTELLIGENCE BLOCK LIST
ADDED TO BLOCK LIST No


CHECK POINT
User Center
TRY OUR PRODUCTS
QUOTING TOOLS
OFFERINGS / UPSELLS
ASSETS / INFO
SUPPORT / SERVICES
Free Demo
Contact Us
Support Center
Blog
Welcome: Daniel Rogic | Sign Out
Home / URL Details
URL Categorization
For: https://mautic.vitaliteocupacional.com.br/wp/wp/oggk/ogk/index.php
Current Categories: Low Risk, Email, Computers / Internet
Low Risk
Applications and Websites that are potentially non business related yet low risk.
Email
Webmail is e-mail that is accessed via a web browser. Examples: http://mail.live.com, http://mail.yahoo.com, http://www.gmail.com
Computers / Internet
This category is intended to cover websites related to computing software and hardware, as well as internet and technology-related companies. This includes, but is not limited to vendors, product reviews, and deployment and maintenance of software and hardware. This also includes addons such as scripts, plugins, drivers, peripherals, and other equipment used in conjunction with computers and networks. Examples: http://www.archive.org, http://www.verisign.com, http://www.limewire.com, http://www.w3schools.com
Request a Category Change
Back
YOU DESERVE THE BEST SECURITY™
Follow Us
©1994-2024 Check Point Software Technologies Ltd. All rights reserved.
Copyright | Privacy Policy | User Agreement

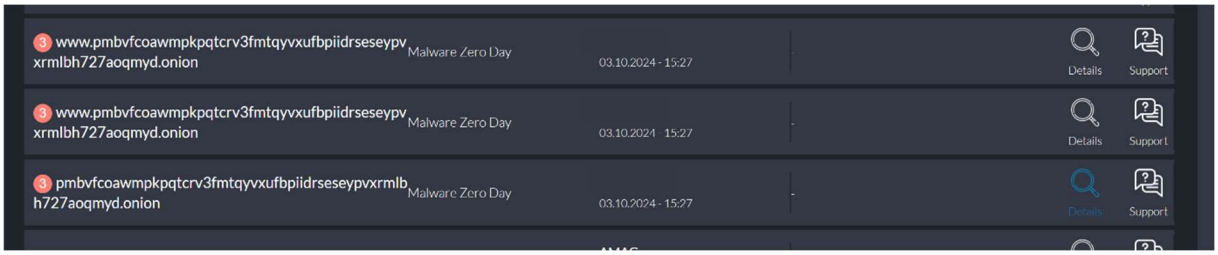

urlscan.io
Home
Search
Live
API
Blog
Docs
Pricing
Login
SecurityTrails
mautic.vitaliteocupacional.com.br
162.241.2.229
Public Scan
Lookup
Go To
Rescan
Add Verdict
Report
URL: https://mautic.vitaliteocupacional.com.br/wp/wp/oggk/ogk/index.php
Submission: On October 03 via manual (October 3rd 2024, 11:55:47 am UTC) from AT — Scanned from AT
Summary
HTTP 2
Redirects
Behaviour
Indicators
Similar
DOM
Content
API
Verdicts
Summary
This website contacted 1 IPs in 1 countries across 1 domains to perform 2 HTTP transactions.
The main IP is 162.241.2.229, located in United States and belongs to NETWORK-SOLUTIONS-HOSTING, US. The main domain is mautic.vitaliteocupacional.com.br.
TLS certificate: Issued by R11 on September 2nd 2024. Valid for: 3 months.
This is the only time mautic.vitaliteocupacional.com.br was scanned on urlscan.io!
urlscan.io Verdict: No classification
Live information
Google Safe Browsing: No classification for mautic.vitaliteocupacional.com.br
Current DNS A record: 162.241.2.229 (AS19871 - NETWORK-SOLUTIONS-HOSTING, US)
Domain & IP information
IP/ASNs
IP Detail
Domains
Domain Tree
Links
Certs
Frames
IP Address
AS Autonomous System
2
162.241.2.229
19871 (NETWORK-SOLUTIONS-HOSTING)
2
1
Screenshot
Live screenshot
Full Image
Detected technologies
PHP (Programming Languages)
Expand
Page Statistics
2 Requests
100 % HTTPS
0 % IPv6
1 Domains
1 Subdomains
1 IPs
1 Countries
13 kB Transfer
13 kB Size
0 Cookies
Copyright © 2024, urlscan GmbH
Version: 2024-09-26T13:04
161 Scans Running
22 Scans Queued
317100 Public (24h)
252282 Unlisted (24h)
1104986 Private (24h)
Status Page
Terms of Service
Privacy Policy
About Us
Security
Sitemap


AbuseIPDB
LOGIN
SIGN UP
Home
Report IP
Bulk Reporter
Pricing
About
FAQ
Documentation
Statistics
IP Tools
Contact
AbuseIPDB » 162.241.2.229
Check an IP Address, Domain Name, or Subnet
e.g. 81.189.191.122, microsoft.com, or 5.188.10.0/24
81.189.191.122
CHECK
feedback
162.241.2.229 was not found in our database
ISP
Unified Layer
Usage Type
Data Center/Web Hosting/Transit
Hostname(s)
162-241-2-229.unifiedlayer.com
Domain Name
unifiedlayer.com
Country
United States of America
City
Provo, Utah
IP info including ISP, Usage Type, and Location provided by IP2Location.
Updated monthly.
REPORT 162.241.2.229
WHOIS 162.241.2.229
IP Abuse Reports for 162.241.2.229:
This IP address has not been reported. File Report
Recently Reported IPs:
Suche


Diese Website ist als bösartig eingestuft.
Das Öffnen dieser Website ist möglicherweise nicht sicher.
https://mautic.vitaliteocupacion...
Wir empfehlen, dass Sie diese Website nicht öffnen, da das Öffnen möglicherweise nicht sicher ist und Ihren Computer schädigen oder in der bösartigen Verwendung Ihrer personenbezogenen Daten resultieren könnte.
Für Feedback zum Microsoft Defender for Office 365
Suche

**Tor-Netzwerk und verdächtige [.]ru Blocks – 03.10.2024**

Am 03.10.2024 sind weitere Blocks aufgetaucht. Dabei wurden Versuche, folgende ONION Links von einem BlueShield Kunden aus aufzurufen, geblockt:



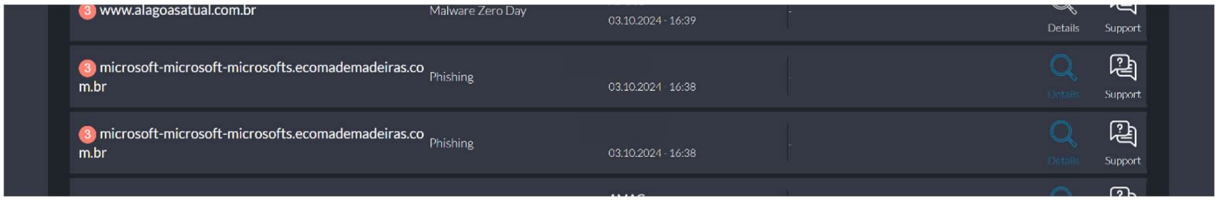

Außerdem wurden folgende Aufrufe ebenfalls geblockt:


Dabei ist es um folgendes gegangen:

- `https://www[].qztx[.]choncisev[].ru/security/2fa/setup/db3f4304ea7c325db3406c8cf83b983ae1edf6c38b2ce230239388decf490fd5`
    - War ein klassischer URL Subpath inkl. KIT
- `https://www[.]zpywrrzzmw8ta8rbep61[].8yn7do7[.]ru/media/file/punycode.js`
    - War ein schädliches Script (JavaScript) getarnt als PDF-Download

**Disclaimer:** Die Domänen waren leider sehr schnell wieder down, weshalb eine Analyse eher beschränkt möglich war. Diese Domänen wechseln laufend, teilweise sogar in Stundentakten, damit sie von den meisten Tools freigeschaltet bleiben. Sie hosten aber in der Regel dann immer dasselbe.

**Microsoft Logon Phishing – 03.10.2024**



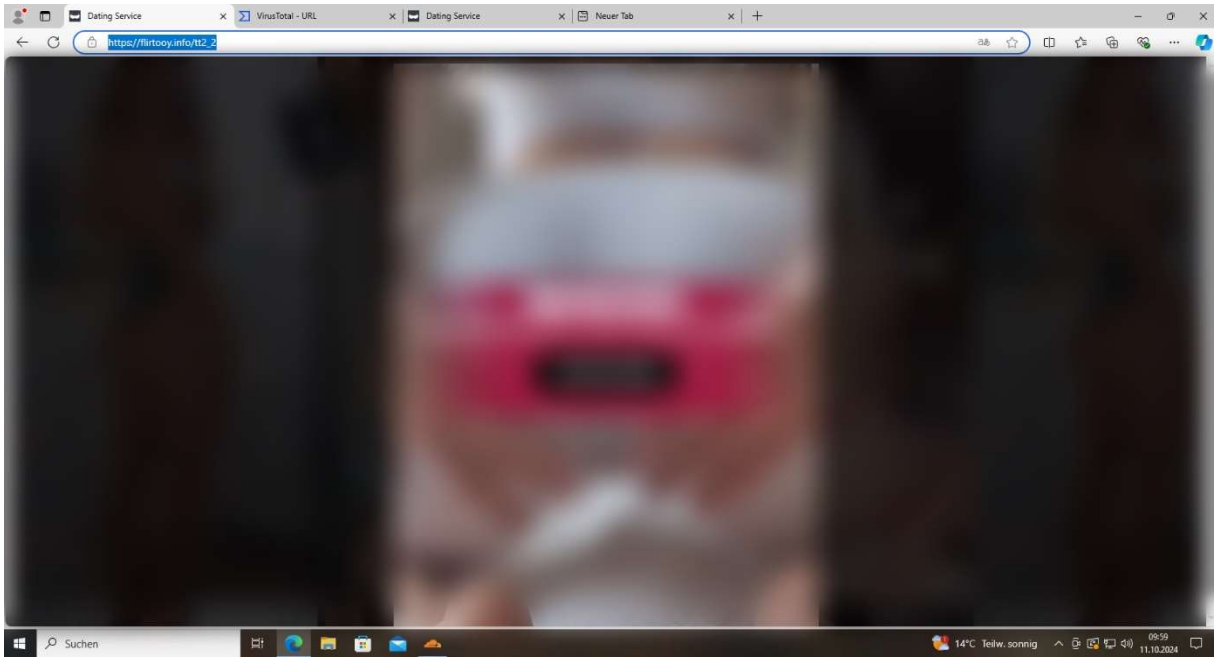

Diese Domains sind am 03.10.2024 von dem Microsoft durchgelassen worden. Sie werden generell von den meisten durchgelassen, da sie sich auch ständig ändern.

`microsoft-microsoft-microsofts[.]ecomademadeiras[.]com[.]br`

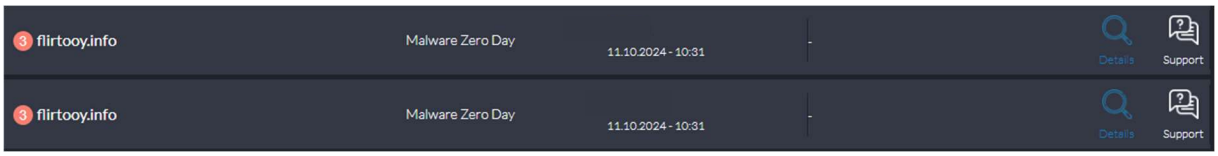
war beispielsweise davor

`office-microsoft-microsoft-microsoft[.]mcarneiroadvocacia[.]com[.]br`

Dating Phishing Scam – 11.10.2024 10:00

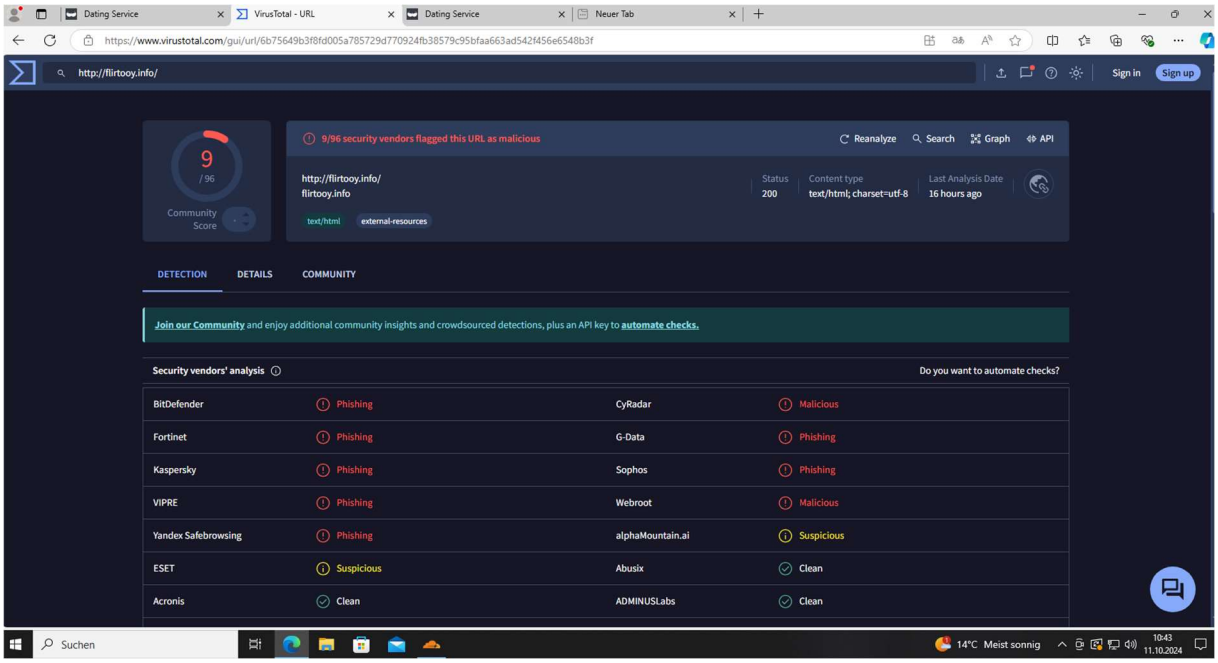



https://eur06[.]safelinks.protection[.]outlook[.]com/?url=https%3A%2F%2Fflirtooy.info%2Ftt2_2&data=05%7C02%7Cdaniel.rogic%40snapsec.at%7C1efab8377b3f44e5dd6608dce9c9ee95%7C6376a8d3df874253982f5dd91e72a429%7C0%7C0%7C638642302015282970%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C40000%7C%7C%7C&sdata=j4F0ZP8%2Bro5zV3YUPpKzYFtjLc3Gf2uqbsrOfA3%2FthU%3D&reserved=0




Die Domain flirtooy[.]info wurde bei einem Kunden über 1000-mal geblockt vom 10.10.2024 - 10:46 bis 11.10.2024 – 10:39. Stand 11.10.2024 10:30 wird es von Microsoft noch immer durchgelassen. Der SafeLink oben wurde dafür verwendet.

Von BlueShield wird es sowohl als Phishing eingestuft, als auch als Malware verteilend. VirusTotal zeigt es bereits auch als Malicious an bei 9/96 Vendors.





**Stand 14.10.2024 17:00**

- Wird von der Microsoft noch immer **nicht geblockt**