**MALICIOUS**

Classifications: -
Threat Names: -
Verdict Reason: -

| Sample Type | URL |
|---|---|
| File Name | hxxps://usgr[.]us08wr139d5[.]co/update?token=kn27oJ5oY7epXEk769 |
| ID | #6626765 |
| MD5 | b1b4b1baae4b86064b29b0ae9c946297 |
| SHA1 | 3fd8af083d53c19a8b375c6e9f9bbe406ce37baf |
| SHA256 | 7fe7db2b5fde6653a3b73cb533e53a20f8d87efd6f5071a577fba4649311ea3b |
| File Size | 59 bytes |
| Report Created | 2024-04-03 20:38 (UTC) |
| Target Environment | windows 10 (64bit TH2 -EN- WEB_ANALYSIS) \| web_root |

# OVERVIEW

## VMRay Threat Identifiers (6 rules, 9 matches)

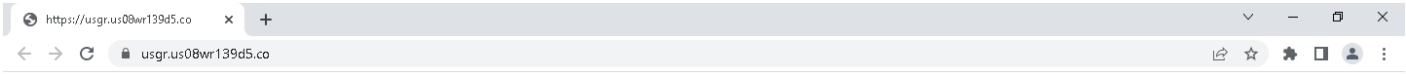
| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 4/5 | Reputation | Malicious host or URL detected via reputation | 4 | - |
| | • Submitted URL "hxxps://usgr[.]us08wr139d5[.]co/update?token=kn27oJ5oY7epXEk769" is a known malicious URL and was reported as "Phishing".<br>• Contacted URL "hxxps://usgr[.]us08wr139d5[.]co/pg?do=index" is a known malicious URL and was reported as "Phishing".<br>• Contacted URL "hxxps://usgr[.]us08wr139d5[.]co" is a known malicious URL and was reported as "Phishing".<br>• Contacted URL "hxxps://usgr[.]us08wr139d5[.]co/favicon.ico" is a known malicious URL and was reported as "Phishing". | | | |
| 4/5 | Heuristics | Combination of other detections indicates the page is malicious | 1 | - |
| | • Pretends to belong to USPS. | | | |
| 2/5 | Heuristics | Page secured via a Domain Validated SSL certificate | 1 | - |
| | • Host usgr.us08wr139d5.co uses DV certificate issued by Google Trust Services LLC to us08wr139d5.co. | | | |
| 2/5 | Heuristics | Page is hosted on a recently registered domain | 1 | - |
| | • Domain usgr.us08wr139d5.co was registered just 7 days ago. | | | |
| 1/5 | Masquerade | Page uses exact favicon of a popular online service | 1 | - |
| | • Uses the exact favicon of USPS. | | | |
| 1/5 | Heuristics | Suspicious page characteristics | 1 | - |
| | • Page hxxps://usgr[.]us08wr139d5[.]co has no meta tags. | | | |

## Sample Information

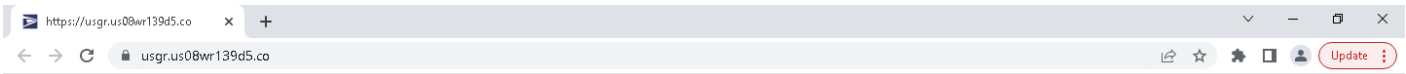
| | |
|---|---|
| ID | #6626765 |
| MD5 | b1b4b1baae4b86064b29b0ae9c946297 |
| SHA1 | 3fd8af083d53c19a8b375c6e9f9bbe406ce37baf |
| SHA256 | 7fe7db2b5fde6653a3b73cb533e53a20f8d87efd6f5071a577fba4649311ea3b |
| SSDeep | 3:N82fkwYBTSkwSTcn:22fkwcTNwSQ |
| File Name | hxxps://usgr[.]us08wr139d5[.]co/update?token=kn27oJ5oY7epXEk769 |
| File Size | 59 bytes |
| Sample Type | URL |
| Has Macros | ✔ |

## Analysis Information

| | |
|---|---|
| Creation Time | 2024-04-03 20:38 (UTC) |
| Analysis Duration | 00:00:28 |
| Termination Reason | No Recent or Pending Activity |
| Number of Monitored Processes | 0 |
| Execution Successful | True |
| Reputation Enabled | ✔ |
| WHOIS Enabled | ✖ |
| Built-in AV Enabled | ✔ |
| Built-in AV Applied On | Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files |
| Number of AV Matches | 0 |
| YARA Enabled | ✔ |
| YARA Applied On | Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files |
| Number of YARA Matches | 0 |




Not Found




Not Found

# NETWORK

## General

7.33 KB total sent

26.83 KB total received

2 ports 443, 53

2 contacted IP addresses

0 URLs extracted

0 files downloaded

1 malicious hosts detected

## DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

## HTTP/S

4 URLs contacted, 1 servers

1 sessions, 18.39 KB sent, 58.14 KB received

## HTTP Requests

| Method | URL | Dest. IP | Dest. Port | Status Code | Response Size | Verdict |
|---|---|---|---|---|---|---|
| GET | hxxps://usgr[.]us08wr139d5[.]co/favicon.ico | - | - | - | 0 bytes | MALICIOUS |
| GET | hxxps://usgr[.]us08wr139d5[.]co/pg?do=index | - | - | - | 0 bytes | MALICIOUS |
| GET | hxxps://usgr[.]us08wr139d5[.]co/update?token=kn27oJ5oY7epXEk769 | - | - | - | 0 bytes | MALICIOUS |
| GET | hxxps://usgr[.]us08wr139d5[.]co | - | - | - | 0 bytes | MALICIOUS |

## DNS Requests

| Type | Hostname | Response Code | Resolved IPs | CNames | Verdict |
|---|---|---|---|---|---|
| A | usgr[.]us08wr139d5[.]co | NO_ERROR | 104.21.25.224, 172.67.134.206 | - | SUSPICIOUS |

# ARTIFACTS

## URL

| URL | Category | IP Address | Country | HTTP Methods | Verdict |
|---|---|---|---|---|---|
| hxxps://usgr[.]us08wr139d5[.]co/update?token=kn27oJ5oY7epXEk769 | Sample, Contacted | 104.21.25.224, 172.67.134.206 | United States | GET | MALICIOUS |
| hxxps://usgr[.]us08wr139d5[.]co/pg?do=index | Contacted | 104.21.25.224, 172.67.134.206 | United States | GET | MALICIOUS |
| hxxps://usgr[.]us08wr139d5[.]co | Contacted, Extracted | 104.21.25.224, 172.67.134.206 | United States | GET | MALICIOUS |
| hxxps://usgr[.]us08wr139d5[.]co/favicon.ico | Contacted | 104.21.25.224, 172.67.134.206 | United States | GET | MALICIOUS |

## Domain

| Domain | IP Address | Country | Protocols | Verdict |
|---|---|---|---|---|
| usgr[.]us08wr139d5[.]co | 104.21.25.224, 172.67.134.206 | United States | DNS, TLS, HTTPS, UDP, TCP | SUSPICIOUS |

## IP

| IP Address | Domains | Country | Protocols | Verdict |
|---|---|---|---|---|
| 104.21.25.224 | usgr[.]us08wr139d5[.]co | - | DNS, TLS, HTTPS, UDP, TCP | CLEAN |
| 172.67.134.206 | usgr[.]us08wr139d5[.]co | United States | DNS | CLEAN |

## YARA / AV

No YARA or AV matches available.

# ENVIRONMENT

### Virtual Machine Information

| | |
|---|---|
| Name | win10_64_th2_en_web |
| Description | windows 10 (64bit TH2 -EN- WEB_ANALYSIS) |
| Architecture | - |
| Operating System | - |
| Kernel Version | - |
| Network Scheme Name | Local Gateway |
| Network Config Name | Local Gateway |

### Platform Information

| | |
|---|---|
| Platform Version | 2024.2.1 |
| Web Engine Version | 1.5.0 / 03/23/2024 11:02 |
| Static Engine Version | 2024.2.1.0 / 2024-03-23 09:36:38 |
| AV Exceptions Version | 2024.2.1.5 / 2024-03-22 20:39:30 |
| ML Detection Models Version | 2024.2.1.5 / 2024-03-22 20:39:30 |
| Link Detonation Heuristics Version | 2024.2.1.9 / 2024-03-26 09:11:11 |
| Signature Trust Store Version | 2024.2.1.9 / 2024-03-26 09:11:11 |
| VMRay Threat Identifiers Version | 2024.2.1.12 / 2024-03-28 09:41:51 |
| Web Engine Auto UI Rules Version | 2024.2.1.9 / 2024-03-26 09:11:11 |
| YARA Built-in Ruleset Version | 2024.2.1.13 |

### Anti Virus Information

| | |
|---|---|
| Built-in AV Version | AVCORE v2.2 Linux/x86_64 11.0.1.21 (August 15, 2021) |
| Built-in AV Database Update Release Date | 2024-04-03 15:37:29 |
| Built-in AV Database Records | 14030512 |

### Software Information

| | |
|---|---|
| Adobe Acrobat Reader Version | Not installed |
| Microsoft Office | Not installed |
| Microsoft Office Version | Not installed |
| Hangul Office | Not installed |
| Hangul Office Version | Not installed |
| Internet Explorer Version | 11.0.10586.0 |
| Chrome Version | 106.0.5249.119 |
| Firefox Version | Not installed |
| Flash Version | Not installed |
| Java Version | Not installed |

### System Information

| | |
|---|---|
| Computer Name | XC64ZB |

| | |
|---|---|
| User Domain | XC64ZB |
| User Name | RDhJ0CNFevzX |
| User Profile | C:\Users\RDhJ0CNFevzX |
| Temp Directory | C:\Users\RDHJ0C~1\AppData\Local\Temp |
| System Root | C:\Windows |