

NETMANAGEIT

Intelligence Report

Threat actors leverage document publishing sites for ongoing credential and session token theft

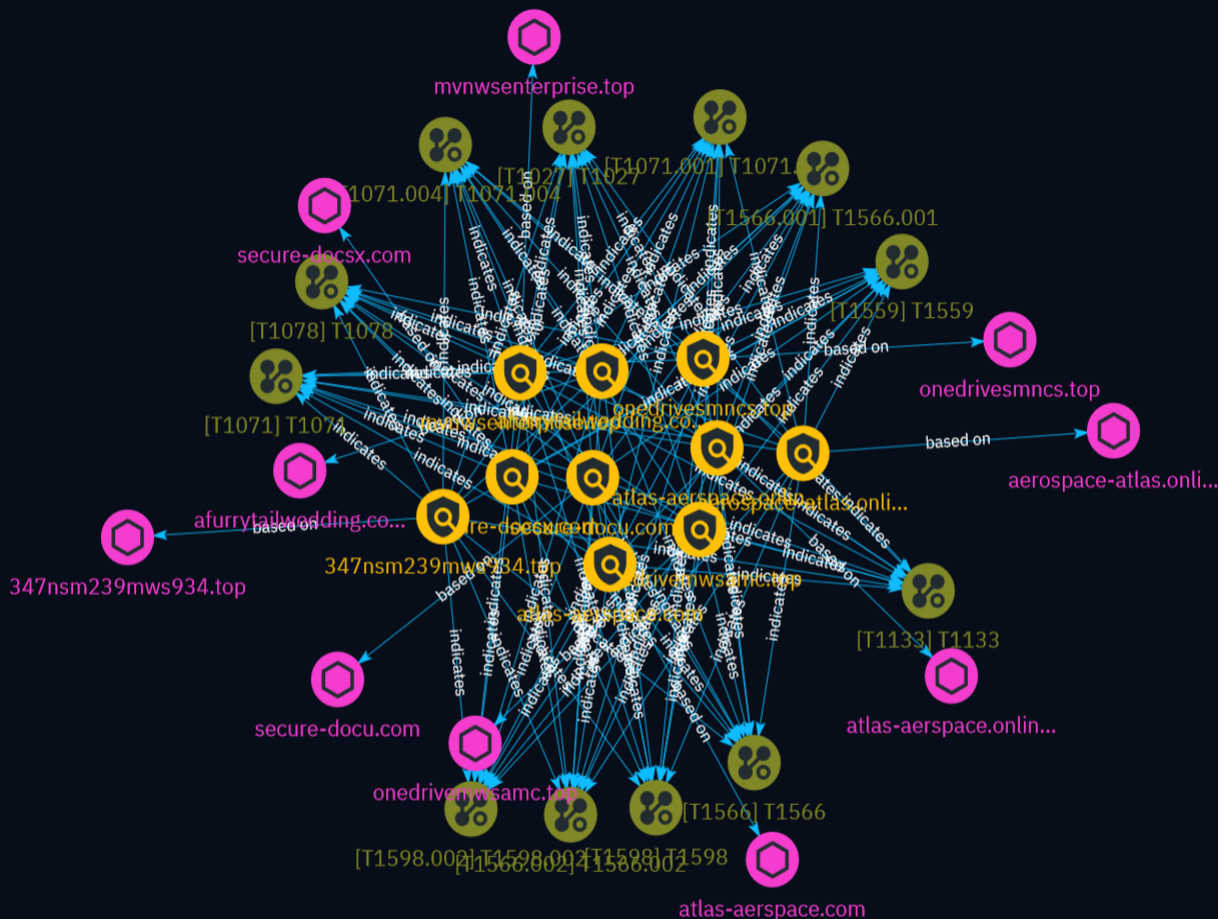


Table of contents

Overview

● Description	3
● Confidence	3
● Content	4

Entities

● Indicator	5
● Attack-Pattern	11

Observables

● Domain-Name	20
---------------	----

External References

● External References	21
-----------------------	----

Overview

Description

Cisco Talos Incident Response has observed threat actors using legitimate digital document publishing sites to host phishing documents and steal credentials. The sites' reputation, customization options, and transient nature create advantages for attackers trying to bypass defenses. Security teams should block these sites if possible, update phishing protections to detect them, and train users to identify and report suspicious documents from unfamiliar sources.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name

secure-docu.com

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '6 months ago', 'timestamp': 1694532075, 'iso': '2023-09-12T11:21:15-04:00'} - **IPQS: Domain:** secure-docu.com - **IPQS: IP Address:** 35.186.223.180

Pattern Type

stix

Pattern

[domain-name:value = 'secure-docu.com']

Name

secure-docsx.com

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '7

months ago', 'timestamp': 1693142934, 'iso': '2023-08-27T09:28:54-04:00'} - **IPQS: Domain:** secure-docsx.com - **IPQS: IP Address:** 35.186.223.180

Pattern Type

stix

Pattern

[domain-name:value = 'secure-docsx.com']

Name

onedrivesmncs.top

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1706257749, 'iso': '2024-01-26T03:29:09-05:00'} - **IPQS: Domain:** onedrivesmncs.top - **IPQS: IP Address:** 165.227.152.218

Pattern Type

stix

Pattern

[domain-name:value = 'onedrivesmncs.top']

Name

onedrivemwsamc.top

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1706304834, 'iso': '2024-01-26T16:33:54-05:00'} - **IPQS: Domain:** onedrivemwsamc.top - **IPQS: IP Address:** 165.227.152.218

Pattern Type

stix

Pattern

[domain-name:value = 'onedrivemwsamc.top']

Name

mvnwsenterprise.top

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1706009367, 'iso': '2024-01-23T06:29:27-05:00'} - **IPQS: Domain:** mvnwsenterprise.top - **IPQS: IP Address:** 165.227.152.218

Pattern Type

stix

Pattern

[domain-name:value = 'mvnwsenterprise.top']

Name

atlas-aerspace.online

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True -
Parking: False - **Spamming:** False - **Malware:** False - **Phishing:** False -
Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3
months ago', 'timestamp': 1702993340, 'iso': '2023-12-19T08:42:20-05:00'} - **IPQS: Domain:**
atlas-aerspace.online - **IPQS: IP Address:** 172.67.192.105

Pattern Type

stix

Pattern

[domain-name:value = 'atlas-aerspace.online']

Name

atlas-aerspace.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True -
Parking: False - **Spamming:** False - **Malware:** False - **Phishing:** False -
Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5
months ago', 'timestamp': 1698236070, 'iso': '2023-10-25T08:14:30-04:00'} - **IPQS: Domain:**
atlas-aerspace.com - **IPQS: IP Address:** 104.21.53.116

Pattern Type

stix

Pattern

[domain-name:value = 'atlas-aerspace.com']

Name

afurrytailwedding.com

Description

- **Unsafe:** False - **Server:** Apache - **Domain Rank:** 0 - **DNS Valid:** True -
 Parking: False - **Spamming:** False - **Malware:** False - **Phishing:** False -
 Suspicious: False - **Adult:** False - **Category:** Shopping - **Domain Age:**
 {'human': '5 years ago', 'timestamp': 1547342236, 'iso': '2019-01-12T20:17:16-05:00'} - **IPQS:
 Domain:** afurrytailwedding.com - **IPQS: IP Address:** 192.185.93.208

Pattern Type

stix

Pattern

[domain-name:value = 'afurrytailwedding.com']

Name

aerospace-atlas.online

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True -
 Parking: False - **Spamming:** False - **Malware:** False - **Phishing:** False -
 Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2
 months ago', 'timestamp': 1706101007, 'iso': '2024-01-24T07:56:47-05:00'} - **IPQS: Domain:**
 aerospace-atlas.online - **IPQS: IP Address:** 104.21.41.2

Pattern Type

stix

Pattern

[domain-name:value = 'aerospace-atlas.online']

Name

347nsm239mws934.top

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1706185084, 'iso': '2024-01-25T07:18:04-05:00'} - **IPQS: Domain:** 347nsm239mws934.top - **IPQS: IP Address:** 165.227.152.218

Pattern Type

stix

Pattern

[domain-name:value = '347nsm239mws934.top']

Attack-Pattern

Name

T1071.001

ID

T1071.001

Description

Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Protocols such as HTTP/S(Citation: CrowdStrike Putter Panda) and WebSocket(Citation: Brazking-Websockets) that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

Name

T1598

ID

T1598

Description

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from [Phishing](https://attack.mitre.org/techniques/T1566) in that the objective is gathering data from the victim rather than executing malicious code. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns. Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means.(Citation: ThreatPost Social Media Phishing)(Citation: TrendMicro Phishing)(Citation: PCMag FakeLogin)(Citation: Sophos Attachment)(Citation: GitHub Phishery) Victims may also receive phishing messages that direct them to call a phone number where the adversary attempts to collect confidential information.(Citation: Avertium callback phishing) Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages. Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Phishing for information may also involve evasive techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014)

Name

T1078

ID

T1078

Description

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised

credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

Name

T1559

ID

T1559

Description

Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution. IPC is typically used by processes to share data, communicate with each other, or synchronize execution. IPC is also commonly used to avoid situations such as deadlocks, which occurs when processes are stuck in a cyclic waiting pattern.

Adversaries may abuse IPC to execute arbitrary code or commands. IPC mechanisms may differ depending on OS, but typically exists in a form accessible through programming languages/libraries or native interfaces such as Windows [Dynamic Data Exchange] (<https://attack.mitre.org/techniques/T1559/002>) or [Component Object Model](<https://attack.mitre.org/techniques/T1559/001>). Linux environments support several different IPC mechanisms, two of which being sockets and pipes.(Citation: Linux IPC) Higher level execution mediums, such as those of [Command and Scripting Interpreter](<https://attack.mitre.org/techniques/T1059>)s, may also leverage underlying IPC mechanisms. Adversaries may also use [Remote Services](<https://attack.mitre.org/techniques/T1021>)

such as [Distributed Component Object Model](<https://attack.mitre.org/techniques/T1021/003>) to facilitate remote IPC execution.(Citation: Fireeye Hunting COM June 2019)

Name

T1598.002

ID

T1598.002

Description

Adversaries may send spearphishing messages with a malicious attachment to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](<https://attack.mitre.org/techniques/T1585>) or [Compromise Accounts](<https://attack.mitre.org/techniques/T1586>)) and/or sending multiple, seemingly urgent messages. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon the recipient populating information then returning the file.(Citation: Sophos Attachment)(Citation: GitHub Phishery) The text of the spearphishing email usually tries to give a plausible reason why the file should be filled-in, such as a request for information from a business associate. Adversaries may also use information from previous reconnaissance efforts (ex: [Search Open Websites/Domains](<https://attack.mitre.org/techniques/T1593>) or [Search Victim-Owned Websites](<https://attack.mitre.org/techniques/T1594>)) to craft persuasive and believable lures.

Name

T1027

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

T1566

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim

systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1071

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

T1566.001

ID

T1566.001

Description

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](<https://attack.mitre.org/techniques/T1204>) to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted source. There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

Name

T1566.002

ID

T1566.002

Description

Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source. All forms of

spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly. Additionally, adversaries may use seemingly benign links that abuse special characters to mimic legitimate websites (known as an "IDN homograph attack").(Citation: CISA IDN ST05-016) URLs may also be obfuscated by taking advantage of quirks in the URL schema, such as the acceptance of integer- or hexadecimal-based hostname formats and the automatic discarding of text before an "@" symbol: for example, `hxxp://google.com@1157586937`. (Citation: Mandiant URL Obfuscation 2023) Adversaries may also utilize links to perform consent phishing, typically with OAuth 2.0 request URLs that when accepted by the user provide permissions/access for malicious applications, allowing adversaries to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s.(Citation: Trend Micro Pawn Storm OAuth 2017) These stolen access tokens allow the adversary to perform various actions on behalf of the user via API calls. (Citation: Microsoft OAuth 2.0 Consent Phishing 2021)

Name

T1071.004

ID

T1071.004

Description

Adversaries may communicate using the Domain Name System (DNS) application layer protocol to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. The DNS protocol serves an administrative function in computer networking and thus may be very common in environments. DNS traffic may also be allowed even before network authentication is completed. DNS packets contain many fields and headers in which data can be concealed. Often known as DNS tunneling, adversaries may abuse DNS to communicate with systems

under their control within a victim network while also mimicking normal, expected traffic. (Citation: PAN DNS Tunneling)(Citation: Medium DnsTunneling)

Name

T1133

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management] (<https://attack.mitre.org/techniques/T1021/006>) and [VNC](<https://attack.mitre.org/techniques/T1021/005>) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](<https://attack.mitre.org/techniques/T1078>) to use the service is often a requirement, which could be obtained through credential phishing or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Domain-Name

Value

secure-docu.com

secure-docsx.com

onedrivesmncs.top

onedrivemwsamc.top

mvnwsenterprise.top

atlas-aerspace.online

347nsm239mws934.top

atlas-aerspace.com

afurrytailwedding.com

aerospace-atlas.online

External References

-
- <https://blog.talosintelligence.com/threat-actors-leveraging-document-publishing-sites/#:~:text=Examples%20of%20DDP%20sites%20include,being%20abused%20by%20threat%20actors>
-
- <https://otx.alienvault.com/pulse/65f32665c68696b8ffb45d81>