

To process and clean the raw results, the output was redirected into a text file and parsed using a combination of grep, cut, and sort commands in Kali Linux. This step extracted the domain names from the output file and presented them in a **sorted, unique list** for clarity and analysis (Figure 46). However, the initial list contained IP-style hostnames and PTR records. To refine the results, a regular expression with grep -vE was applied to remove irrelevant entries. This produced a concise and **actionable set of unique domains** associated with the same range, including domains such as **buyer27.buyerads.com, hecticate.com, li1011-145.members.linode.com, and sistema.hipertrade.com.br** (Figure 47).

This multi-step process demonstrates how **fierce, combined with command-line filtering techniques, can enhance domain intelligence efforts by uncovering related domains and shared infrastructure within a target's IP range.**

```
(root💀KALI) - [~]
# host+careers.umgc.edu
careers.umgc.edu is an alias for umuccareers.buyerads.com.
umuccareers.buyerads.com has address 45.33.65.132
```

Figure 44: Resolution of careers.umgc.edu alias to umuccareers.buyerads.com using host command.

Source: Output from Kali Linux terminal.

```
[root💀KALI] -[~] # fierce --range 45.33.65.128/27
Nearby:
{'45.33.65.129': 'hecticate.com.',
 '45.33.65.130': '45-33-65-130.ip.linodeusercontent.com.',
 '45.33.65.131': '45-33-65-131.ip.linodeusercontent.com.',
 '45.33.65.132': 'buyer27.buyerads.com.',
 '45.33.65.133': '45-33-65-133.ip.linodeusercontent.com.',
 '45.33.65.134': '45-33-65-134.ip.linodeusercontent.com.',
 '45.33.65.135': 'li1011-135.members.linode.com.',
 '45.33.65.136': '45-33-65-136.ip.linodeusercontent.com.',
 '45.33.65.137': '45-33-65-137.ip.linodeusercontent.com.',
 '45.33.65.138': 'sistema.hipertrade.com.br.',
 '45.33.65.139': '45-33-65-139.ip.linodeusercontent.com.',
 '45.33.65.141': '45-33-65-141.ip.linodeusercontent.com.',
 '45.33.65.142': '45-33-65-142.ip.linodeusercontent.com.',
 '45.33.65.143': '45-33-65-143.ip.linodeusercontent.com.',
 '45.33.65.144': '45-33-65-144.ip.linodeusercontent.com.',
 '45.33.65.145': 'li1011-145.members.linode.com.',
 '45.33.65.146': '45-33-65-146.ip.linodeusercontent.com.',
 '45.33.65.147': '45-33-65-147.ip.linodeusercontent.com.',
 '45.33.65.148': 'li1011-148.members.linode.com.',
 '45.33.65.149': '45-33-65-149.ip.linodeusercontent.com.',
 '45.33.65.150': '45-33-65-150.ip.linodeusercontent.com.',
 '45.33.65.151': '45-33-65-151.ip.linodeusercontent.com.',
 '45.33.65.152': 'li1011-152.members.linode.com.',
 '45.33.65.153': '45-33-65-153.ip.linodeusercontent.com.',
 '45.33.65.154': '45-33-65-154.ip.linodeusercontent.com.',
 '45.33.65.155': 'li1011-155.members.linode.com.',
 '45.33.65.157': '45-33-65-157.ip.linodeusercontent.com.',
 '45.33.65.158': 'li1011-158.members.linode.com.',
 '45.33.65.159': '45-33-65-159.ip.linodeusercontent.com.'}
```

Figure 45: Nearby domains discovered using the command `fierce --range 45.33.65.128/27`

`45.33.65.128/27.`

Source: Output from Kali Linux terminal.

```
[root💀KALI] -[~] # fierce --range 45.33.65.128/27 > output.txt.cat.com.
cat output.txt | grep -oP "[0-9.]+:\$*[^\"]+\" | cut -d\" -f4 | sort -u
45.33.65.130: 45-33-65-130.ip.linodeusercontent.com.
45-33-65-130.ip.linodeusercontent.com.45-33-65-131.ip.linodeusercontent.com.
45-33-65-131.ip.linodeusercontent.com.linode.com.
45-33-65-133.ip.linodeusercontent.com.linodecontent.com.
45-33-65-134.ip.linodeusercontent.com.linodecontent.com.
45-33-65-136.ip.linodeusercontent.com.linodecontent.com.
45-33-65-137.ip.linodeusercontent.com.linodecontent.com.
45-33-65-139.ip.linodeusercontent.com.linodecontent.com.
45-33-65-141.ip.linodeusercontent.com.linodecontent.com.
45-33-65-142.ip.linodeusercontent.com.linodecontent.com.
45-33-65-143.ip.linodeusercontent.com.linodecontent.com.
45-33-65-146.ip.linodeusercontent.com.linodecontent.com.
45-33-65-147.ip.linodeusercontent.com.linodecontent.com.
45-33-65-149.ip.linodeusercontent.com.linode.com.
45-33-65-150.ip.linodeusercontent.com.linodecontent.com.
45-33-65-151.ip.linodeusercontent.com.linode.com.
45-33-65-153.ip.linodeusercontent.com.linode.com.
45-33-65-154.ip.linodeusercontent.com.linode.com.
45-33-65-157.ip.linodeusercontent.com.linodecontent.com.
45-33-65-158.members.linode.com.
li1011-155.members.linode.com.
li1011-157.ip.linodeusercontent.com.
li1011-158.members.linode.com.
li1011-159.ip.linodeusercontent.com.

buyer27.buyerads.com.011-155.members.linode.com.
hecticate.com. 45-33-65-157.ip.linodeusercontent.com.
li1011-135.members.linode.com.members.linode.com.
li1011-145.members.linode.com.ip.linodeusercontent.com.)
li1011-148.members.linode.com.
li1011-152.members.linode.com.
li1011-155.members.linode.com do host 45.33.65.sip; done
li1011-158.members.linode.com.
sistema.hipertrade.com.br. nph not found: 3(NXDOMAIN)
```

Figure 46: Processed output redirected to file and filtered with grep, cut, and sort for unique domain extraction.

Source: Output from Kali Linux terminal.

```
(root㉿KALI)-[~] arp domain name pointer 45-33-65-130.ip.linodeusercontent.com,
# cat output.txt | grep -oP "[0-9.]+:\$*[^\n]+\n" | cut -d"\n" -f4 | grep -vE '^[\0-9\.-]+\.\ip\.' | sort -u
132.0.33.49.in-addr.arpa domain name pointer buyer27.buyerads.com.
buyer27.buyerads.com.
hecticate.com.
l11011-135.members.linode.com.in name pointer l11011-135.members.linode.com.
l11011-145.members.linode.com.in name pointer 45-33-65-136.ip.linodeusercontent.com.
l11011-148.members.linode.com.in name pointer 45-33-65-137.ip.linodeusercontent.com.
l11011-152.members.linode.com.in name pointer sistema.hipertrade.com.br.
l11011-155.members.linode.com.in name pointer 45-33-65-139.ip.linodeusercontent.com.
l11011-158.members.linode.com.. not found: 3(NXDOMAIN)
sistema.hipertrade.com.br.domain name pointer 45-33-65-141.ip.linodeusercontent.com.
```

Figure 47: Refined domain list using regular expression filtering with grep -vE to remove IP-style hostnames.

Source: Output from Kali Linux terminal.

As part of the threat intelligence analysis for the subdomain **phones.umgc.edu**, the first step involved using the host command to resolve the domain to its underlying infrastructure. The results showed that phones.umgc.edu is an alias (CNAME) for **s3-website-us-east-1.amazonaws.com**, which in turn resolved to multiple IP addresses within Amazon Web Services (AWS) infrastructure (Figure 48). This mapping indicates the subdomain is hosted on AWS's cloud platform, highlighting potential dependencies on third-party services.

After resolving the IP address, a proximity scan was performed to uncover nearby domains within the same network block. Using the **fierce** tool with the /27 subnet range, the command `fierce --range 52.217.8.160/27 > output.txt` was executed, followed by a post-processing pipeline with grep, cut, and sort to filter and extract meaningful domain

names. This process uncovered several nearby AWS-hosted domains, including **s3-1.amazonaws.com**, **s3-l-w.amazonaws.com**, **s3-external-1.amazonaws.com**, **s3-external-1-w.amazonaws.com**, **s3-fips-r-w.us-east-1.amazonaws.com**, **s3-us-east-1-r-w.amazonaws.com**, and **s3-website-us-east-1.amazonaws.com** (Figure 49).

These findings demonstrate how subdomain reconnaissance and proximity scanning can provide valuable insight into external infrastructure dependencies and potential attack surfaces for further investigation.

```
(root💀KALI)-[~]
# host phones.umgc.edu

phones.umgc.edu is an alias for s3-website-us-east-1.amazonaws.com.
s3-website-us-east-1.amazonaws.com is an alias for s3-website.us-east-1.amazonaws.com.
s3-website.us-east-1.amazonaws.com has address 3.5.12.56
s3-website.us-east-1.amazonaws.com has address 52.217.8.187
s3-website.us-east-1.amazonaws.com has address 52.216.221.141
s3-website.us-east-1.amazonaws.com has address 54.231.128.125
s3-website.us-east-1.amazonaws.com has address 52.217.71.171
s3-website.us-east-1.amazonaws.com has address 52.217.162.117
s3-website.us-east-1.amazonaws.com has address 52.217.116.173
s3-website.us-east-1.amazonaws.com has address 16.15.216.176
```

Figure 48: Output of the host phones.umgc.edu command showing alias resolution to AWS S3 infrastructure.

Source: Executed in Kali Linux terminal.

```
(root💀KALI)-[~]
# fierce --range 52.217.8.160/27 > output.txt

(running)
# cat output.txt | grep -oP "'[0-9.]+:\s*[^:]+'" | cut -d":" -f4 | grep -vE '^([0-9.-]+\.\.ip\.)' | sort -u

s3-1.amazonaws.com.
s3-1-w.amazonaws.com.
s3-external-1.amazonaws.com.
s3-external-1-w.amazonaws.com.
s3-fips-r-w.us-east-1.amazonaws.com.
s3-us-east-1-r-w.amazonaws.com.
s3-website-us-east-1.amazonaws.com.
```

Figure 49: Output of `fierce --range 52.217.8.160/27` with filtering to identify nearby AWS-hosted domains.

Source: Executed in Kali Linux terminal.

The **Start of Authority (SOA)** record for the domain **umgc.edu** was identified during DNS reconnaissance. The SOA record specifies the authoritative nameserver responsible for the domain and provides the IPv4 address associated with it. The analysis revealed that the SOA for umgc.edu is managed by **ns-1246.awsdns-27.org**, with the corresponding IPv4 address **205.251.196.222**.

To obtain this information, the **fierce** tool was executed with the command `fierce --domain umgc.edu`, which successfully enumerated the SOA record and its associated details. This finding highlights the authoritative infrastructure behind the domain, offering insight into the hosting and DNS management environment.

```

root@kali:~# fierce --domain umgc.edu
phones.umgc.edu is an alias for s3-website-us-east-1.amazonaws.com.
NS: ns-758.awsdns-30.net.ns-1246.awsdns-27.org.ns-1863.awsdns-40.co.uk.ns-412.awsdns-51.com.
SOA:ns-1246.awsdns-27.org.(205.251.196.222) 3.5.12.50
Zone failure: no nameservers have address 52.217.8.187

```

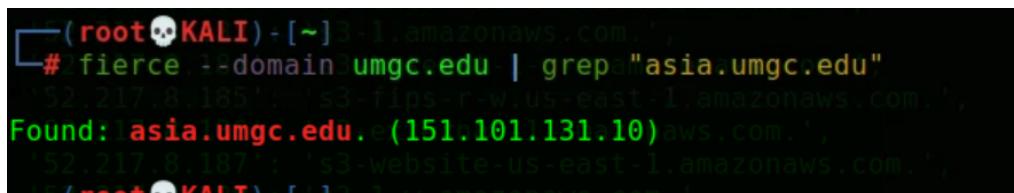
Figure 50: Output of the `fierce --domain umgc.edu` command showing SOA record resolution.

Source: Executed in Kali Linux terminal.

The IPv4 address associated with the subdomain **asia.umgc.edu** was identified as **151.101.131.10**. This resolution was achieved using the **fierce** tool to enumerate subdomains of umgc.edu, with the output filtered through the `grep` command to isolate

the Asia-specific entry. By targeting the results in this manner, the enumeration process effectively revealed the resolved IP address directly tied to asia.umgc.edu.

This finding provides insight into the global infrastructure supporting umgc.edu, as the Asia subdomain reflects distributed hosting and potential regional services. Such intelligence is valuable for assessing attack surfaces across geographic deployments of the organization's domain.



```
(root💀KALI)㉿3-1.amazonaws.com: ~
# fierce --domain umgc.edu | grep "asia.umgc.edu"
[52.217.8.185]: 's3-fips-r-w.us-east-1.amazonaws.com.',
Found: 1 asia.umgc.edu.e(151.101.131.10)aws.com.,
[52.217.8.187]: 's3-website-us-east-1.amazonaws.com.',
[52.217.8.188]: 's3-website-us-east-1.amazonaws.com.'
```

Figure 51: Output of `fierce --domain umgc.edu` with `grep` filter showing `asia.umgc.edu` resolution

Source: Executed in Kali Linux terminal.

OSINT

Open Source Intelligence (OSINT) tools enable cybersecurity analysts to gather and analyze publicly accessible information such as DNS data, domain ownership, technology stacks, and IP footprints to uncover potential threats, map an organization's digital presence, and enrich intelligence without direct network intrusion (Northland Controls, n.d.). By leveraging platforms like osint.sh alongside Kali based tools, analysts gain deeper visibility into adversary infrastructure, accelerating early threat detection and proactive threat hunting efforts. These capabilities make OSINT indispensable in building timely, cost-effective, and context rich threat intelligence.

The DNS lookup tool on **osint.sh** was used to query the authoritative name servers (NS) for the domain **umgc.edu**. The results returned four NS records, which aligned with those discovered earlier using Kali Linux tools. The identified name servers are:

- **ns-1246.awsdns-27.org**
- **ns-412.awsdns-51.com**
- **ns-1863.awsdns-40.co.uk**
- **ns-758.awsdns-30.net**

This consistency between OSINT-based lookup and active Kali-based enumeration validates the accuracy of the domain's DNS infrastructure mapping. Identifying these authoritative name servers is critical in threat intelligence, as they play a vital role in directing traffic for the domain and can reveal potential misconfigurations or dependencies on third-party DNS hosting.

DNS LOOKUP

Provides a report on DNS records for a specified domain or hostname

CHECK NOW

No	Type	Records	TTL
1	NS	ns-1246.awsdns-27.org.	21600
2	NS	ns-412.awsdns-51.com.	21600
3	NS	ns-1863.awsdns-40.co.uk.	21600
4	NS	ns-758.awsdns-30.net.	21600

Figure 52: DNS lookup results from osint.sh showing authoritative NS records for umgc.edu

Source: Output from osint.sh DNS Lookup tool.

The DNS lookup tool on **osint.sh** identified the IPv4 addresses associated with the **A records** for the domain **umgc.edu**. These results are consistent with those obtained using the *dnsrecon* tool in Kali Linux, thereby validating the enumeration findings across different platforms. The four IPv4 addresses resolved for umgc.edu are:

- **151.101.131.10**
- **151.101.3.10**
- **151.101.195.10**
- **151.101.67.10**

These A records represent the domain's primary endpoints and are critical in mapping the infrastructure that supports its web services. From a cybersecurity perspective, confirming these IPs provides insight into the domain's hosting environment and can assist in identifying potential exposure points during reconnaissance.

No	Type	Records	TTL
1	A	151.101.131.10 umgc.edu. Fastly, Inc., United States	60
2	A	151.101.3.10 umgc.edu. Fastly, Inc., United States	60
3	A	151.101.195.10 umgc.edu. Fastly, Inc., United States	60
4	A	151.101.67.10 umgc.edu. Fastly, Inc., United States	60

Figure 53: DNS lookup results from osint.sh showing A records for umgc.edu

Source: Output from the DNS Lookup tool on osint.sh for the domain umgc.edu.

Using the **DNS Lookup tool** on the **osint.sh** platform, the analysis revealed only one **MX (Mail Exchange) record** associated with the domain **umgc.edu**. The identified record is:

- **0 umgc-edu.mail.protection.outlook.com**

This indicates that inbound email traffic for the umgc.edu domain is routed through Microsoft Outlook's mail protection service, a common setup for organizations leveraging Microsoft 365 for secure email handling. Identifying MX records is significant in cybersecurity assessments, as it helps determine potential exposure points for phishing, spoofing, or misconfigured mail servers.

No	Type	Records	TTL
1	MX	0 umgc-edu.mail.protection.outlook.com.	300

Figure 54: DNS lookup results from osint.sh showing MX record for umgc.edu

Source: Output from the DNS Lookup tool on osint.sh for the domain umgc.edu.

From the **osint.sh** platform, a **TXT record** was identified for the domain **umgc.edu**, which contains a **DocuSign verification ID**. TXT records are often used for domain ownership verification, email security configurations (SPF, DKIM, DMARC), and third-party service integrations. In this case, the discovered record reveals that the organization is using DocuSign for trusted electronic document workflows.

The specific TXT record discovered was:

- **docusign=b8294918-7886-4f86-93a1-c5d6f1a30d4a**

This finding highlights how external integrations, such as DocuSign, can leave recognizable footprints in public DNS records, which may be leveraged during reconnaissance to identify technologies in use within an organization.

4	TXT	docusign=b8294918-7886-4f86-93a1-c5d6f1a30d4a
---	-----	---

Figure 55: DNS lookup results from osint.sh showing TXT record for umgc.edu

Source: Output from the DNS Lookup tool on osint.sh website.

To validate the finding, the command **dnsrecon -d umgc.edu** was executed in Kali Linux. The output confirmed the presence of the **same DocuSign TXT record** (docusign=b8294918-7886-4f86-93a1-c5d6f1a30d4a), verifying consistency with the earlier osint.sh results.

```
(root💀KALI)-[~]
# grep "TXT" dnsrecon_output.txt

[*]      TXT umgc.edu v=spf1 ip4:40.92.0.0/15 ip4:40.107.0.0/16 ip4:52.100.0.0/15 ip4:52.102.0.0/16 ip4:52.103.0.0/16 ip4:8.21.240.0/20 ip4:13.58.57.211 ip4:13.58.58.6 ip4:13.58.82.59 ip4:13.58.86.183 ip4:13.58.208.255.239 ip4:34.209.181.84 ip4:35.161.82.137 ip4:37.98.232.0/22 ip4:50.31.32.0/19 ip4:52.1.108.153 ip4:52.1.109.153
[*]      TXT umgc.edu facebook-domain-verification=9tsadilriqe6b7rbmboutrt3gey7m5d
[*]      TXT umgc.edu jamf-site-verification=0ZsifkLDG2NdErLYiP-PkQ
[*]      TXT umgc.edu 8bsrjc25l6z2c1tn4hs9wmt5zrlift9dk
[*]      TXT umgc.edu onetrust-domain-verification=3f6990995e754b359f4eb2704423597f
[*]      TXT umgc.edu google-site-verification=34CNPwhiho_jbeHZ_fMSNGcmJ6VTNC0hRp2nwt22Re0
[*]      TXT umgc.edu google-site-verification=i_kpE2_102REl0m43WeVICAV-8oMKN7nCMrpW2l_bqE
[*]      TXT umgc.edu google-site-verification=hTH7q23mqMwr3vaDuFppjGurn64bbB_q2qUjq6M13HWI
[*]      TXT umgc.edu docusign=b8294918-7886-4f86-93a1-c5d6f1a30d4a
[*]      TXT umgc.edu apple-domain-verification=8s4Ct8Vrn88hRtw9
[*]      TXT umgc.edu canva-site-verification=-jahID3iBokuB0JncEcsHg
[*]      TXT umgc.edu airtable-verification=aff2c684657278d3ef76a37b79f7dae0
```

Figure 56: Dnsrecon output showing DocuSign TXT record for umgc.edu.

Source: Output from **dnsrecon -d umgc.edu** in Kali Linux.

The **Time-To-Live (TTL)** values for the *umgc.edu* domain records vary by record type, reflecting their intended stability and update frequency:

- **NS (Name Server) records:** 21,600 seconds – A high TTL ensures stability since authoritative name servers rarely change. Longer caching reduces DNS query load and improves overall resolution efficiency.
- **A (Address) records:** 60 seconds – A short TTL allows rapid IP switching, particularly useful when records are managed by CDNs or load balancers such as Fastly, enabling quick adaptation to traffic changes.
- **TXT (Text) records:** 300 seconds – A moderate TTL provides flexibility to update records like SPF, DKIM, or domain verification values while still offering reasonable caching.

This variation in TTL values provides a balance between performance, reliability, and agility, ensuring DNS responses remain both efficient and adaptable to operational requirements (Cloudflare, n.d.; ICANN, n.d.).

3	NS	ns-1863.awsdns-40.co.uk.	21600
4	NS	ns-758.awsdns-30.net.	21600
<hr/>			
No	Type	Records	TTL
1	A	151.101.131.10 umgc.edu. Fastly, Inc., United States	60
2	A	151.101.3.10 umgc.edu. Fastly, Inc., United States	60
3	A	151.101.195.10 umgc.edu. Fastly, Inc., United States	60
4	A	151.101.67.10 umgc.edu. Fastly, Inc., United States	60
<hr/>			
No	Type	Records	TTL
1	MX	0 umgc.edu.mail.protection.outlook.com.	300
<hr/>			
No	Type	Records	TTL
1	TXT	google-site-verification=I_kpE2_1O2RElOm43WeVicAV-8oMkN7nCMrpW2I_bqE	300
2	TXT	airtable-verification=af2c684657278d3ef76a37b79f7dae0	300
3	TXT	jamf-site-verification=0Zs1RkIG2NnfLYIP-PxQ	300
4	TXT	docusign=b8294918-7886-4fb6-93a1-c5d6f1a30d4a	300

Figure 57: DNS Lookup results for umgc.edu showing TTL values

Source: Output from the DNS Lookup tool on the osint.sh website.

The server-side language discovered for **learn.umgc.edu** is **Java**.

The client-side language discovered is **JavaScript**.

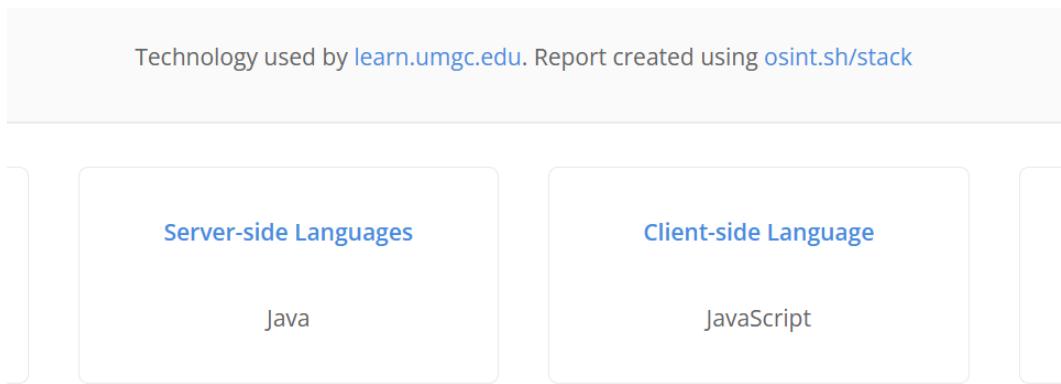


Figure 58: Technology stack identified for *learn.umgc.edu*, showing Java as the server-side language and JavaScript as the client-side language.

Source: Output from the Technology Lookup tool on the osint.sh website.

A total of **92 subdomains** were discovered for the domain umgc.edu using the Subdomain Finder tool on osint.sh.

Total results for **umgc.edu** = 92 subdomain. Scanned on 29 Jul 2025 03:40:56 AM. Scan ID 688842b400603

No	Subdomain	IP	Provider
1	ropsi.umgc.edu	54.85.95.118	Amazon Technologies Inc. Ashburn, United States
2	kai-opsvcse-01.europe.umgc.edu	109.73.132.53	k.net.de

Figure 59: Discovery of 92 subdomains for the *umgc.edu* domain using the Subdomain Finder tool on osint.sh

Source: Output from the Subdomain Finder tool on the osint.sh website.

Identifying the hosting provider for subdomains such as **asia.umgc.edu** is a critical part of threat intelligence and risk assessment. In this case, the subdomain is hosted by **Fastly, Inc., located in San Francisco, United States** (Figure 60). Knowing the provider helps analysts understand the security posture, geographic distribution, and potential third-party dependencies of an organization's infrastructure. It also highlights reliance on cloud/CDN providers, which may impact availability, compliance, and vulnerability management.

22	asia.umgc.edu	151.101.67.10	Fastly, Inc. San Francisco, United States
----	---------------	---------------	--

Figure 60: Provider details for the subdomain *asia.umgc.edu* showing hosting by *Fastly, Inc., San Francisco, United States*.

Source: Output from the Subdomain Finder tool on the osint.sh website.

IP GEO

The IP GEO Location Lookup tool was used to determine the approximate geographic locations of selected **umgc.edu** subdomains. This method helps identify the physical hosting regions of online infrastructure, which is valuable for understanding geographic distribution and potential compliance or risk considerations.

For the three subdomains analyzed, the following latitude and longitude values were identified:

- **europe.umgc.edu** – Latitude: **37.77712**, Longitude: **122.41964**
- **careers.umgc.edu** – Latitude: **40.80849**, Longitude: **74.46444**

- **content.umgc.edu** – Latitude: **39.05232**, Longitude: **77.48270**

These results highlight that the subdomains are hosted across different geographic regions, underscoring the distributed nature of the university's digital presence.

IP GEO Mapping Results:

To further validate the IP GEO lookup results, the identified latitude and longitude values were mapped using **Google Maps**. This helped pinpoint the physical locations associated with the umgc.edu subdomains: **europe.umgc.edu**, **careers.umgc.edu**, and **content.umgc.edu**.

- **europe.umgc.edu** mapped to **San Francisco, California**.
- **careers.umgc.edu** mapped to **Hanover, New Jersey**, with **Morristown** as the closest visible city.
- **content.umgc.edu** mapped to **Ashburn, Virginia**, a well-known hub for data centers.



Figure 61: Google Maps location result for **europe.umgc.edu** showing **San Francisco, CA**.

Source: Screenshot taken from Google Maps on July 29, 2025.

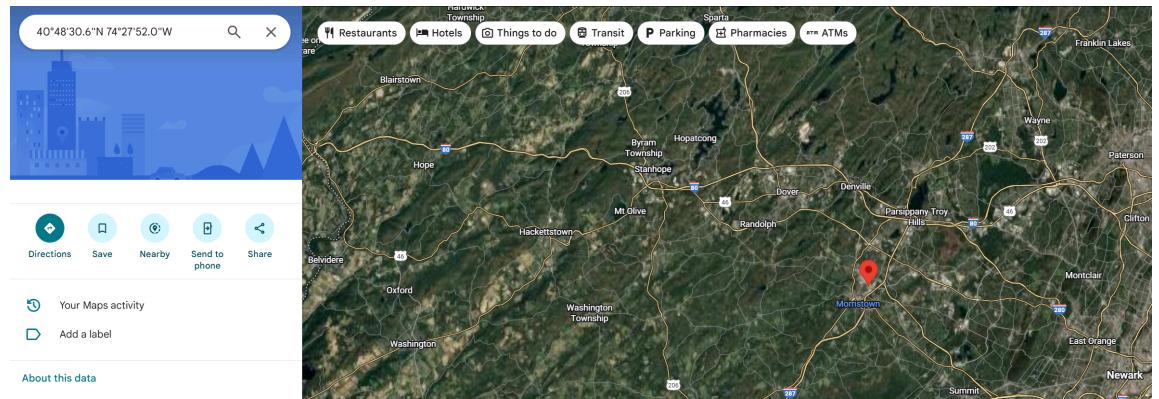


Figure 62: Google Maps location result for careers.umgc.edu showing Hanover, NJ (near Morristown).

Source: Screenshot taken from Google Maps on July 29, 2025.

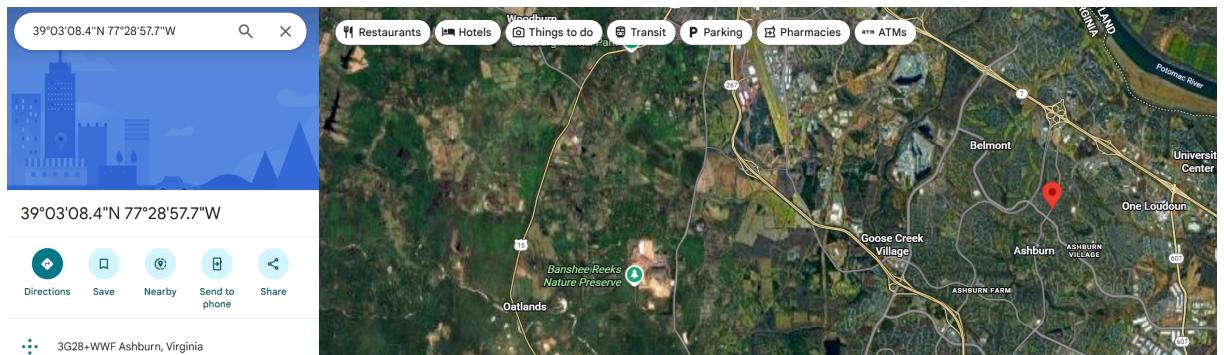


Figure 63: Google Maps location result for content.umgc.edu showing Ashburn, VA.

Source: Screenshot taken from Google Maps on July 29, 2025.

VirusTotal

VirusTotal in Threat Intelligence:

VirusTotal is a cloud-based threat intelligence platform that allows cybersecurity analysts to scan and analyze suspicious files, IP addresses, domains, and URLs using multiple antivirus engines and reputation services. It provides valuable insights into potential threats by aggregating data from over 70 security vendors, making it a critical resource for malware detection, indicator of compromise (IOC) identification, and incident response. Its ability to correlate file behavior and detect malicious artifacts supports proactive threat hunting and enhances situational awareness in security operations (VirusTotal, n.d.).

The IP address 206.123.128.45 was investigated using both **Cisco Talos** and **VirusTotal** threat intelligence platforms to assess its reputation and potential malicious activity.

Cisco Talos identified the IP as being involved in **email-based malware distribution**, as shown in the geographic visualization (Screenshot 1). The map highlights the distribution of email threats, with the analyzed IP associated with a volume of **7.5 malware emails** within the last 24 hours, suggesting active participation in a spam or phishing campaign.

VirusTotal confirmed this threat intelligence. Three out of ninety-four security vendors flagged the IP address as **malicious**, with tags including "MalwareURL" and "Suspicious" from trusted sources like Abusix and SOCRadar (Screenshot 2). This supports Talos' categorization of the IP as a security threat.

Further, the **Relations tab** in VirusTotal (Screenshot 3) revealed that this IP address is referenced in multiple **malicious email files** such as Temp[208].eml,

Temp[131].eml, and Quotation Air_Sea #Electronics.eml. These emails were scanned on July 29, 2025, and showed detection rates ranging from **6/63 to 33/63**, indicating widespread detection by antivirus engines. This evidence strongly associates the IP with malware-laden spam campaigns rather than legitimate use.

While the IP is not currently linked to an active malicious URL, its inclusion in numerous malicious email attachments and its detection by multiple security engines classify it as a threat source and a potential Command-and-Control (C2) or distribution node.

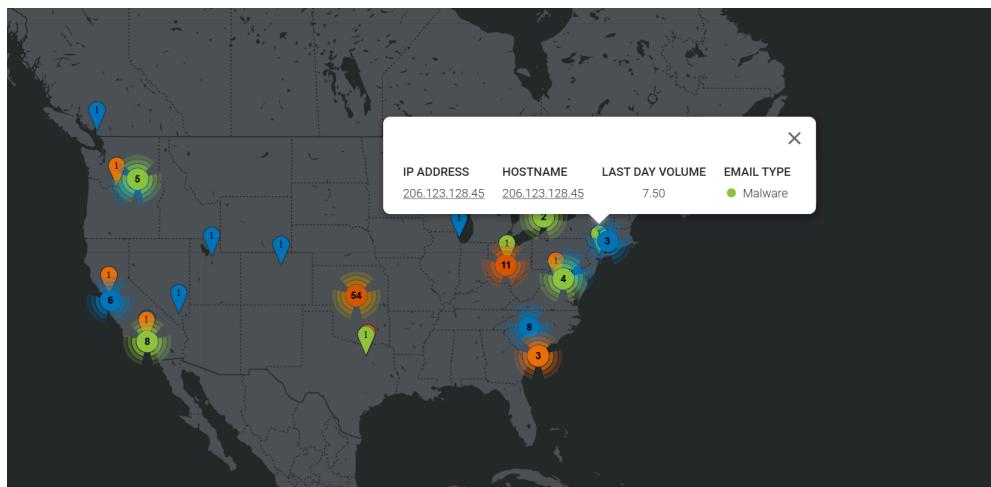


Figure 64: Cisco Talos Intelligence Map displaying malware email activity for IP address 206.123.128.45.

Source: Cisco Talos Intelligence – <https://talosintelligence.com>

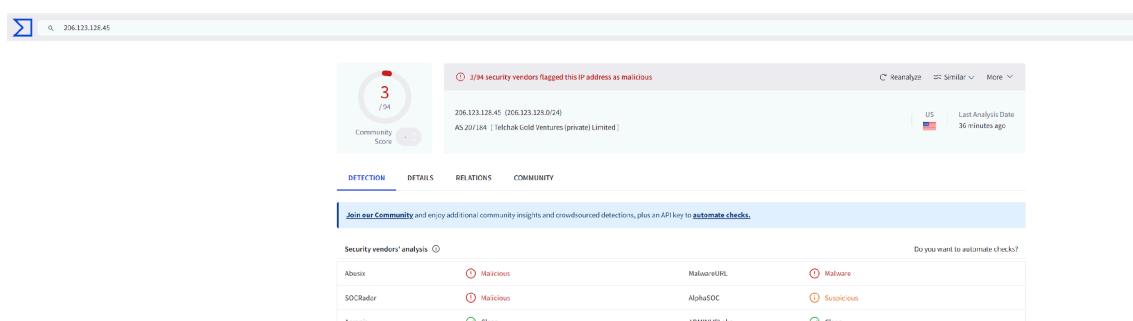


Figure 65: VirusTotal IP reputation analysis showing 3/94 security vendors flagging IP 206.123.128.45 as malicious.

Source: VirusTotal – <https://www.virustotal.com>

Scanned	Detections	Type	Name
2025-07-29	28 / 63	Email	banned-20250727T095541-01594-15
2025-07-29	13 / 63	Email	Temp[208].eml
2025-07-29	12 / 63	Email	Temp[207].eml
2025-07-29	26 / 63	Email	Quotation Air _ Sea (20_40ft Dry) #Electronics.eml
2025-07-29	13 / 63	Email	Temp[131].eml
2025-07-29	6 / 63	Email	Temp[130].eml
2025-07-29	25 / 63	Email	Temp[120].eml
2025-07-29	25 / 63	Email	Temp[122].eml
2025-07-29	26 / 63	Email	Temp[121].eml
2025-07-25	33 / 63	Email	banned-20250724T192955-26074-17

Figure 66: VirusTotal Relations tab presenting email samples linked to IP 206.123.128.45 along with detection counts.

Source: VirusTotal – <https://www.virustotal.com>

A harmless text file named *virustotal file.txt* was selected for testing, containing no sensitive data. The File Hash Online Calculator was used to generate its SHA-256 hash value: **db4067cec62c58bf8b2f8982071e77c082da9e00924bf3631f3b024fa54e7d7e** (Figure 67).

The generated hash was then submitted to VirusTotal for threat intelligence analysis. The results (Figure 68) confirmed that none of the 59 security vendors flagged

the file as malicious. This outcome was expected since the file was a plain text test file with no executable code or harmful content.

File Hash Online Calculator^{WASM}

- Calculates MD5, SHA1, SHA2 (SHA256), and SHA512 hashes all at once
- The browser performs all calculations without uploading data to the server
- Supports unlimited files of any size

Drop files here or click to select

and hash them all

Choose Files: virustotal file.txt

virustotal file.txt - 11 bytes

MD5: 39d11ab1c3c6c9eab3f5b3675f438db#

SHA1: 22c219648f00c61e5b3b1bd81ffa8e7767e2e3c5

SHA256: db4067cec62c58bf8b2f8982071e77c082da9e00924bf3631f3b024fa54e7d7e

SHA512: 1ca107777d9d999bdd8099875438919b5dca244104e393685f7d05f4feb5f181f1878e1178daf1a8c97c5b290222609c9515dd096344b625b37d7a8910076ed2

Figure 67: File hash generation using the File Hash Online Calculator.

Source: Output from File Hash Online Calculator.

The screenshot shows the VirusTotal analysis interface. At the top, there's a search bar with the hash value: db4067cec62c58bf8b2f8982071e77c082da9e00924bf3631f3b024fa54e7d7e. Below the search bar, it says "No security vendors flagged this file as malicious". On the right, there are buttons for "Reanalyze", "Similar", and "More". The file details are listed: Size 11 B, Last Analysis Date 7 years ago, and a TXT file type icon. Below this, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. The DETECTION tab is selected, showing a table of security vendor analysis results. The table has two columns: Vendor and Result. The results are all "Undetected" with green checkmarks. The vendors listed are Ad-Aware, AlinLab-V3, AntiAVL, Avast, AVG, AvAware, BitDefender, AvgLab, AIYES, Arcabit, Avast-Mobile, Avira (no cloud), Baidu, and EKav Pro. A note at the bottom of the table says "Do you want to automate checks?".

Vendor	Result
Ad-Aware	Undetected
AlinLab-V3	Undetected
AntiAVL	Undetected
Avast	Undetected
AVG	Undetected
AvAware	Undetected
BitDefender	Undetected
AvgLab	Undetected
AIYES	Undetected
Arcabit	Undetected
Avast-Mobile	Undetected
Avira (no cloud)	Undetected
Baidu	Undetected
EKav Pro	Undetected

Figure 68: VirusTotal scan results showing no detections for the submitted SHA-256

hash.

Source: Output from VirusTotal – <https://www.virustotal.com>

To perform domain analysis, three domains were selected: **google.com**, **microsoft.com**, and **umgc.edu**, and submitted each to VirusTotal for inspection. VirusTotal aggregates intelligence from multiple vendors and provides reputation scores, categories, DNS data, and popularity metrics for domains (VirusTotal, n.d.).

Google.com

The domain google.com was flagged clean by all security vendors. It is categorized under search engines & portals, telephony, and top-1K websites. The popularity rankings from sources like Cloudflare Radar, Cisco Umbrella, and Majestic all ranked Google as the top domain , indicating its massive global presence and trustworthiness.

Microsoft.com

Similar to Google, microsoft.com was also reported clean across all vendor engines. It was categorized under information technology, moderate forums, and collaboration-office. While still highly ranked, Microsoft had a Cloudflare Radar position of 200 and a majestic rank of 7. This suggests strong credibility, but slightly lower global DNS visibility compared to Google.

UMGC.edu

The domain umgc.edu was also found to be clean. It falls under the educational institutions category. However, its popularity rankings were significantly lower, Majestic ranked it at 15163, and Cisco Umbrella placed it at 164191. These rankings align with the domain's nature as a university-specific website rather than a globally used service.

Comparison and Contrast Based on Categories and Popularity Scores

The three domains analyzed were **google.com**, **microsoft.com**, and **umgc.edu**, which demonstrated distinct categorizations and popularity rankings reflective of their organizational functions and online reach.

Google.com is categorized under “telephony,” “search engines & portals,” and “top 1K” by multiple vendors including alphaMountain.ai and Sophos, which aligns with its core functionality as a global search engine. It ranks **no 1 across all five popularity sources** (Cloudflare Radar, Cisco Umbrella, Majestic, Statvoo, and Alexa), indicating exceptionally high visibility and web traffic.

Microsoft.com is labeled under “information technology,” “moderated forums,” and “collaboration - office.” While these categories are appropriate, it’s notable that **Cloudflare ranks it at position 200**, and the other sources range from position 2 (Cisco Umbrella) to 24 (Alexa/Statvoo), reflecting moderately high but not universal dominance like Google.

In contrast, **umgc.edu** is consistently categorized as “education” or “educational institutions” by all vendors, which is accurate for an academic site. However, its popularity scores are lower, ranking **#100,000 on Cloudflare**, and beyond **#15,000 on other trackers**. This comparison shows how category tagging helps identify a domain’s purpose and use case, while popularity scores offer a quantifiable view of its reputation, accessibility, and visibility in the global web ecosystem.

Domain	Categories (Selected Vendors)	Popularity Rankings (Top Positions)
google.com	<ul style="list-style-type: none"> - Telephony (alphaMountain.ai) - Search Engines & Portals (Xcitium, Sophos) - Misc 	<ul style="list-style-type: none"> - Cloudflare Radar: 1 - Cisco Umbrella: 1 - Majestic: 1 - Alexa: 1 - Statvoo: 1
microsoft.com	<ul style="list-style-type: none"> - Business/Economy, Information Technology (alphaMountain.ai) - Collaboration - Office - Moderated Forums (Xcitium) - Misc 	<ul style="list-style-type: none"> - Cloudflare Radar: 200 - Cisco Umbrella: 2 - Majestic: 7 - Alexa: 24 - Statvoo: 24
umgc.edu	<ul style="list-style-type: none"> - Education (BitDefender, 	<ul style="list-style-type: none"> - Cloudflare Radar: 100000

	Sophos, Forcepoint ThreatSeeker)	- Cisco Umbrella: 164191 - Majestic: 15163 - Alexa: 19827 - Statvoo: 19227
--	-------------------------------------	--

In **VirusTotal**, the *Relations* tab for the domain **umgc.edu** shows a total of **269 subdomains**. These include various internal services, web portals, test environments, and mail systems associated with the university. VirusTotal compiles this data from numerous security vendors and historical DNS scans, resulting in a comprehensive list of known subdomains over time.

In comparison, when analyzing **umgc.edu** using the **Maltego Community Edition**, I used the transform:

► [DNS from Domain]

This transform has returned **53 subdomains**, which is significantly fewer than Virus Total's 269.

The disparity occurs because Maltego's free edition relies on real time and publicly visible DNS records. It does not have access to Virus Total's extensive database of passive DNS records and third-party data sources, which explains the limited results.

In summary:

- **VirusTotal** listed: **269 subdomains**.
- **Maltego (DNS from Domain transform)** listed: **53 subdomains**.

This demonstrates that while Maltego is excellent for visual analysis and entity mapping, platforms like VirusTotal provide more comprehensive subdomain intelligence for a domain.

Subdomains (269) ◎					
ai-form.umgc.edu	0 / 94	13.107.253.38			
sra.umgc.edu	0 / 94	13.107.246.38			
apply-int.umgc.edu	0 / 94	3.146.43.227	3.146.43.228	3.146.43.229	
apply-uat.umgc.edu	0 / 94	3.146.43.227	3.146.43.229	3.146.43.228	
amplify.umgc.edu	0 / 94	13.107.253.38			
studentportal-prd.umgc.edu	0 / 94	13.107.246.38			
hackthebox.umgc.edu	1 / 94	13.107.246.38	13.107.253.38		
linkedinelearning.umgc.edu	0 / 94	13.107.246.38			
impact-dev.umgc.edu	0 / 94	151.101.67.10	151.101.195.10	151.101.131.10	...
portal-qat.umgc.edu	0 / 94	13.107.253.38			
portal-dev.umgc.edu	0 / 94	13.107.253.38			
skill-finder.umgc.edu	0 / 94	34.111.179.208			
leoweb-sitemaps.umgc.edu	0 / 94	13.107.246.38			
studentportal-stg.umgc.edu	0 / 94	13.107.246.38			
sfstage.umgc.edu	0 / 94	13.107.246.38			
studentportal-qat.umgc.edu	0 / 94	13.107.253.38	13.107.246.38		
volunteer.umgc.edu	0 / 94	13.107.246.38			
svgateway-nonprod.umgc.edu	0 / 94	107.22.7.215	34.224.190.159	34.233.96.86	
transcend.umgc.edu	0 / 94	13.107.246.38			
facebook-api.umgc.edu	0 / 94	52.205.6.168	52.1.241.113	54.221.191.24	...
ltidev-widgets.umgc.edu	0 / 94	54.175.47.51	52.71.62.235	54.167.131.108	...
phones.umgc.edu	0 / 94	52.217.171.109	52.216.213.37	52.216.251.35	...
attask.umgc.edu	0 / 94	52.217.42.147	52.217.84.211	52.217.228.61	...
vaultqa.umgc.edu	0 / 94	10.190.40.55			
salesforcetraining.umgc.edu	0 / 94	13.107.246.38			
orientation-stage.umgc.edu	0 / 94	151.101.67.10	151.101.131.10	151.101.3.10	...
stories.umgc.edu	0 / 94	151.101.3.10	151.101.67.10	151.101.131.10	...
aem-stg.umgc.edu	0 / 94	151.101.3.10	151.101.195.10	151.101.67.10	...
studentportal-dev.umgc.edu	0 / 94	13.107.246.38			
leoweb-prd.umgc.edu	0 / 94	13.107.246.38			
medialavet.umgc.edu	0 / 94	13.107.246.38			
preview.umgc.edu	0 / 94	52.183.213.3			

Figure 69: Subdomains of umgc.edu discovered using Virus Total Domain Relations.

Source: [VirusTotal – Domain Relations](#)

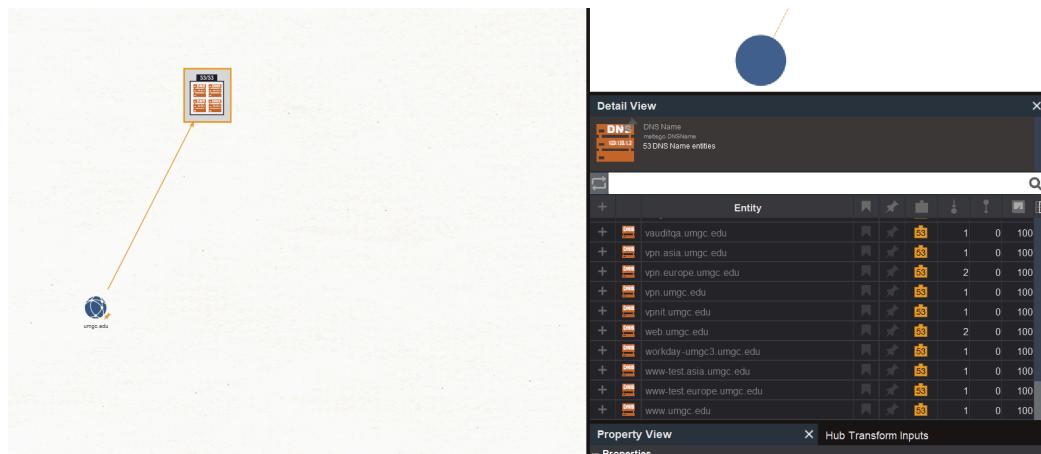


Figure 70: Visualization of umgc.edu subdomains generated in Maltego.

Source: Maltego Community Edition

Google Dorks exercise

Google Dorking, also known as Google hacking, refers to the use of advanced search operators to uncover sensitive information indexed by search engines but not intended for public access. In the context of threat intelligence, it is a powerful technique for open-source intelligence (OSINT) gathering, allowing security analysts to discover exposed files, misconfigured servers, login portals, or even vulnerable systems. Ethical hackers and security researchers use Google Dorks to assess an organization's online footprint and identify weaknesses that adversaries could exploit (Scarfone & Mell, 2007).

Tangier Sound is a body of water located in the **Chesapeake Bay**, between **Maryland** and **Virginia** in the **United States**. The region is bordered by Deal Island, Crisfield, Smith Island, and Tangier Island. Camp Arifjan is in the country of **Kuwait**, in the **Middle East**. These were verified using the using the Google Dork search. Yes, there appears to be a **food court or dining area** inside Camp Arifjan. This was determined from the image and description shown in the Google Maps result for "**Camp ArifjanPX**," which included a Subway restaurant and a menu board, indicating a food court-style setting within the PX shopping mall at the base.

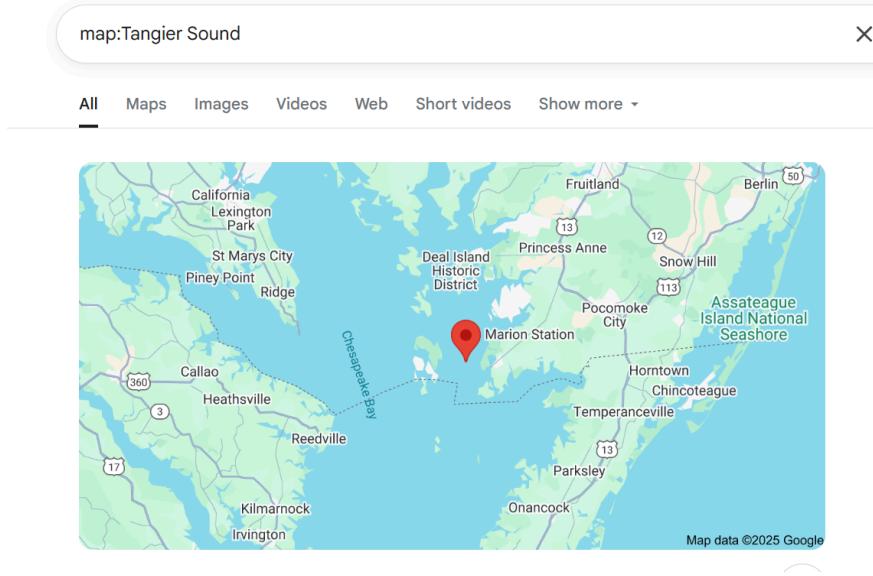


Figure 71: Map result for Tangier Sound.

Source: Google Maps. <https://www.google.com/maps>

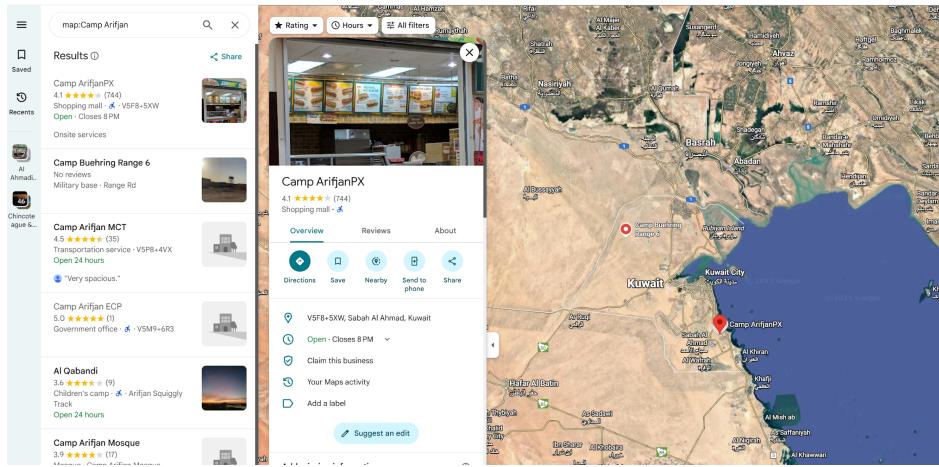


Figure 72: Map and facility result for Camp ArifjanPX.

Source: Google Maps. <https://www.google.com/maps>

The Google Dork command **set timer for 10 minutes** was executed in the Google Search bar, which activated Google's built-in timer feature directly within the search results. The timer started at 10:00 minutes and began counting down immediately. A screenshot was taken when the timer displayed **9:57** in progress, and another when the

timer reached **0**, accompanied by an audible alert. This feature highlights how Google Dorks can be used not only for information discovery but also to leverage interactive tools built into search, supporting tasks such as productivity tracking, reminders, or timed assessments.

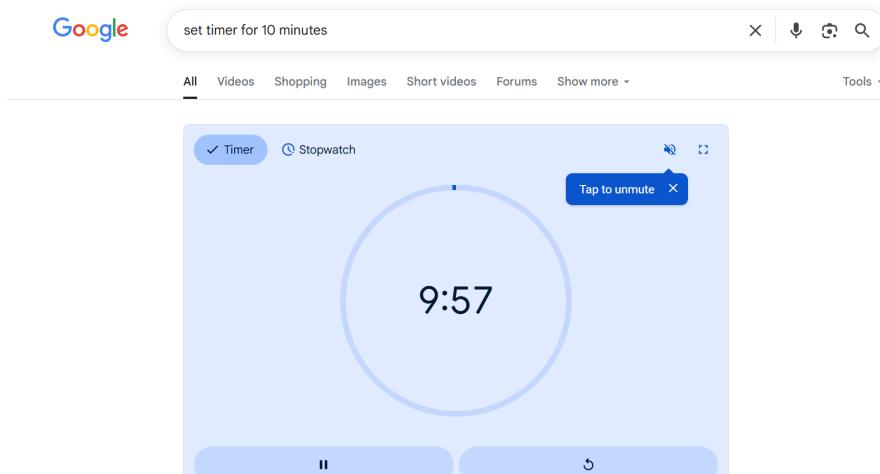


Figure 73: Google Search timer set to 10 minutes (screenshot showing 9:57).

Source: Google Search. <https://www.google.com>

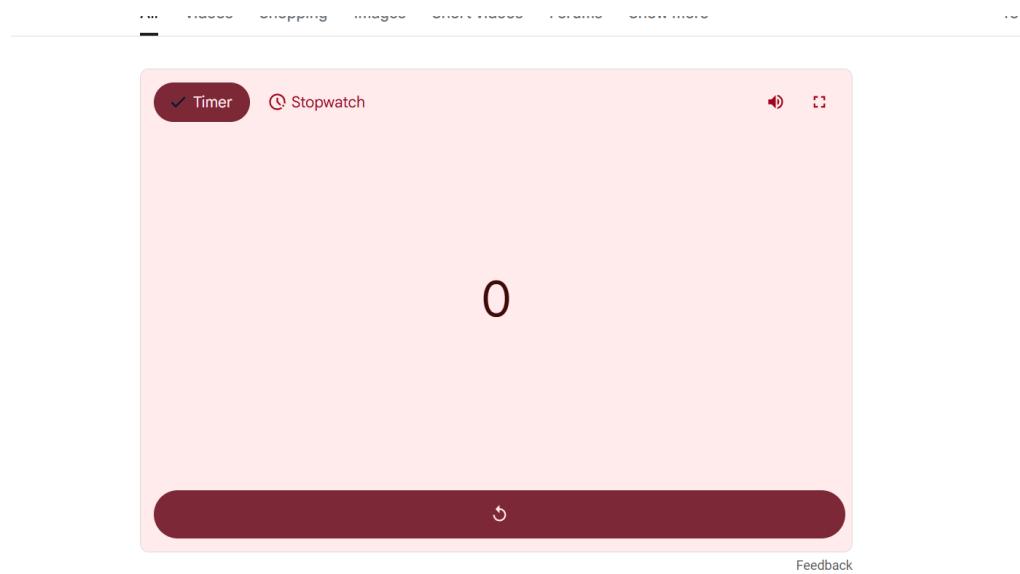


Figure 74: Google Search timer completion (screenshot showing 0).

Source: Google Search. <https://www.google.com>

To identify servers still displaying the Apache2 Ubuntu Default Page, the Google Dork command intitle:"Apache2 Ubuntu Default Page: It works" was executed. This query specifically targets web pages with the given HTML <title> tag, making it possible to detect systems that are either misconfigured or not yet secured. The results included publicly accessible servers, such as one associated with the Massachusetts Institute of Technology, along with others running on Ubuntu infrastructure.

The discovery of default Apache2 pages is significant from a security perspective. Such findings often indicate servers are in development stages or lack proper access controls. While ethical hackers and penetration testers may use this intelligence to notify administrators and strengthen defenses, malicious actors could view it as an opportunity for exploitation. Early identification of these misconfigurations allows organizations to address potential vulnerabilities before they can be leveraged.

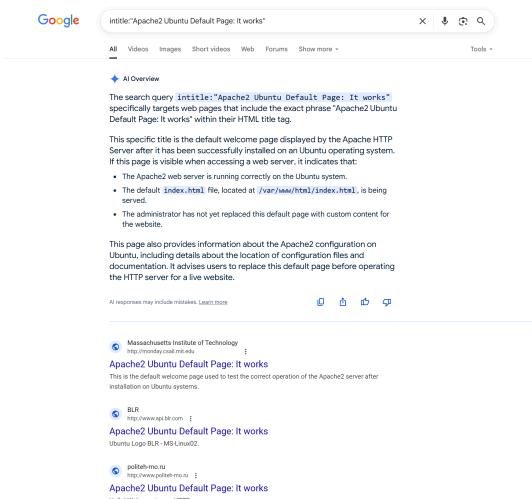


Figure 75: Google Search results for intitle:"Apache2 Ubuntu Default Page: It works".

Source: Google Search. <https://www.google.com>

To compare definitions of **Google Dorking**, the command **define: Google Dorking** was executed in Google Search, and results from several cybersecurity-focused sources were reviewed. According to **Imperva (2024)**, Google Dorking is a legitimate technique that leverages advanced search operators to uncover internet information that is not easily accessible through standard queries, often used by security professionals. **Okta (2024)** defines it as a method used by hackers to exploit search engines to identify vulnerabilities by locating exposed systems or sensitive data. Similarly, **Recorded Future (2024)** explains Google Dorks as advanced search techniques that help uncover hidden or specific information, providing cybersecurity analysts with critical intelligence that is otherwise difficult to obtain.

Collectively, these insights describe Google Dorking as the strategic use of specialized Google search operators to locate publicly accessible but sensitive content. This approach has dual relevance, serving ethical hackers and OSINT professionals for proactive defense, while also being misused by malicious actors. Its proper use strengthens cybersecurity posture by identifying weaknesses before they are exploited.

The screenshot shows Google search results for the query "define:Google Dorking". The top result is from Splunk, titled "Google Dorking: An Introduction for Cybersecurity ...". Below it is a snippet from Wikipedia about "Google hacking". Other results include links from Recorded Future and Okta, both discussing Google Dorking.

Figure 76: Google Search results for define:Google Dorking.

Source: Google. (2025). Google Search. <https://www.google.com>

The screenshot shows the Imperva Learning Center page for "Google Dorking". The page has a sidebar with "Article's content" sections like "What is Google Hacking/Dorking?", "How Does Google Dorking Work?", etc. The main content area is titled "Google Dorking" and defines it as a technique using advanced search operators to find specific information. It also discusses its legal nature and how it's used by security professionals.

Figure 77: Imperva definition of Google Dorking.

Source: Imperva. (2024). Google Dorking: What is Google Hacking/Dorking?

[Screenshot]. <https://www.imperva.com/learn/application-security/google-dorking/>

The screenshot shows a web page from Recorded Future. At the top, there is a navigation bar with links for 'Platform', 'Why Recorded Future', 'Services', 'Inkti Group', 'Research', and 'Resources'. A search bar is located at the top right. Below the navigation, a main content area starts with a heading 'Key Takeaways' followed by a bulleted list of points about Google Dorks. Underneath this is another section titled 'What are Google Dorks?' with a detailed explanation.

Figure 78: Recorded Future definition of Google Dorks.

Source: Recorded Future. (2024). What are Google Dorks? [Screenshot].

<https://www.recordedfuture.com/threat-intelligence-101/threat-analysis-techniques/google-dorks>

The screenshot shows a web page from Okta. The header includes links for 'Products', 'Why Okta', 'Developers', 'Resources', and a 'Free trial' button. The main title is 'Google Hacking (Google Dorking): Definition & Techniques'. Below the title, there is a brief description and a 'SHARE' button. The main content area contains sections on 'How does a Google hack work?' and 'How can you prevent Google hacking attacks?'. There is also a sidebar with links for 'TOPICS' like 'Cybersecurity' and 'TABLE OF CONTENTS'.

Figure 79: Okta definition of Google Hacking (Google Dorking).

Source: Okta. (2024, August 30). Google Hacking (Google Dorking): Definition & Techniques [Screenshot]. <https://www.okta.com/identity-101/google-hacking/>

To check for the presence of publicly accessible Microsoft Excel (.xlsx) files on the University of Maryland Global Campus (UMGC) domain, the Google Dork query **site:umgc.edu filetype:xlsx** was executed. This query restricts search results to only Excel files hosted on the specified domain. The search produced no results, displaying the message “*did not match any documents.*” This outcome suggests that UMGC does not host publicly available Excel files, or such files are intentionally restricted from being indexed by Google. Techniques like this are widely used in open-source intelligence (OSINT) and cybersecurity investigations to identify potentially exposed documents that may hold sensitive data.

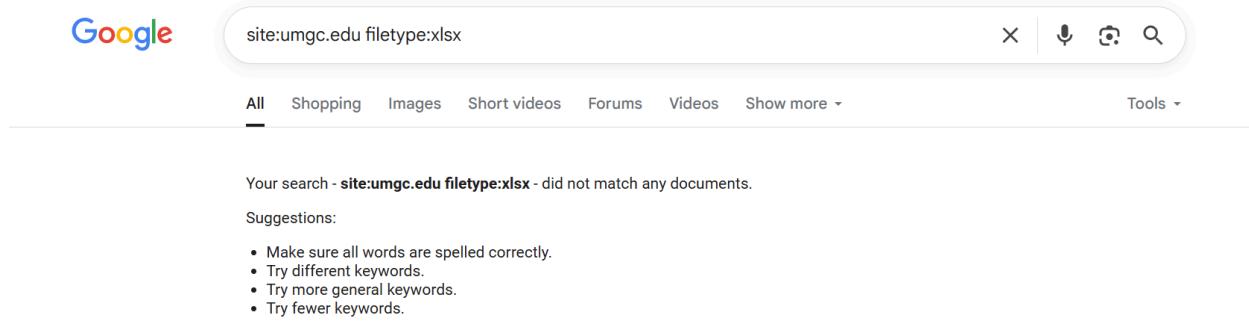


Figure 80: Google Dork query for Excel files on umgc.edu.

Source: Google. (2025). Search results for "site:umgc.edu filetype:xlsx" [Screenshot].

Google Search. <https://www.google.com>

Final IOC Analysis

A department requested access to four blocked domains: **mars.umgc.edu**, **linuxhint.com**, **financereports.co**, and **creativebookmark.com**. A comprehensive threat intelligence review was conducted using **Virus Total**, **Cisco Talos Intelligence Center**, and **AlienVault OTX** to determine whether access should be permitted.

The analysis of **mars.umgc.edu** confirmed the domain to be safe across all tools. Virus Total reported a clean status with no detections, Cisco Talos categorized it under *Education* with a favorable web reputation, and AlienVault OTX validated the site as whitelisted without associated threats. Based on these consistent findings, access to **mars.umgc.edu** is recommended for approval.

The domain **linuxhint.com** also demonstrated a safe profile. Virus Total showed no detections, Cisco Talos classified it under *Computers and Internet* with a favorable reputation, and AlienVault OTX indicated whitelisted status, though it noted historical telemetry. Since there is no evidence of active threats, access to **linuxhint.com** can be approved, with periodic monitoring advised.

The domain **financereports.co** raised significant concerns. Virus Total flagged it with multiple detections for phishing and malware, including from reputable vendors such as BitDefender and Sophos. Cisco Talos reported a *Neutral* reputation with outdated validation, while AlienVault OTX confirmed recent telemetry and suspicious activity. Given these consistent red flags, access to **financereports.co** should remain blocked.

The final domain, **creativebookmark.com**, also showed evidence of malicious activity. Virus Total flagged phishing and malware detections, Cisco Talos classified it as *Untrusted* with no defined category, and AlienVault OTX confirmed related malicious pulses. Since all platforms report threats and the domain lacks a trustworthy profile, access to creativebookmark.com should remain blocked.

Conclusion: Based on evidence from multiple intelligence sources, **mars.umgc.edu** and **linuxhint.com** should be approved for access, while **financereports.co** and **creativebookmark.com** should remain blocked due to phishing and malware concerns.

The screenshot shows the VirusTotal analysis page for the domain `mars.umgc.edu`. The top navigation bar includes a search field, a file upload button, and links for 'RECENT', 'TOP 1M', 'SITES', 'FILES', and 'API'. Below the search bar, there's a large green circle with a white '0' and a slash followed by '94', indicating 'Community Score'. To the right, a message says 'No security vendors flagged this domain as malicious'. The 'DETAILS' tab is selected, showing the domain's name and its IP address, `192.168.122.130`. The 'RELATIONS' tab shows no connections. The 'COMMUNITY' tab has a note about joining the community for more insights. A table titled 'Security vendors' analysis' lists results from various vendors:

Vendor	Result
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
benkow.cc	Clean
Blueliv	Clean
Acronis	Clean
Allabs (MONITORAPP)	Clean
Anti-AVL	Clean
BitDefender	Clean
Certego	Clean

At the bottom right, there's a link to 'Automate checks' and a note about automating analysis.

Figure 81: VirusTotal domain analysis for mars.umgc.edu.

Source: VirusTotal. Retrieved from <https://www.virustotal.com>

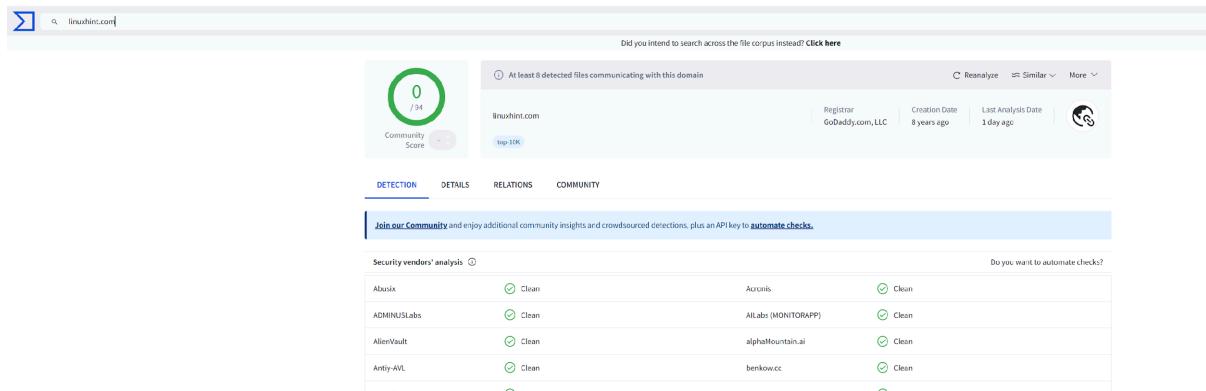


Figure 82: Cisco Talos Intelligence – mars.umgc.edu domain reputation.

Source: Cisco Talos. Retrieved from <https://talosintelligence.com>

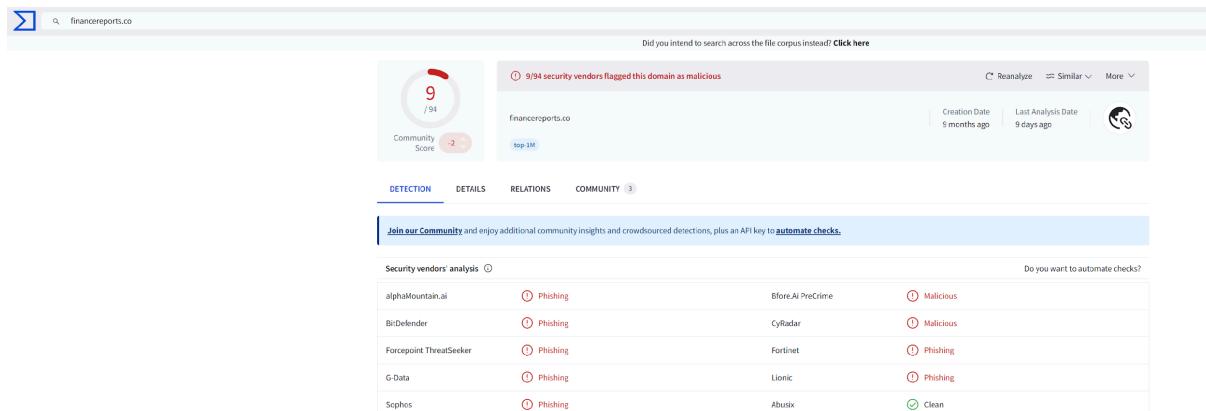


Figure 83: AlienVault OTX threat analysis for mars.umgc.edu.

Source: AlienVault OTX. Retrieved from <https://otx.alienvault.com>

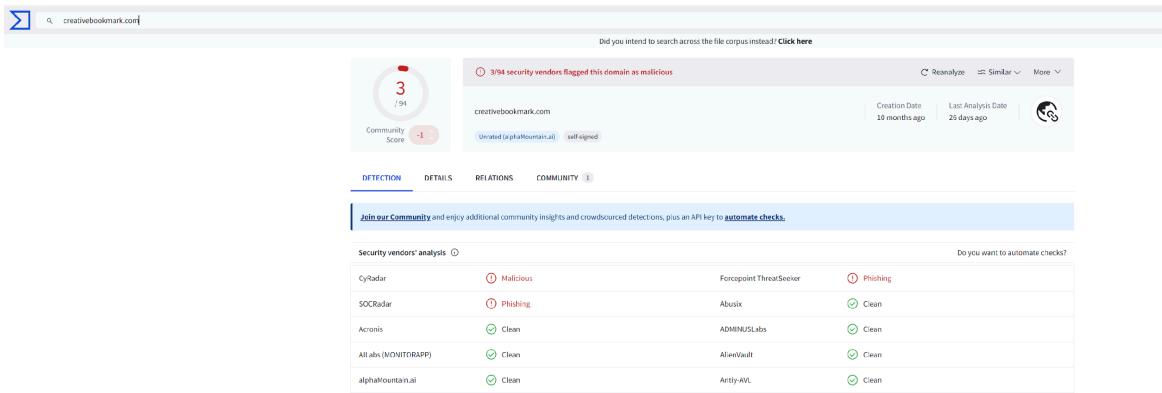


Figure 84: VirusTotal domain analysis for `linuxhint.com`.

Source: VirusTotal. Retrieved from <https://www.virustotal.com>

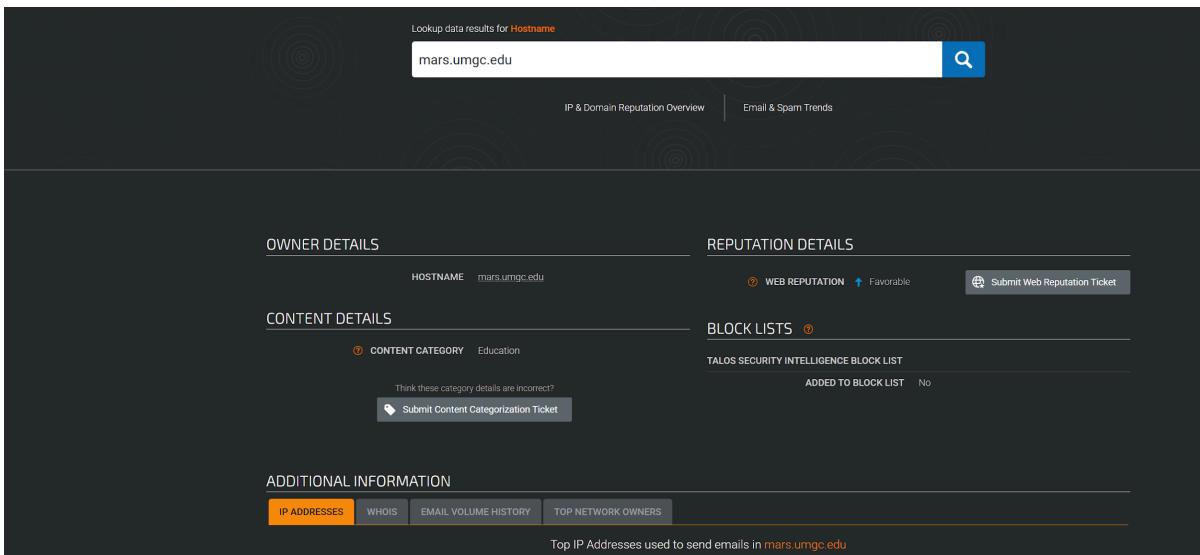


Figure 85: Cisco Talos Intelligence – `linuxhint.com` domain reputation.

Source: Cisco Talos. Retrieved from <https://talosintelligence.com>

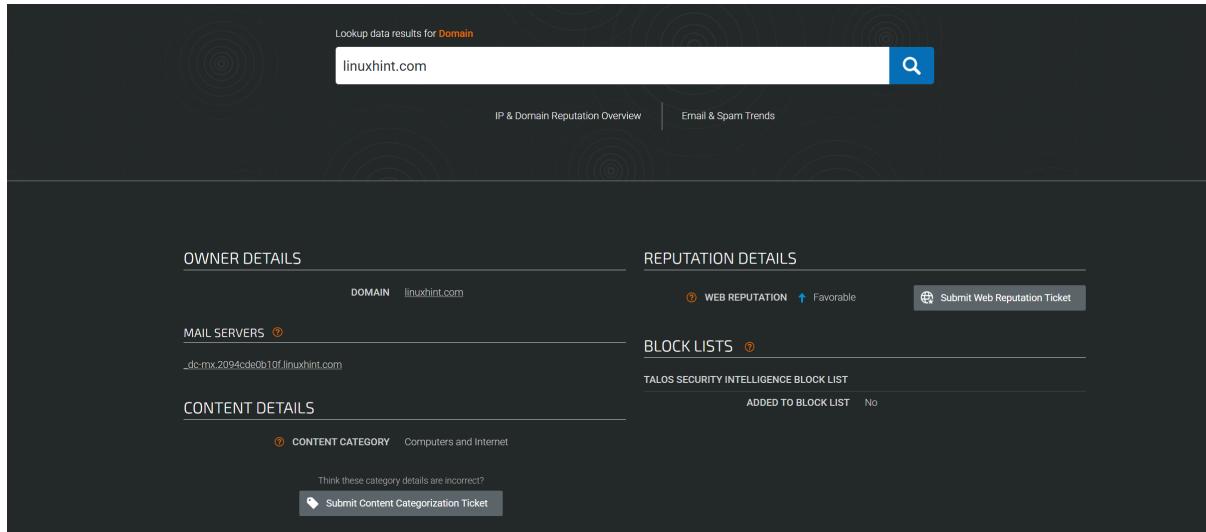


Figure 86: AlienVault OTX threat analysis for `linuxhint.com`.

Source: AlienVault OTX. Retrieved from <https://otx.alienvault.com>

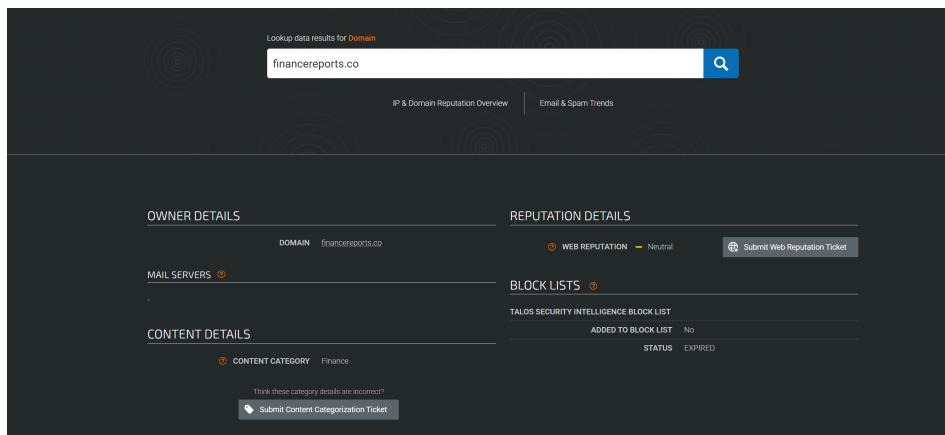


Figure 87: VirusTotal domain analysis for `financereports.co`.

Source: VirusTotal. Retrieved from <https://www.virustotal.com>

The screenshot shows the Cisco Talos Intelligence domain reputation page for the domain `creativebookmark.com`. The interface is dark-themed with orange highlights. At the top, there's a search bar with the query "creativebookmark.com" and a magnifying glass icon. Below the search bar are two tabs: "IP & Domain Reputation Overview" and "Email & Spam Trends".

OWNER DETAILS: Shows the domain as `creativebookmark.com`.

REPUTATION DETAILS: Shows "WEB REPUTATION" as "Untrusted". There's a button to "Submit Web Reputation Ticket".

CONTENT DETAILS: Shows "CONTENT CATEGORY" as "No established content categories". A link to "Submit Content Categorization Ticket" is present.

BLOCK LISTS: Shows "TALOS SECURITY INTELLIGENCE BLOCK LIST" with "ADDED TO BLOCK LIST" set to "No".

ADDITIONAL INFORMATION: Includes tabs for "IP ADDRESSES", "WHOIS", "EMAIL VOLUME HISTORY", and "TOP NETWORK OWNERS".

Figure 88: Cisco Talos Intelligence – `financereports.co` domain reputation.

Source: Cisco Talos. Retrieved from <https://talosintelligence.com>

The screenshot shows the AlienVault OTX threat analysis page for the domain `financereports.co`. The interface is light-themed. At the top, there's a search bar with the query "financereports.co" and a dropdown menu "Add to Pulse".

Basic Information: Verdict is "Whitelisted". Domain is `umgc.edu`, with 0 Pulses, 500 Passive DNS, 231 URLs, and 0 Files. IP Address is 151.101.131.10, 151.101.185.10, 151.101.3.10, 151.101.67.10. Location is United States. ASN is AS54113 fastly. Nameservers are ns-79.firebaseioapp.com and ns-1146.firebaseioapp-97.org. Related Pulses and Tags are both "None".

Indicator Facts: Historical OTX telemetry, Running webserver, Resolves to 4 IPs, Present in Majestic. Certificate Issuer is D-LIS, O-DigCert Inc, CH-DigCert Global Q2 '15 RSA SHA256 2020 CA!. Certificate Subject is CN=adobebeemcloud.com. External Resources include Whois, UrlVoid, and VirusTotal.

Analysis: Buttons for "Analysis", "Related Pulses", and "Comments (0)".

Figure 89: AlienVault OTX threat analysis for `financereports.co`.

Source: AlienVault OTX. Retrieved from <https://otx.alienvault.com>

The screenshot shows the AlienVault OTX threat analysis page for the domain `linuxhint.com`. The interface is light-themed. At the top, there's a search bar with the query "linuxhint.com" and a dropdown menu "Add to Pulse".

Basic Information: Verdict is "Whitelisted". IP Address is 104.216.173.172.67.136.17. Location is United States. ASN is AS13335 cloudflare. Nameservers are ns-georgia.cloudflare.com and ns-jersey.cloudflare.com. WHOIS information shows Registrar: GoDaddy.com, LLC, Creation Date: Dec 29, 2016. Related Pulses and Tags are both "None".

Indicator Facts: Malicious files hosted, Historical OTX telemetry, Running webserver, 2 subdomains, Resolves to 2 IPs, SPF record, Present in Majestic. AV Detection Rate is 0/1. External Resources include Whois, UrlVoid, and VirusTotal.

Analysis: Buttons for "Analysis", "Related Pulses", and "Comments (0)".

Figure 90: VirusTotal domain analysis for creativebookmark.com.

Source: VirusTotal. Retrieved from <https://www.virustotal.com>

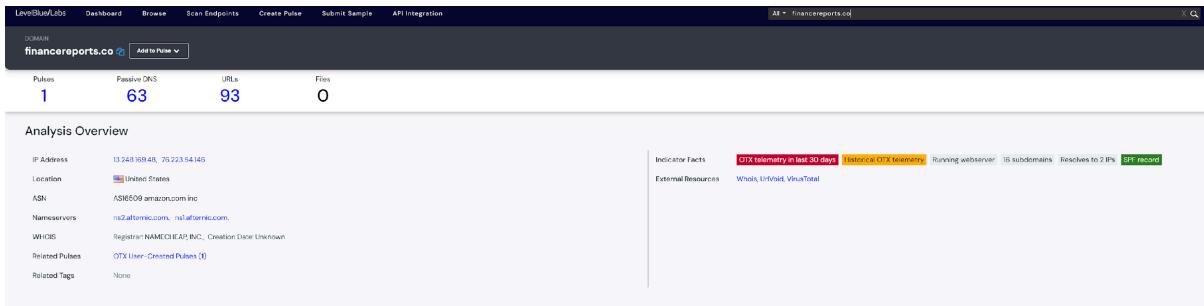


Figure 91: Cisco Talos Intelligence – creativebookmark.com domain reputation.

Source: Cisco Talos. Retrieved from <https://talosintelligence.com>

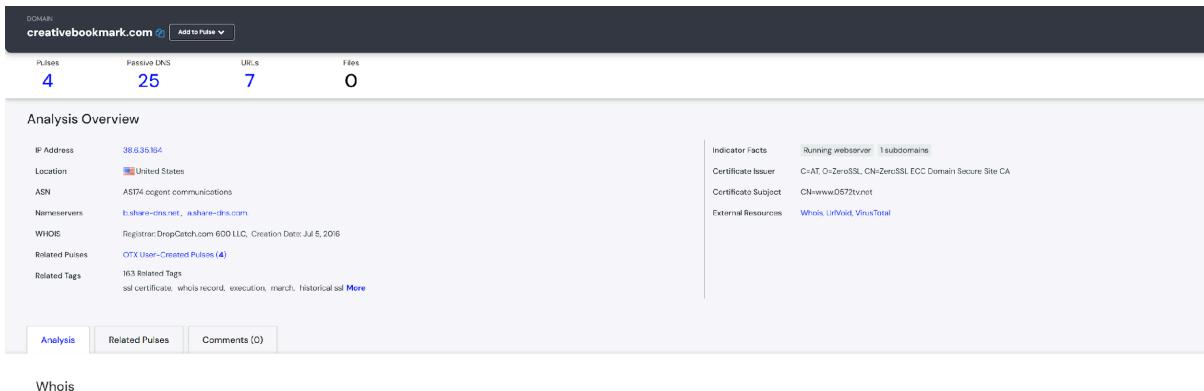


Figure 92: AlienVault OTX threat analysis for creativebookmark.com.

Source: AlienVault OTX. Retrieved from <https://otx.alienvault.com>

The file associated with the SHA-256 hash

b4bd56a2aebe3f5e020c5421e01c2d16804c25da673ecb125b074a94581cecf was

identified as **malicious by 59 of 72 security vendors** on VirusTotal. The detections

consistently label them as a **Ryuk or Hermes ransomware variant** (e.g.,

Ransomware.Ryuk, Generic.Ransom.Hermes.24692503, Windows.Ransomware.Ryuk).

Ryuk ransomware is a severe threat, commonly deployed in **targeted enterprise attacks**, where it encrypts files and renders systems inoperable until ransom demands are met. It is often distributed via **phishing campaigns** or paired with malware such as **Emotet or TrickBot** to facilitate lateral movement and persistence. The association with Hermes suggests added **anti-debugging and evasion capabilities**, making remediation more difficult.

The VirusTotal analysis, last updated **two months ago**, indicates the sample remains **active in the threat landscape**. Given its destructive impact, the file should be **immediately quarantined**, and a **full forensic investigation** should be conducted to assess organizational exposure.

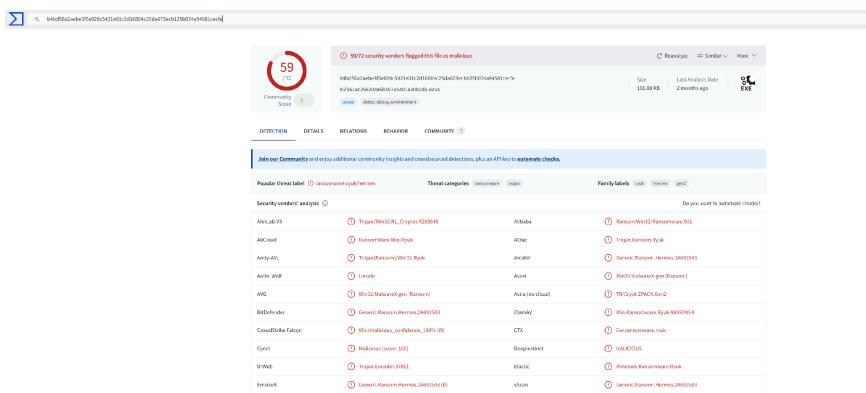


Figure 93: VirusTotal detection report for file hash

b4bd56a2aebe3f5e020c5421e01c2d16804c25da673ecb125b074a94581cecfe.

Source: VirusTotal – <https://www.virustotal.com>

The file associated with the SHA-256 hash d893a28a885344f46e74f3131d5ae3b3ecd2f5d29571afb124f556db86da40f3 was identified as **malicious by 56 of 72 security vendors** on VirusTotal. The primary

detection label is **Trojan.AutoIT.MalIT**, a malware family linked to AutoIT-based malicious scripts.

Detection results from trusted security vendors including **Kaspersky, AVG, BitDefender, and Microsoft**, confirm this file as a high-risk Trojan, with tags such as *autoit, malit, and multiverse*. These indicators suggest a **modular structure** capable of executing multi-stage payloads or employing obfuscation techniques to evade defenses. Additional behavioral markers, including **sandbox evasion, persistence, and anti-debugging tactics**, reinforce its classification as an advanced and adaptable threat.

The analysis, performed **one month ago**, highlights that this malware remains an **active risk** in the threat landscape. Given its ability to persist undetected and deliver multi-stage attacks, this file should be **immediately quarantined**, and systems exposed to it should undergo a **comprehensive forensic review** to prevent potential compromise.

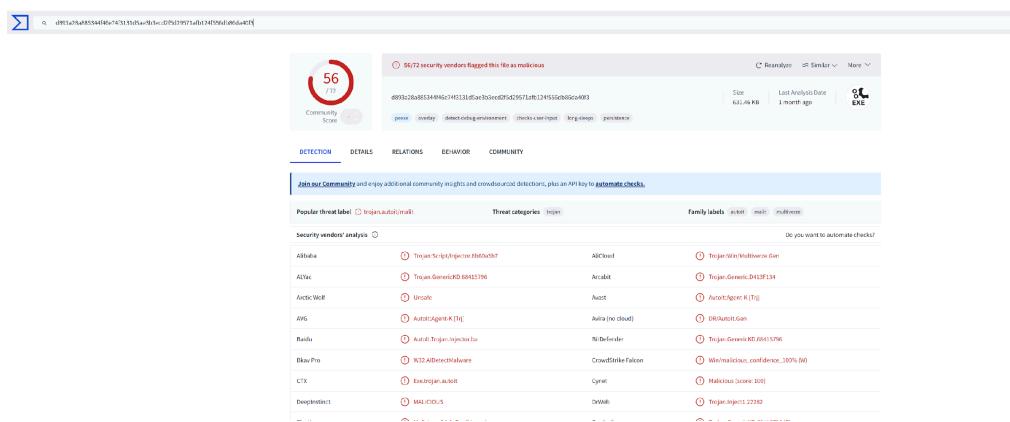


Figure 94: VirusTotal detection report for file hash

d893a28a885344f46e74f3131d5ae3b3ecd2f5d29571afb124f556db86da40f3.

Source: VirusTotal – <https://www.virustotal.com>

The file associated with the SHA-256 hash
5dc84570905973f2719578179596e36b4e29f2343ca360aeff730aacf7e37ed0 was flagged as **malicious by 30 of 72 security vendors** on VirusTotal. The most common detection label is **Adware.AmyBar/DNRHZ**, categorized as **adware, trojan, and potentially unwanted application (PUA)**.

Multiple vendors—including **Avira, Bkav Pro, CTX, and DrWeb**—identified the file as part of the *AmyBar* or *Adware.Bho.3907* family. Microsoft flagged it as **PUA:Win32/Bitregrep.B**, while ESET-NOD32 classified it as a **Win32/Adware.Toolbar.Amy variant**. The file type is a **.DLL**, and its behavior tags include **detect-debug-environment** and **overlay**, both of which are indicators of evasion tactics designed to bypass analysis and detection.

This adware family is known to alter browser configurations, install unwanted toolbars, and potentially expose systems to additional malware through secondary payloads. The last analysis date, recorded **three months ago**, highlights its ongoing relevance. Given its potential to compromise **privacy, system integrity, and user security**, this file should be **immediately quarantined**, and any affected systems should undergo remediation.

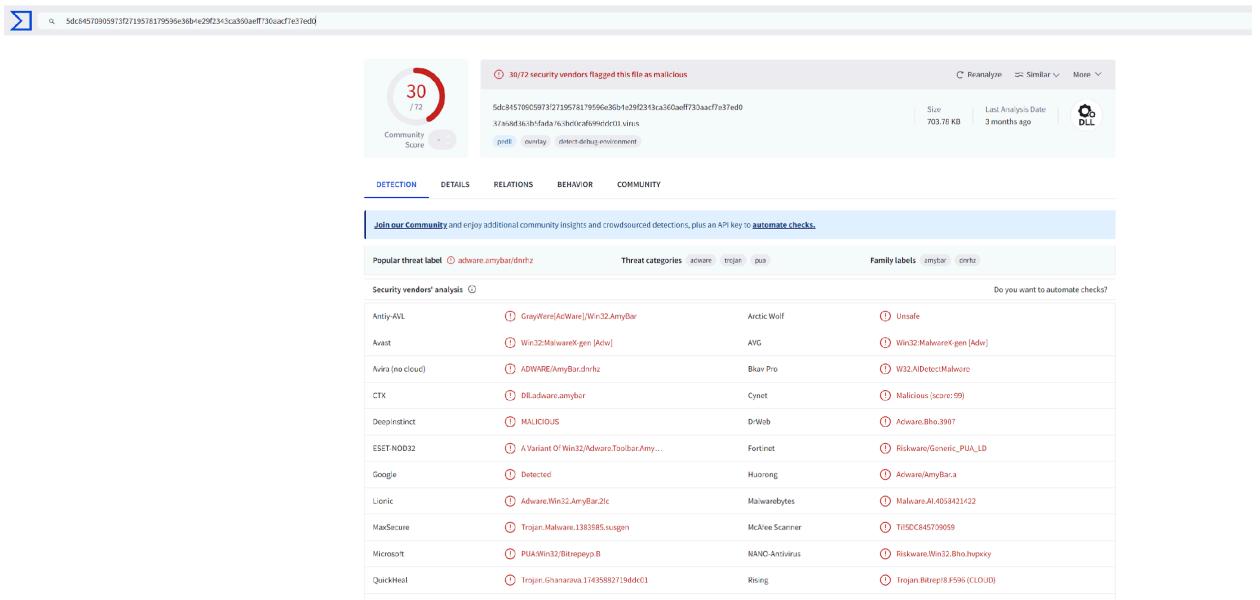


Figure 95: VirusTotal detection report for file hash

5dc84570905973f2719578179596e36b4e29f2343ca360aeff730aacf7e37ed0.

Source: VirusTotal – <https://www.virustotal.com>

The files associated with the SHA-256 hashes

D94BB76D6A8FBA54D6579A6265F6EAE66E905B8667D1B33080D28A2F7D068C0D and

456A194F501984067435393729294ECC02E75973C011F1E765EEB3FC6C23CBE4 were

analyzed on VirusTotal, and **no malicious detections** were reported by any security

vendors. This indicates that both files are currently considered **safe for routine use**.

While no threats were identified, it is recommended that these files remain under **periodic reevaluation**. The evolving threat landscape means that previously benign files may later be weaponized or flagged as suspicious by updated detection engines. Maintaining them on a **watchlist** ensures proactive monitoring against any emerging risks.

The screenshot shows the VirusTotal search interface. The search bar at the top contains the file hash: D94BB76D6A8FBA54D6579A6265F6EAE66E905B8667D1B33080D28A2F7D068C0D. Below the search bar, there is a 'COMMENTS' section with a count of 0. A message encourages users to 'Join our Community' and provides instructions for API keys and automated checks. The main search results area displays a message: 'We currently don't have any comments that fit your search'. It also includes a note about refining search terms or checking syntax, a link to documentation for query tips and modifiers, and a 'Try a new search' button.

Figure 96: VirusTotal analysis result for file hash

D94BB76D6A8FBA54D6579A6265F6EAE66E905B8667D1B33080D28A2F7D068C0D.

Source: [VirusTotal](#)

The screenshot shows the VirusTotal search interface. The search bar at the top contains the file hash: 456A194F501984067435393729294ECC02E75973C011F1E765EEB3FC6C23CBE4. Below the search bar, there is a 'COMMENTS' section with a count of 0. A message encourages users to 'Join our Community' and provides instructions for API keys and automated checks. The main search results area displays a message: 'We currently don't have any comments that fit your search'. It also includes a note about refining search terms or checking syntax, a link to documentation for query tips and modifiers, and a 'Try a new search' button.

Figure 97: VirusTotal analysis result for file hash

456A194F501984067435393729294ECC02E75973C011F1E765EEB3FC6C23CBE4.

Source: [VirusTotal](#)

To verify the integrity and safety of the organization's documents, SHA-256 hashes were generated for three files and subsequently analyzed using VirusTotal to detect any potential malware threats.

- The first file, **2022-2023catalog.pdf**, produced the SHA-256 hash
d391a0bd202f075c9725bfa21422fa6ca378caa234bba743cf75012593b8ec93. Upon scanning this hash with VirusTotal, the file was found to be clean with **zero security vendors flagging it as malicious**.
- The second file, **courseplanner.pdf**, had a generated hash of
9ed6d10aece6f0b9a3289f440003c4734ea931e2577cf05354a984437a092de3. Like the first file, it was also scanned by VirusTotal, and **no malicious activity was detected** by any of the 64 antivirus engines.
- Finally, the **samplecoverletter.pdf** file resulted in the SHA-256 hash
b59633e1a54a06ff7c5cfa8dd7efa3217a1db9c6610fa8f9b857920a7e10c02f. This hash was also submitted to VirusTotal and received a **clean report**, with **zero detections** across all participating security vendors. Based on this thorough analysis, all three files are confirmed safe and pose no malware threat, ensuring secure distribution and verification across the organization's systems.

The screenshot shows a web-based SHA-256 file checksum calculator. The interface has three main sections: Settings, Input, and Output.

- Settings:** Contains options like "Hash" (selected), "Auto-Update" (checked), "Remember Input" (unchecked), "Input Type" (set to "File"), "Output Encoding" (set to "Hex (Lower Case)" checked), and "Enable HMAC" (unchecked).
- Input:** Shows a file icon and the path "2022-2023catalog.pdf".
- Output:** Displays the SHA-256 hash value: "d391a0bd202f075c9725bfa21422fa6ca378caa234bba743cf75012593b8ec93".

Figure 98: SHA-256 hash generation for 2022-2023catalog.pdf using OnlineHashCrack SHA256 Generator.

Source: [OnlineHashCrack SHA256 Generator](#)

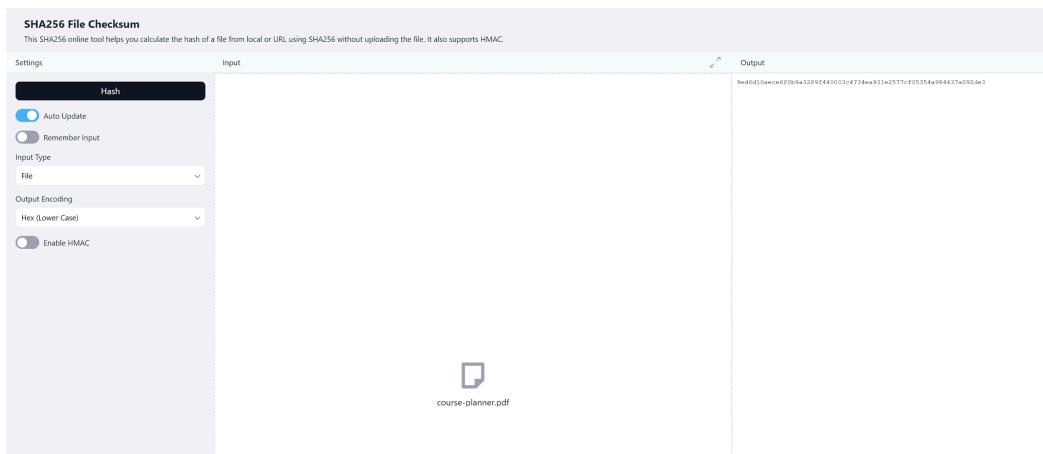


Figure 99: SHA-256 hash generation for courseplanner.pdf using OnlineHashCrack SHA256 Generator.

Source: [OnlineHashCrack SHA256 Generator](#)

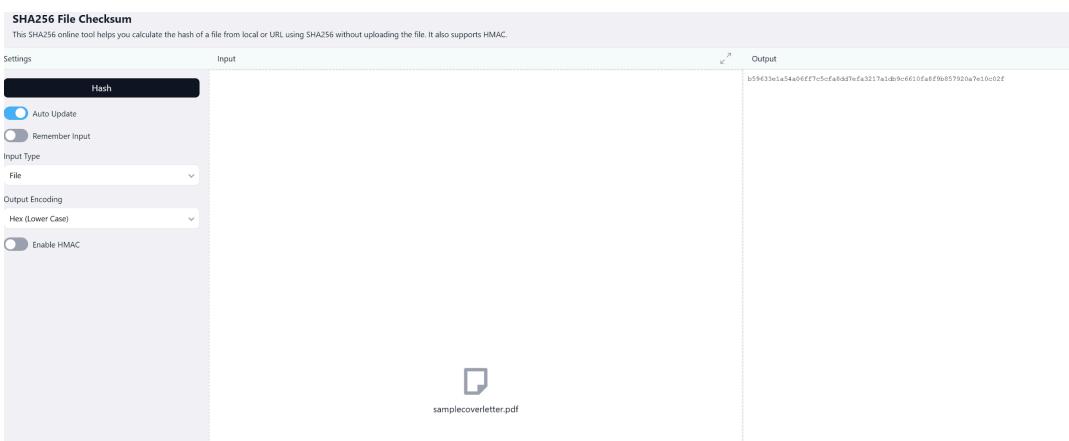


Figure 100: SHA-256 hash generation for samplecoverletter.pdf using OnlineHashCrack SHA256 Generator.

Source: [OnlineHashCrack SHA256 Generator](#)

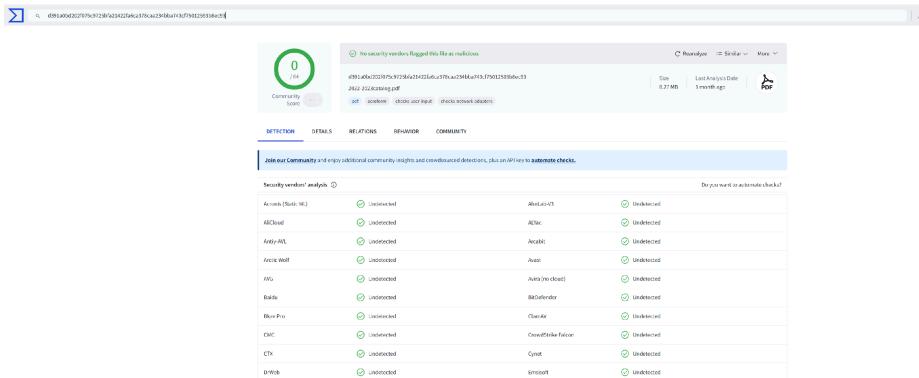


Figure 101: VirusTotal scan results for 2022-2023catalog.pdf showing no detections.

Source: VirusTotal

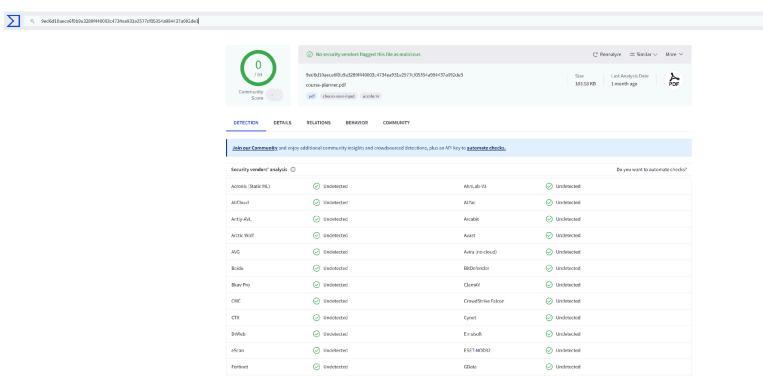


Figure 102: VirusTotal scan results for courseplanner.pdf showing no detections.

Source: VirusTotal

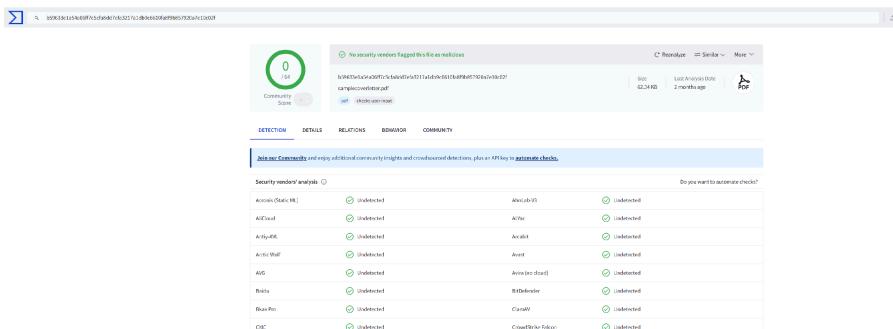


Figure 103: VirusTotal scan results for samplecoverletter.pdf showing no detections.

Source: VirusTotal

Summary

Throughout this project, a wide range of open source threat intelligence tools and techniques were applied, each providing distinct strengths in identifying, validating, and contextualizing Indicators of Compromise (IOCs). Tools such as Virus Total and Cisco Talos enabled foundational file and domain-based threat analysis, supporting rapid identification of malware through hash lookups and domain categorizations. Virus Total's multi-engine scanning and accessible interface proved particularly effective in validating suspicious files. However, its reliance on known threats limits effectiveness against novel or obfuscated malware, making it unsuitable for zero-day detection. Cisco Talos, while rich in research insights and reputation data, offered less flexibility for large scale API-driven analysis in its free tier.

AlienVault OTX added value by providing community driven intelligence feeds that enriched IOC context with peer sourced threat pulses. Its ability to correlate and share threat data across organizations is a key advantage for SOC teams monitoring emerging threats. Nevertheless, reliance on community input can introduce false positives or unverified claims, requiring human validation to filter noise. Maltego further strengthened investigative workflows by enabling visual correlation of domains, IP addresses, and organizational relationships. The platform's graphical mapping enhanced understanding of complex entity connections, though its steep learning curve and partial reliance on third party integrations limited efficiency in time sensitive scenarios.

Reconnaissance tools available in Kali Linux, including Nmap, dnsenum, dnsrecon, dnsmap, and fierce, proved critical in surface level and in depth enumeration

of network infrastructure. Nmap remains an industry standard for its customizable port scanning and scripting capabilities but can be noisy and easily detected by intrusion detection systems. DNS enumeration tools such as dnsrecon and fierce were particularly effective in uncovering subdomains and misconfigured servers, contributing to asset discovery. Despite these strengths, the absence of modern GUIs and reporting functionality means these tools often require manual log parsing and interpretation. Their command line orientation provides flexibility for advanced users but may limit accessibility for non-technical analysts.

In parallel, OSINT techniques such as Google Dorks highlighted the risk of publicly exposed sensitive data. While simple, this method underscored how improperly secured or misclassified information can serve as an entry point for attackers. The ability to creatively leverage search operators makes this technique invaluable during passive reconnaissance, but its effectiveness depends heavily on analyst expertise. Correlation with structured platforms such as Virus Total or Maltego provided the necessary contextual analysis to strengthen findings and reduce ambiguity.

Looking forward, the breadth of tools used underscores the importance of integrating multiple data sources to create a holistic threat picture. Commercial platforms such as Recorded Future, Anomali, or ThreatConnect represent the next step in scaling enterprise capabilities. These solutions offer enriched feeds, real-time alerting, machine learning-driven noise reduction, and SIEM integration, enabling more efficient triage and deeper historical analysis (Paganini, 2023). While open-source platforms

remain indispensable for enrichment and initial analysis, enterprise-grade solutions reduce analyst fatigue and streamline workflows.

Each tool served a distinct role within the investigative lifecycle, from domain and file analysis to infrastructure mapping. No single solution provided comprehensive coverage; however, layering tools, validating results, and automating workflows produced stronger resilience against modern cyber threats. For organizations seeking to balance agility with accuracy, adopting a hybrid ecosystem leveraging OSINT for enrichment and commercial platforms for decision making represents the most strategic path forward.

References

A10 Networks. (n.d.). *What is IPv6 and what is IPv4 to IPv6 translation?*

<https://www.a10networks.com/learning-center/ipv6/ipv4-to-ipv6-translation/>

AT&T Cybersecurity. (n.d.). *AlienVault OTX: Open Threat Exchange.* <https://otx.alienvault.com/>

AWS. (n.d.). *Key differences between IPv4 and IPv6.* Amazon Web Services. Retrieved July 27, 2025, from <https://aws.amazon.com/compare/the-difference-between-ipv4-and-ipv6/>

CISA. (2021). *Federal government cybersecurity incident and vulnerability response playbooks.* Cybersecurity and Infrastructure Security Agency.

https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Cisco Talos Intelligence Group. (n.d.). *Reputation center.* <https://talosintelligence.com/>

Cloudflare. (2022). *Using DNS to estimate the worldwide state of IPv6 adoption.* Cloudflare Blog.
<https://blog.cloudflare.com/ipv6-from-dns-pov/>

Cloudflare. (n.d.). *Types of DNS records.* Retrieved July 27, 2025, from
<https://www.cloudflare.com/learning/dns/dns-records/>

GeeksforGeeks. (n.d.). *Differences between IPv4 and IPv6.*
<https://www.geeksforgeeks.org/computer-networks/differences-between-ipv4-and-ipv6/>

L

ICANN. (n.d.). *DNS terminology*. Internet Corporation for Assigned Names and Numbers.

<https://www.icann.org/resources/pages/glossary-2014-02-03-en#t>

Imperva. (2024). *Google dorking: What is Google hacking/dorking?*

<https://www.imperva.com/learn/application-security/google-dorking/>

Kali Linux Tools. (n.d.). *Fierce*. <https://tools.kali.org/information-gathering/fierce>

Kinsta. (2024, March 25). *What is a nameserver? Why are nameservers important?*

<https://kinsta.com/knowledgebase/what-is-a-nameserver/>

Lifewire. (2020, March 31). *IPv4 vs. IPv6: What's the difference?*

<https://www.lifewire.com/ipv4-vs-ipv6-4780834>

Lyon, G. F. (n.d.). *Nmap: The network mapper – Free security scanner*. <https://nmap.org/>

MITRE ATT&CK. (2024). *Tactics, techniques, and procedures*. <https://attack.mitre.org/>

National Institute of Standards and Technology. (2007a). *Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94)*.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf>

National Institute of Standards and Technology. (2007b). *Guide to vulnerability assessment (NIST Special Publication 800-115)*. <https://csrc.nist.gov/publications/detail/sp/800-115/final>

Northland Controls. (n.d.). *The growing importance of open source intelligence (OSINT) within your safety and security toolkit*.

[https://www.northlandcontrols.com/blog/the-growing-importance-of-open-source-intel
ligence-osint-within-your-safety-and-security-toolkit](https://www.northlandcontrols.com/blog/the-growing-importance-of-open-source-intelligence-osint-within-your-safety-and-security-toolkit)

Nmap. (n.d.). *Network mapper – Free security scanner.* <https://nmap.org/>

Offensive Security. (n.d.). *Dnsenum – DNS enumeration script.* Kali Linux Tools.

<https://www.kali.org/tools/dnsenum/>

Offensive Security. (n.d.). *Dnsmap – Passive DNS mapping tool.* Kali Linux Tools.

<https://www.kali.org/tools/dnsmap/>

Offensive Security. (n.d.). *DNSRecon.* Kali Linux Tools.

<https://tools.kali.org/information-gathering/dnsrecon>

Okta. (2024, August 30). *Google hacking (Google dorking): Definition & techniques.*

<https://www.okta.com/identity-101/google-hacking/>

OnlineHashCrack. (n.d.). *Online hash calculator (SHA-256, MD5, etc.).*

<https://www.onlinehashcrack.com/hash-calculator.php>

Paganini, P. (2023). *Threat intelligence: Best platforms and emerging trends.* Security Affairs.

<https://securityaffairs.com>

Recorded Future. (2024). *Google dorks: Threat intelligence 101.*

<https://www.recordedfuture.com/threat-intelligence-101/threat-analysis-techniques/google-dorks>

Scarfone, K., & Mell, P. (2007). *Guide to vulnerability assessment (NIST SP 800-115).* National Institute of Standards and Technology.

<https://csrc.nist.gov/publications/detail/sp/800-115/final>

Seclists. (2023). *SecLists: Security tester's companion*. GitHub.

<https://github.com/danielmiessler/SecLists>

VirusTotal. (n.d.). *VirusTotal – Free online virus, malware, and URL scanner*.

<https://www.virustotal.com/>

Wikipedia. (n.d.). *IPv6*. <https://en.wikipedia.org/wiki/IPv6>