

Blue Team Level 1 Certification
(Standard)

Introduction to BTL1

Welcome to Blue Team Level 1

4 Topics

Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN

Introduction to Security Fundamentals

1 Topic

Soft Skills

7 Topics

Security Controls

5 Topics 1 Quiz

Networking

6 Topics 1 Quiz

Management Principles

4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

PA2) Types of Phishing Emails

10 Topics 2 Quizzes

PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

Section Introduction: Analysing Artifacts

Visualization Tools

URL Reputation Tools

File Reputation Tools

Malware Sandboxing

[Video] Manual Artifact Analysis

Artifact Analysis With PhishTool

[Video] Artifact Analysis with PhishTool

Activity: End of Section Review: Analysing Artifacts

PA6) Taking Defensive Actions

12 Topics 1 Quiz

PA7) Report Writing

7 Topics 1 Quiz

PA8) Phishing Response Challenge

3 Topics 1 Quiz

THREAT INTELLIGENCE DOMAIN

TI1) Introduction to Threat Intelligence

7 Topics

TI2) Threat Actors & APTs

6 Topics 2 Quizzes

TI3) Operational Threat Intelligence

7 Topics 1 Quiz

URL Reputation Tools

Blue Team Level 1 Certification (Standard) > PA5) Analysing URLs, Attachments, and Artifacts > U...

COMPLETE



This lesson will cover how to perform reputation checks for potentially malicious URLs, helping us to decide if they are actually malicious or not. Whilst there are a number of free online reputation tools, we are going to be focusing on VirusTotal and URLScan.io, as they are the most complete and easy to use. Below we will cover how to use these tools to determine if URLs have been marked as malicious by the security community. **It is extremely important to remember that if something is not being identified as malicious by online reputation tools, it does not mean it is safe.** We're sure you've heard of the phrase "innocent until proven guilty" – we need to use the opposite here. Assume that suspicious sites are malicious until you can prove it is safe to visit.

While reputation sites can be a good resource, you need to remember they are not always effective, and further analysis is always needed. If a URL or domain has a malicious community score, it means the URL has been analyzed and reported as malicious before. Targeted and unique attacks will not have been analyzed by other security professionals, therefore URLs could come back with no negative comments, but could be extremely malicious.

VIRUSTOTAL

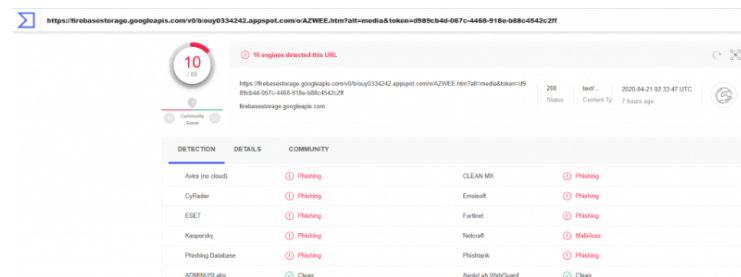
Head over to VirusTotal and you'll be met with the simple web GUI. Click on the URL tab, and you'll see the same as the below screenshot. Here we can enter malicious URLs to retrieve reputation scores.



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community



Now I'm going to enter in a URL that I know goes to a live Outlook credential harvester. We can see that the URL has been recognized as malicious by a number of vendors, including Kaspersky, ESET, and Fortinet.



<div><div></div><div>I14) Iactical Threat Intelligence</div></div> <div><div>7 Topics</div><div>1 Quiz</div></div>
<div><div></div><div>T15) Strategic Threat Intelligence</div></div> <div><div>5 Topics</div><div>1 Quiz</div></div>
<div><div></div><div>T16) Malware and Global Campaigns</div></div> <div><div>6 Topics</div><div>1 Quiz</div></div>
<div>DIGITAL FORENSICS DOMAIN</div>
<div><div></div><div>DF1) Introduction to Digital Forensics</div></div> <div><div>5 Topics</div></div>
<div><div></div><div>DF2) Forensics Fundamentals</div></div> <div><div>10 Topics</div><div>5 Quizzes</div></div>
<div><div></div><div>DF3) Digital Evidence Collection</div></div> <div><div>8 Topics</div><div>1 Quiz</div></div>
<div><div></div><div>DF4) Windows Investigations</div></div> <div><div>3 Topics</div><div>3 Quizzes</div></div>
<div><div></div><div>DF5) Linux Investigations</div></div> <div><div>4 Topics</div><div>2 Quizzes</div></div>
<div><div></div><div>DF6) Volatility</div></div> <div><div>3 Topics</div><div>1 Quiz</div></div>
<div><div></div><div>DF7) Autopsy</div></div> <div><div>4 Topics</div><div>1 Quiz</div></div>
<div>SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN</div>
<div><div></div><div>SI1) Introduction to SIEM</div></div> <div><div>7 Topics</div><div>1 Quiz</div></div>
<div><div></div><div>SI2) Logging</div></div> <div><div>6 Topics</div><div>2 Quizzes</div></div>
<div><div></div><div>SI3) Aggregation</div></div> <div><div>2 Topics</div><div>1 Quiz</div></div>
<div><div></div><div>SI4) Correlation</div></div> <div><div>6 Topics</div><div>1 Quiz</div></div>
<div><div></div><div>SI5) Using Splunk</div></div> <div><div>5 Topics</div><div>2 Quizzes</div></div>
<div>INCIDENT RESPONSE DOMAIN</div>
<div><div></div><div>IR1) Introduction to Incident Response</div></div> <div><div>8 Topics</div><div>1 Quiz</div></div>
<div><div></div><div>IR2) Preparation Phase</div></div> <div><div>10 Topics</div><div>2 Quizzes</div></div>
<div><div></div><div>IR3) Detection and Analysis Phase</div></div> <div><div>7 Topics</div><div>4 Quizzes</div></div>
<div><div></div><div>IR4) Containment, Eradication, and Recovery Phase</div></div> <div><div>5 Topics</div><div>1 Quiz</div></div>
<div><div></div><div>IR5) Lessons Learned and Reporting</div></div> <div><div>7 Topics</div></div>
<div><div></div><div>IR6) MITRE ATT&CK</div></div> <div><div>13 Topics</div><div>2 Quizzes</div></div>
<div>BTL1 EXAM</div>
<div><div></div><div>Exam Preparation</div></div>
<div><div></div><div>Using RDP and SSH</div></div>
<div><div></div><div>How to Start Your Exam</div></div>

AlertVault	Clean	Anti-Mal	Clean
Artists Against ISIS	Clean	BACKPAGE INFO	Clean

URLSCAN

URLScan is a service that can provide us with **tons** of information about a URL. To walk you through this tool, we're going to enter the same URL that we just saw was flagged as malicious on VirusTotal.

firebasestorage.googleapis.com

2a00:1450:4001:81d::200a **Malicious Activity!**

URL: https://firebasestorage.googleapis.com/v0/ouy0334242.appspot.com/u/AZWEE.htm?alt=media&token=d989cb4d-067c-4468-918e-b88c4542c2ff

Submission: On April 21 via manual (April 21st 2020, 9:57:31 am) from GB

Summary HTTP to Behaviour IoCs Similar Links DOM Content API

Summary

This website contacted 7 IPs in 4 countries across 5 domains to perform 10 HTTP transactions. The main IP is 2a00:1450:4001:81d::200a, located in Frankfurt am Main, Germany and belongs to GOOGLE US. The main domain is firebasestorage.googleapis.com. TLS certificate: Issued by GTS CA 101 on April 1st 2020. Valid for: 3 months.

The main domain was scanned 10288 times on urlscan.io Show Scans 10288

17951 structurally similar pages on different IPs, domains and ASNs found Show Scans 17951

Verdict: **Malicious** (Score: 100/100)

urlscan **Score: 100** phishing Show Details

Phishing against **Outlook Web Access (Online)**

Google Safe Browsing: **Clean** (Current Classification)

Additional live information

Current DNS A record: 172.217.22.74 (AS15169 - GOOGLE, US)

Domain created: January 25th 2005, 17:52:26 (UTC)

Domain registrar: MarkMonitor Inc.

Screenshot

Live screenshot Full Image

Detected technologies

Bootstrap (Web Frameworks) Website

Font Awesome (Font Scripts) Website

Stats

10 Requests

0 Ad-blocked

0 Malicious

100% HTTPS

100% IPv6

5 Domains

6 Subdomains

7 IPs

4 Countries

203kB Transfer

506kB Size

0 Cookies

Domain & IP information

IP/ASNs IP Detail (Sub)Domains Domain Tree Links Certificates

	IP Address	AS Autonomous System
1	2a00:1450:4001:81d::200a	15169 (GOOGLE)
2	2001:4840::1:1	2001:4840::1:1

As you can see, we've been presented with so much useful information. From a reputation score to a screenshot, web technologies used on the site to domain and IP information. Whilst all of this information can be useful during high profile investigations, typically using URL2PNG for visualization will be enough.

THREAT FEEDS

There are a number of public threat feeds that can provide security teams with intelligence regarding phishing attacks and malicious artifacts that can be used to power blacklists for email security products. Examples of these feeds include [URLhaus](#) and [PhishTank](#). Let's explore them both below.

Firstly, let's look at the [URLhaus Database](#), a huge collection of malicious URLs reported by researchers. In this screenshot, you can see the date the URL was added to the database, the malicious URL, the status showing whether this resource is still available on the internet or not, tags that show at a glance what the malware is (in these URLs we can see they're hosting Quakbot), and the final column shows which user reported these URLs.

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2020-06-10 20:04:05	https://mpiamyanmar.com/jpkdeozpnnj/3MrzSwYZO...	Offline	Quakbot Quakbot zip	@spamhaus
2020-06-10 20:03:56	http://epimarket.com.ua/vgbfVXXuDosp7E6.zip	Online	Quakbot Quakbot zip	@spamhaus
2020-06-10 20:03:47	http://hainstylingio.gr/pduvkn/d/DVgO1g71.zip	Online	Quakbot Quakbot zip	@spamhaus
2020-06-10 20:03:43	http://adamhyland.co.uk/gyhb/VScqYlVnKzC.zip	Online	Quakbot Quakbot zip	@spamhaus
2020-06-10 20:03:34	https://www.guer-immobilier.com/bafimwksz/D/nL...	Online	Quakbot Quakbot zip	@spamhaus
2020-06-10 20:03:29	https://inspocoach.com/xcdfyggshy/r1ZbbE7YB9.zip	Online	Quakbot Quakbot zip	@spamhaus
2020-06-10 20:03:21	http://www.victoriadirtysecret.net/knoihesuwj...	Online	Quakbot Quakbot zip	@spamhaus
2020-06-10 20:03:08	http://xianbaoku.com/zhmqqghtml/7rOQ38Kfg3.zip	Online	Quakbot Quakbot zip	@spamhaus

URLhaus offers a number of [threat feeds](#) that can provide specific information, and as mentioned above can be used to generate blacklists of malicious URLs that can be blocked proactively to prevent users from visiting these known malicious sites.

ASN Feed

The *ASN Feed* contains all URLs from the URLhaus database whose domain name resolve to an IP address associated with a particular AS number, no matter whether the URL is active (online) or not.

Please do not fetch the feed more often than every 10 minutes.

ASxxxx

Generate

Country Feed

The *Country Feed* contains all URLs from the URLhaus database whose domain name resolve to an IP address associated with a particular geo IP location (country code), no matter whether the URL is active (online) or not.

Please do not fetch the feed more often than every 10 minutes.

CH

Generate

TLD Feed

The *TLD Feed* contains all URLs from the URLhaus database whose domain name is associated with a specific ccTLD or gTLD (e.g. de, com, etc), no matter whether the URL is active (online) or not.

Please do not fetch the feed more often than every 10 minutes.

com

Generate

PhishTank operates like URLhaus, and allows users to submit phishing artifacts which are then verified by the wider community. In the below screenshot you can see what looks like the URLhaus database.

Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
6622615	https://mundoaspirin.com/dna/dna/login.php/dna/d...	ICAN000
6622613	https://theaircity.com/BankofAmerica/bankofamer...	ICAN000
6622612	https://thathugabotapp44.g00s.com/login.php	ICAN000
6622610	https://pymcars.com/one/OneDriveCloud/login.php/om...	ICAN000
6622607	https://www.goldcoastluxuryhomebuilders.com.au/web...	ICAN000
6622606	https://user7799874097892.af1.aapposet.com/james...	ICAN000
6622604	https://goldcoastships.com/daum/daum/login.p...	ICAN000
6622603	http://ten.asapipin.com/	ICAN000
6622602	https://freshhugplay.com/gdp/login.php?l=..._jmfP...	ICAN000
6622601	https://www.indiamartforetech.com/v/dqpc2hylene&omf...	ICAN000
6622600	http://wellobristan.com/Office/login.php?u1=..._KDF...	ICAN000
6622597	https://theaircity.com/BankofAmerica/bankofamer...	ICAN000
6622596	https://pymcars.com/one/OneDriveCloud/login.php/om...	ICAN000
6622595	http://kashmir-packages.com/-well-known/wp/login.p...	ICAN000
6622594	https://www.teagles.pro/links/	ICAN000