Cyber Security

BCA 305-5

Lab 3

Analyzing phishing domains using urlscan.io, including phishing campaign details, TTP (Tactics, Techniques, and Procedures), attribution, and similar campaigns.

1. Introduction

- **urlscan.io**: A public service for scanning and analyzing websites. It provides detailed reports about a URL, including IP addresses, domain info, visual snapshots, and more.
- **Phishing Domain**: A domain used to impersonate a trusted entity to deceive users into providing sensitive information.
- **TTP (Tactics, Techniques, and Procedures)**: Refers to how attackers conduct operations—useful for threat hunting and attribution.
- **Attribution**: Linking malicious activity to specific actors or campaigns using collected data.
- **Campaign Correlation**: Comparing phishing domains to identify similar infrastructure, visuals, or tactics used in multiple attacks.

2. Objectives

- Learn how to use urlscan.io for investigating phishing domains.
- Extract threat indicators such as URLs, IPs, ASNs, certificates, and HTML content.
- Identify and document phishing TTPs based on scans.
- Attempt attribution to known actors or campaigns using patterns.
- Correlate with other similar phishing domains or campaigns.

Python Setup

If you'd like to automate urlscan.io lookups:

Step 1: Install Requests

```
bash
pip install requests
```

Step 2: Set Up API Key

Create a .env file or secure storage for your urlscan.io API key.

Domain Analysis with urlscan.io

Step 1: Submit URL to urlscan.io

Use either the GUI at https://urlscan.io or API.

Using Python (API Submission):

```
python
import requests

API_KEY = 'your_api_key_here'
```

```
headers = {'API-Key': API_KEY, 'Content-Type': 'application/json'}
data = {"url": "http://suspicious-domain.com", "visibility": "public"}
response = requests.post("https://urlscan.io/api/v1/scan/", headers=headers,
json=data) print(response.json())
```

Step 2: Retrieve and Inspect Scan Results

Use the GUI or API to view detailed results.

Key Elements to Examine:

• **Visual Screenshot**: See if the page imitates brands (e.g., Microsoft, Google). • **Domain Info**: WHOIS, registrar, creation date — check for recently registered domains. • **HTML/JS Snippets**: Look for fake login forms, credential capture scripts. • **External Resources**: Embedded links, remote scripts (possible exfiltration). • **Network Info**: IP, ASN, geolocation — check if it's linked to known bad actors. • **Certificate Details**: TLS certificate reuse may connect to other campaigns.

Phishing Campaign Analysis

Step 3: Extract TTPs

Document observed attacker behavior. Example TTPs:

Tactic	**Technique**	**Example Observation**
Initial Access	Phishing via Email	URL embedded in phishing email
Credential Access	HTML Form Credential Harvesting	Fake login page replicating Microsoft login
Command & Control	Exfiltration via HTTP	Credentials sent to remote PHP script

Step 4: Attribution Clues

• **Domain Registrant Info**: Shared email or registrar name across domains • **Shared Infrastructure**: Same IPs, ASNs, or certificate reuse
• **Page Source Similarities**: Identical HTML/CSS layouts
• **Language/Metadata**: Comments or UI language hinting attacker origin

Step 5: Correlate with Similar Campaigns

• Use Search on urlscan.io with:

  • Keywords: login, secure, bank, account, microsoft

  - Domain patterns: .top, .xyz, recently registered
  - IP Address or Certificate fingerprints

- Look at the "**Related Scans**" section on each scan result page.
- Use services like VirusTotal, ThreatFox, or AbuseIPDB to validate findings.

Testing and Validation Tips

- Try submitting known phishing domains to practice identifying red flags.
- Compare a benign login page with a phishing one to spot differences. •
Use WHOIS history tools to validate registrant behaviors.
- Use multiple URLs from a campaign to connect infrastructure dots.

Best Practices

Practice	**Reason**
Use urlscan's public scans for threat hunting	Build broader understanding of phishing trends
Report identified phishing to abuse contacts or blocklists	Help the community stay safer
Store your analysis notes (IPs, hashes, domains)	Useful for future attribution and investigation
Use screenshots and HTML hashes for comparison	Helps correlate lookalike phishing campaigns
Cross-reference with other threat intel feeds	More context improves confidence in attribution

Use Case Examples

Use Case	**Technique**	**Description**
Phishing Analysis	urlscan.io, WHOIS, HTML analysis	Investigate fake login domains and look for reused infrastructure
Campaign Correlation	Certificate & IP reuse	Identify related phishing attempts by fingerprint
Threat Intel Sharing	TTPs + IOCs	Share findings with teams or external threat platforms
Automated Monitoring	urlscan API	Monitor for newly registered suspicious clones

Incident Response DNS/IP blocking Rapid action from phishing site detection