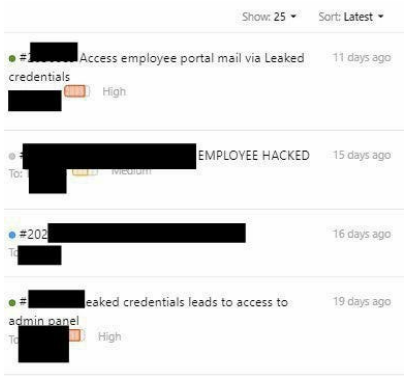
Using Dark Web in Bug Bounty

Muhammad Mater · Follow
5 min read · Jun 25

Hi Hackers ,

como estas ?

In this article, I'll talk about some findings and bugs that I've reported recently by using **CTI** and **Dark web**



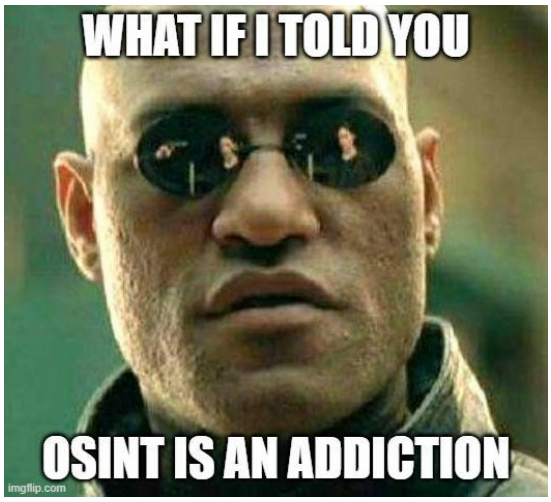
At first, I like to say that I love cybersecurity in every detail.

Offensive & Defensive

I like to understand most security tracks, whether offensive or defensive,

there are always some cross-skills that can be used for both defensive and offensive paths, like OSINT.

I learned Osint two years ago and became addicted to it



I loved to follow the threats that occurred and the breaches that occurred.

And I discovered that there is a cybersecurity path for these things called **CTI OR Cyber threat intelligence**

CTI refers to the knowledge and information about potential or ongoing cyber threats, including the tactics, techniques, and procedures (TTPs) used by threat actors. It involves collecting, analyzing, and disseminating actionable intelligence to organizations, enabling them to understand and mitigate risks posed by cyber threats.

CTI got me into the world of **Dark Web**

The dark web is a part of the internet that is intentionally hidden and accessible only through specific software, such as Tor . It is often associated with illegal activities, including the sale of stolen data, hacking tools, drugs, counterfeit goods, and various other illicit services.

The relationship between cyber threat intelligence and the dark web lies in the fact that the dark web is a common platform for threat actors to exchange information, tools, and services related to cyber threats. It serves as a marketplace for cybercriminals, where they can buy and sell valuable data, exploit kits, zero-day vulnerabilities,**Data Base** , and other resources that can be used in cyber attacks.

I wanted to know how this data is stolen and keep myself up2date with

The new threats and attack vectors and analyze them to understand how they target the victim.

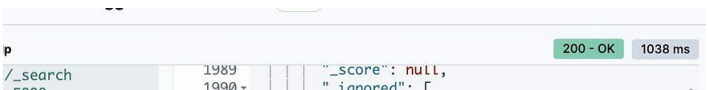
I'm starting to understand that there's some kind of malware called an info stealer

info stealer malware is a type of malicious software designed to infiltrate a victim's system and steal sensitive information.

It can capture data through methods such as keylogging, screen capturing, clipboard monitoring, form grabbing, and memory scraping.

Info stealers are typically distributed through malicious email attachments, compromised websites, or as payloads delivered by other malware.

In Bug Bounty Many tools like Cracked Burp suite is an infostealer malware

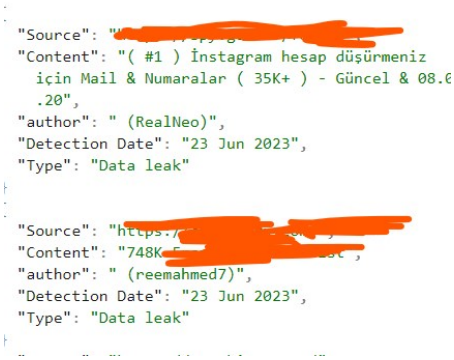


These Data belong to bug hunters hh

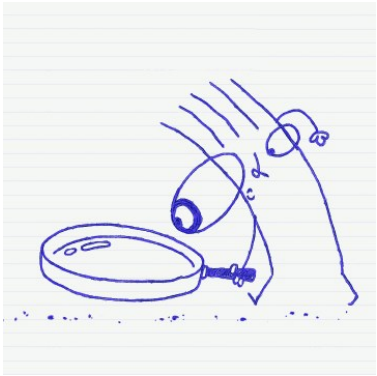
Hackers have been hacked

These stolen data are sold on the dark web or dark forums.

And I started to learn how can I collect & Monitor this data From The Dark web By Making Bot get data from dark and public web forums

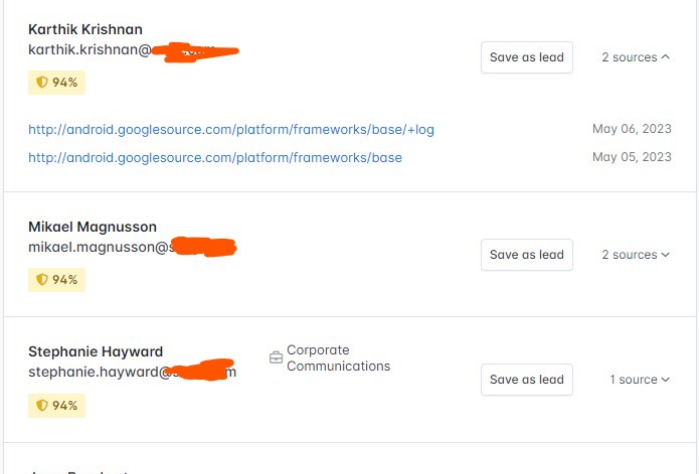


So I decided to use these data in bug bounty Because I'm a Bug hunter.



at first I tried this on vdp programs

So I started to target the emails of the company employees by a punch of search engines such as https://hunter.io/search/



get all emails for company employees

Then, I searched for any leaks for this Company or any old breach to the company,

And Get leaked data from dark web.

Ok How ?

To monitor the dark web:

Utilize dark web search engines like Grams, Torch, or Ahmia to find websites and hacking forums.

Leverage specialized dark web monitoring tools such as DarkOwl, Flashpoint, or Recorded Future to automate monitoring and analyze content.

There are paid products that offer this service
You can search the hacking forums as I did and used more than one forum to collect data

Exercise caution when joining dark web forums and communities, ensuring to prioritize legal and ethical practices and avoiding engagement in illegal activities or accessing illegal content.

check if any email in leak or not ,after get data with credentials

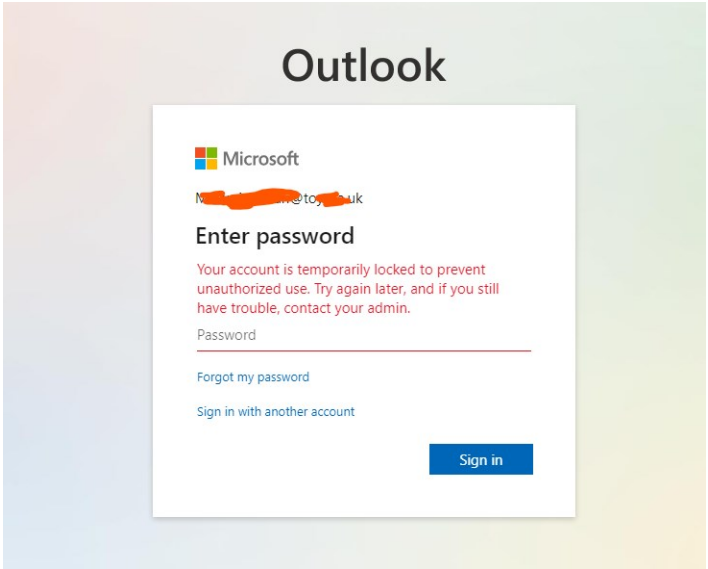
Next step is searching for any login portal using dorks

```
site:target.com inurl:"login"
```

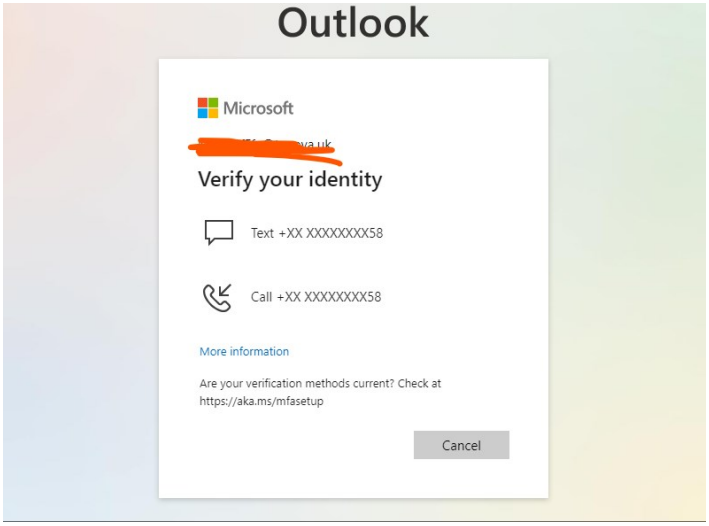
and tools such as https://github.com/Mr-Robert0/Logsensor ,

logsensor searches about any login panels of the target.

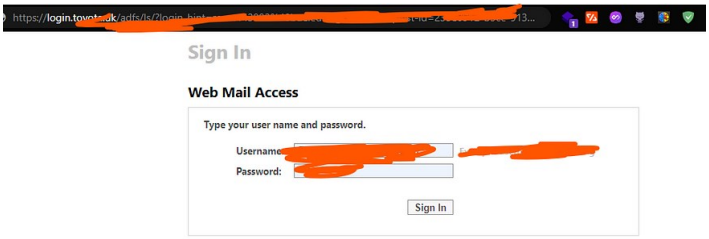
I tried to log in with almost all login panels and portals even the mail portal panel.



Again and Again



And Finally I hacked an employe



Another scenario that happened I reached the company's admin panel with one of the credentials.

There are some important tips to be mentioned :

1- not all programs will accept this as a bug, some of them will consider it as a NA or informative so make sure to understand the program policy.

2- most of triage team if they found out that the data is vailed they will ask for additional information to know the source of this information and how you got them :

Can you please provide additional details such as what method of OSINT did you use to identify this finding and what OSINT tool you used? Also, can you please provide steps to reproduce? " here you will just explain the whole process.

3- try to get impact of the data don't just report them.

I want to say a note:

I explained the idea to you and told you how to exploit it and get bounty from it

I did not publish names for hacking forums because this information can be misused away from Big Bounty or black hat activity

Thanks

My Linkedin : https://www.linkedin.com/in/micro0x00/

My Twitter : https://twitter.com/micro0x00

Support me :

https://www.buymeacoffee.com/Micro0x00

Hacking Darkweb Bug Bounty Bug Bounty Tips SEC

449 6

Written by Muhammad Mater

Follow

589 Followers

Just a Boy Loves Infosec (REDTEAM, CTI, OSINT, Bug Bounty)

More from Muhammad Mater

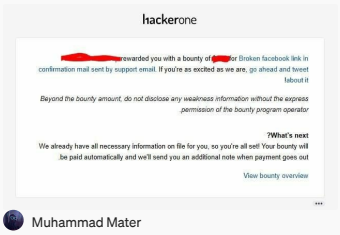
Muhammad Mater

Analyzing JavaScript Files To Find Bugs

Hi Hackers,

3 min read · May 23

436 5



Muhammad Mater

Easy Bugs Easy Bounty

Hi Hackers This is a Bug For beginner hackers and Bug Hunters to get their first valid bug or...

3 min read · Sep 30

116 2

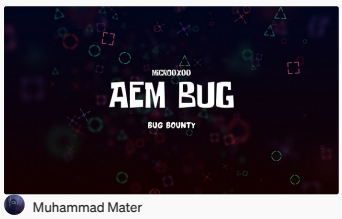
Muhammad Mater

CVE VS CWE VS ZERO DAY WHAT THESE THINGS

When I started cybersecurity, I was young, and I was afraid of shortcuts with 3 or 4 letters.

4 min read · Jun 5

77 2



Muhammad Mater

AEM Bug in Adobe

hi hackers

3 min read · May 21

99

See all from Muhammad Mater

Recommended from Medium

Shrirang Diwakar

Bypassing 403s like a PRO! ($2,100): Broken Access control

This article highlights my way of dealing with 403s and how I managed to get a P1 in...

3 min read · Apr 21

1.1K 8

Gokulvinesh

RCE | XSS via Image Exif metadata

Hello guys,

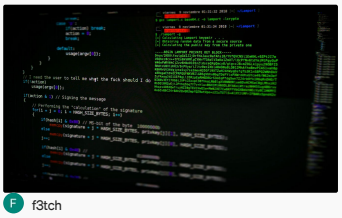
3 min read · Sep 13

132 1

Lists

Medium Publications Accepting Story Submissions

154 stories · 827 saves



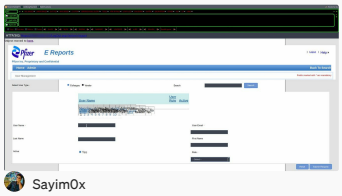
f3tch

My First Bug: A Unique $500 XSS.

whoami

4 min read · Jun 8

516 8



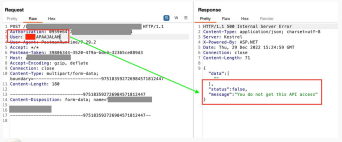
Sayim0x

Admin Panel Bypass without the credentials

Assalamu Alaikum, peace be upon you

2 min read · Jun 15

360 6



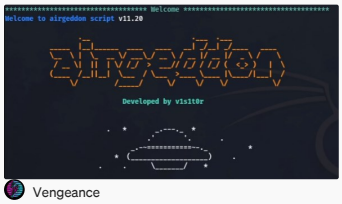
yoshi m lutfi in InfoSec Write-ups

SQL Injection in The HTTP Custom Header

It has been a long time since my last write-up. in this short write up I wanna share my last...

2 min read · Jun 14

546 3



Vengeance

Evil Twin Attack: Steal Wi-Fi Password

Cracking wifi password through a dictionary attack can only be successful if the password...

4 min read · Jul 5

141 1

See more recommendations