SPLUNK WEAPONISATION 2025/12/15

Weaponization

In the weaponization phase, the adversaries would:

- Create Malware / Malicious document to gain initial access / evade detection etc.
- Establish domains similar to the target domain to trick users.
- Create a Command and Control Server for the post-exploitation communication/activity etc.

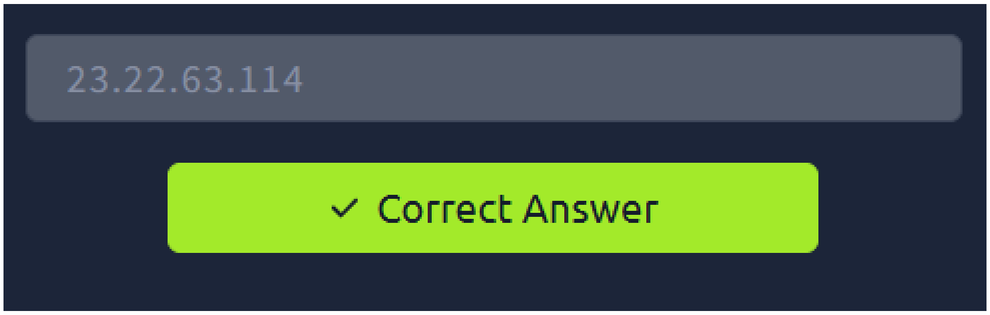
We have found some domains / IP addresses associated with the attacker during the investigations. This task will mainly look into OSINT sites to see what more information we can get about the adversary.

So far, we have found a domain prankglassinebracket.jumpingcrab.com associated with this attack. Our first task would be to find the IP address tied to the domains that may potentially be pre-staged to attack Wayne Enterprise.

In the following exercise, we will be searching the online Threat Intel sites for any information like IP addresses/domains / Email addresses associated with this domain which could help us know more about this adversary.

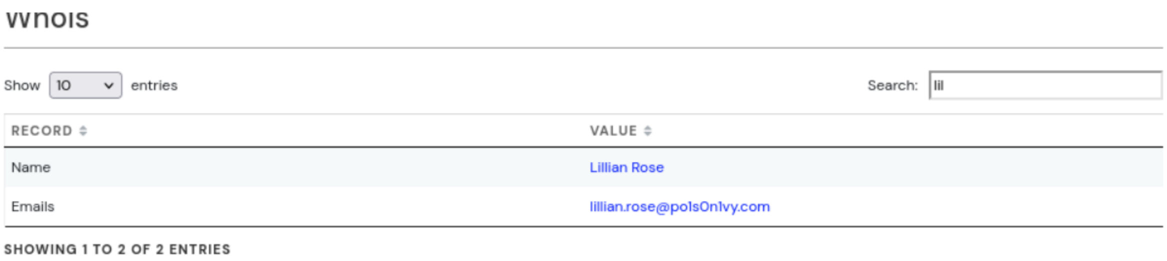
Robtex:
Robtex is a Threat Intel site that provides information about IP addresses, domain names, etc.

STEP 1: What IP address has P01s0n1vy tied to domains that are pre-staged to attack Wayne Enterprises?



23.22.63.114

STEP 2: Based on the data gathered from this attack and common open-source intelligence sources for domain names, what is the email address that is most likely associated with the P01s0n1vy APT group?



Whois

Show 10 entries   Search: lil

RECORD	VALUE
Name	Lillian Rose
Emails	lillian.rose@po1s0n1vy.com

SHOWING 1 TO 2 OF 2 ENTRIES

I opened up '**alienvault**' and looked up the domain www.po1s0n1vy.comand scrolled down and saw the name associated with it – **Lillian Rose.** I searched lil in the 'Whois' section and found the relevant email - **lillian.rose@po1s0n1vy.com.**

Conclusion Summary

In the Weaponization phase, the investigation focused on using open-source intelligence to profile the adversary's infrastructure and identify indicators linked to the attack. By analysing domains associated with the activity, including prankglassinebracket.jumpingcrab.com, threat intelligence platforms such as Robtex and AlienVault were used to uncover related IP addresses and attacker infrastructure. Further OSINT analysis identified **lillian.rose@po1s0n1vy.com** as the email address most likely associated with the P01s0n1vy APT group. These findings provide valuable insight into the attacker's preparation phase and help strengthen detection and attribution efforts.