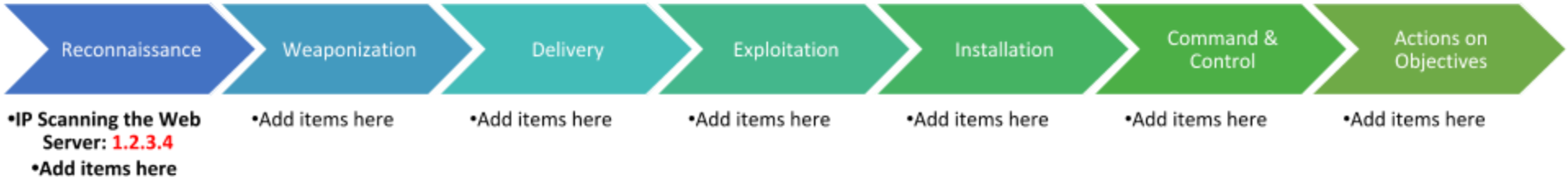
Summary of APT Group- PoisonIvy



(On this page provide more detailed notes about each item from above. An example is provided below.)

Report of the Cyber Kill Chain for APT Group PoisonIvy (P01s0n1vy)

Threat actor is APT Group known as PoisonIvy. PoisonIvy has defaced Wayne Enterprises web server. Below are the actions taken during each phase of the Cyber Kill Chain.

1) Reconnaissance
    a. Upon receiving the Index for Wayne Enterprises systems, I began searching for clues. Since PoisonIvy defaced the web server, I looked over the HTTP stream data by using the index=botsv1 sourcetype=stream:http. Upon looking over the source (src) data, I noticed that there were 3 IP addresses shown. After comparing these addresses with the Suricata data, I discovered that 40.80.148.42 appeared most often in those records. Therefore I believe 40.80.148.42 is responsible for scanning Wayne Enterprise's web server. **IP Address that scanned our Web Server: 40.80.148.42**
    b. As I searched through the source headers via HTTP, I began seeing that Acunetix, a content management system vulnerability scanner was being used to check over Joomla, Wayne Enterprises Content Management system. I saw that the IP source was reaching the destination on port 80.
    Acunetix was used to find vulnerabilities in Joomla.
    c. The destination IP that was accessed the most by the source IP 40.80.148.42 was 192.168.250.70, Wayne Enterprises web server. Looking via the intrusion detection system Suricata, I saw that the source IP was looking for directories on Joomla's PHP Component Index Search. Joomla was hosting imreallynotbatman.com and the components that might be active on Wayne Enterprises system via Joomla.
    The index.php has been scanned and altered by the source IP 40.80.148.42 responsible for scanning Wayne Enterprises' web server, 192.168.250.70.
    d. Looking at the http methods of the destination IP by statistical counting and sorting, I discovered that the administration page was attempted to be accessed 835 times that was being scanned by 40.80.148.42. By counting and sorting client side captures via http method 200, I discovered that many page URI's were successfully loaded from the destination IP and modified by the scanning IP 40.80.148.42.
    Multiple pages were successfully loaded with component access, suggesting that the address 40.80.148.42 is responsible for capturing and manipulating these pages.
2) Weaponization
    a. Using Robtex's IP index, I discovered that the IP address responsible for defacing the website, 23.22.63.114, is associated with multiple domain names, some of which look to belong to Wayne Enterprises. The malicious IP address, 23.22.63.114, according to Robtex, is associated with Wayne Enterprises domains and is also being routed by an AWS service provider in the Eastern Seaboard of the USA, specifically in Ashburn.
    The historical DNS records show that the IP 23.22.63.114 is associated with entities such as www.po1s0n1vy.com prankglassinebracket.jumpingcrab.com & po1s0n1vy.com.

b. Using Threatcrowd's visualization tool, as discovered using Splunk and Robtex, the IP address 23.22.63.114 is associated with multiple domain aliases such as www.po1s0n1vy.com prankglassinebracket.jumpingcrab.com & po1s0n1vy.com. E**mail addresses associated with the domain aliases I discovered were lillian.po1s0n1vy.com & lillian.rose@po1s0n1vy.com**

3) Delivery (wasn't sure about this phase, didn't see any of the PDF's that were labeled with this phase..?)
4) Exploitation
    a. I used a form data table to check login data from input forms on "imreallynotbatman.com". I found that multiple attempts were made to login using a multitude of different hashes and passwords. On the login form that was passed from the client browser to the web server, I used stat count to check what passwords were used with username "admin". I discovered that IP address 40.80.148.42 filled out username and password fields once, and 23.22.63.114 filled out password fields 412 times. There were 413 total attempts to access the "admin" account username and password.
    This suggests that 23.22.63.114 was used to initiate a "brute force" password attack. This will be detailed more in the Exploitation phase.
    b. I used a table to create new fields based on the password query; I searched the userpassword within a piped query- then created a stat count of the source IP by the field "userpassword" generated in the table query. I found that the password "batman" was used more than once, once by 23.22.63.114, once by 40.80.148.42 and is likely the password that garnered either IP address access to the server's content management system.
    Both external source addresses flagged by Suricata used the same password "batman" to access the administrative index page.
    c. Discovered that 23.22.63.114 initiated the most brute force attacks to gain access to administrative index.php- discovered sourcetype from streaming HTTP POST methods; looked at dest IP sources and did a stats count by source IP, saw more than double the amount of POSTS from this IP to the destination IP than GET requests.
    23.22.63.114 initiated multiple POST requests and likely is the IP address that discovered the password "batman" by brute force.
    d. Searching the HTTP POST methods and using a field to find form data, I searched for "userpassword" as the fieldname and used the functions search, eval, and stats to retrieve input form data within a table so as to evaluate the average password length using len, or length..
    The average password length was 6 characters across the organization Wayne Enterprises, suggesting that the required password policy is vulnerable to brute force attacks.
    e. I confirmed with a search for the password "batman" within the input form and created a table based on time that the source IP using the password "batman". The two IP addresses in question, from my previous investigation, accessed the index page on "imreallynotbatman.com" twice, within 2 minutes of each other on 08-10-2016. This indicates that the source IP address 23.22.63.114 was trying as many passwords with the username "admin" as possible, found the password through doing that, and then logged into the administrative index page with another IP address, 40.80.148.42. There was a duration between logins.
    The source IP 23.22.63.114 was the first of the two IP's to access the index page with the password "batman" at the time 9:46 PM. The second source IP 40.80.148.42 accessed the index page at 9:48 PM. The duration between those logins from different source IP's was 92 seconds.
5) Installation

a. I looked at the destination IP for events that have an executable file or patch with them. I used the intrusion detection system Suricata as the sourcetype and found two executable files that were detected as possibly malicious installation patches. Upon adding in the hostname into my query, a lookup on the POST methods that traveled to Wayne Enterprises web server, and the file info and file name of one of the possibly malicious executables, I found an additional binary code file that is a gateway to passing logs to the web server, as well as the source IP 40.80.148.42 that was listed in the field names as having posted the executable 3791.exe.
The source IP 40.80.148.42 is confirmed to be the ATP Group PoisonIvy, as the malicious executables detected by our sourcetype search within Suricata (intrusion detection system) were delivered to Wayne Enterprises web server from this source IP.

b. I began searching the botsv1 index for the command line that installed the executable 3791.exe. Since I didn't have access to the original source file, I knew it would be useful to utilize the hashes left behind by the executable for further investigation. There was one MD5 hash associated with the executable. I was able to derive this by creating a table of hashes piped from searching for the command line that executed 3791.exe.
I found that the MD5 hash of the uploaded executable by APT PoisonIvy was AAE3F5A29935E6ABCC2C2754D12A9AF0.

6) Command and Control

a. Looking at the malicious file within the firewalls logs and looking at the source and destinations, I discovered that the web server is hosting three instances of the same JPEG file, as seen previously as a defacement of the enterprises' website. The destination address the web server is communicating with is the same address from PoisonIvy that initiated the brute force attack. Looking at the URL field, I also discovered the website where this same JPEG file was also uploaded.
The source IP address 23.22.63.114 is the address that defaced the website, as it is clearly shown that three copies of the JPEG were event logged. 23.22.63.114 is what Wayne Enterprises' web server is actively communicating with. The website that the JPEG was from is prankglassinebracket.jumpingcrab.com:1337/poisonivy-is-coming-for-you-batman.jpeg.

7) Actions on Objectives

a. As I was searching the Suricata sourcetype and by changing the the dest_ip to src_ip for the webserver IP address being used in the sourcetype search and looking at the destination IP fields, I noticed that the webserver IP was communicating with external IPs outside of the network class organization. This is irregular. The web server should be listening for requests and only responding, not directly sending data out to an external IP address regularly. The intrusion detection system flagged a few URLs on the web server, one of those being the JPEG that defaced the website, and two other Joomla Component and gateway URLs. Looking at the HTTP stream, using the Wayne Enterprises' webserver as the source IP, and then checking the URI fields, I saw that the same PoisonIvy JPEG was included in the URI field name.
The web server's intrusion detection system flagged three URLs initiated by the web server, and even worse, the web server was sending out information to external addresses not within the Wayne Enterprise organization.

b. I decided to look at the Fortigate firewall logs on the web server's IP address. Looking at sources under the field names, I discovered that the same PoisonIvy IP addresses, 23.22.63.114 & 40.80.148.42, were shown. Additionally, to narrow down the large amount of results, I used a NOT logic statement to filter out any events in which the destination was the Wayne Enterprise web server. Looking at the category description field of the Fortigate logs, I can see that 3 out of 9 events are categorized as malicious websites. These labeled as such, include the PoisonIvy JPEG that belongs to the allowed category in policy.
This file, /poisonivy-is-coming-for-you-batman.jpeg is the file that is shown as the defacement of the Wayne Enterprises' website,

imreallynotbatman.com.