Q1

This is a simple question to get you familiar with submitting answers. What is the name of the company that makes the software that you are using for this competition? Just a six-letter word with no punctuation.

**Splunk**

Q2

What is the likely IP address of someone from the Po1s0n1vy group scanning imreallynotbatman.com for web application vulnerabilities?

**40.80.148.42**

Q3

What company created the web vulnerability scanner used by Po1s0n1vy? Type the company name. (For example, "Microsoft" or "Oracle")

**Acunetix**

Q4

What content management system is imreallynotbatman.com likely using? (Please do not include punctuation such as . , ! ? in your answer. We are looking for alpha characters only.)

**joomla**

Q5

What is the name of the file that defaced the imreallynotbatman.com website? Please submit only the name of the file with the extension (For example, "notepad.exe" or "favicon.ico").

**poisonivy-is-coming-for-you-batman.jpeg**

Q6

This attack used dynamic DNS to resolve to the malicious IP. What is the fully qualified domain name (FQDN) associated with this attack?

**prankglassinebracket.jumpingcrab.com**

Q7

What IP address has Po1s0n1vy tied to domains that are pre-staged to attack Wayne Enterprises?

**23.22.63.114**

Q8

Based on the data gathered from this attack and common open-source intelligence sources for domain names, what is the email address most likely associated with the Po1s0n1vy APT group?

**lillian.rose@po1s0n1vy.com**

Q9

What IP address is likely attempting a brute force password attack against imreallynotbatman.com?

**23.22.63.114**

Q10

What is the name of the executable uploaded by Po1s0n1vy? Please include the file extension. (For example, "notepad.exe" or "favicon.ico")

**3791.exe**

Q11

What is the MD5 hash of the executable uploaded?

**AAE3F5A29935E6ABCC2C2754D12A9AF0**

Q12

GCPD reported that common TTP (Tactics, Techniques, Procedures) for the Po1s0n1vy APT group, if initial compromise fails, is to send a spear-phishing email with custom malware attached to their intended target. This malware is usually connected to Po1s0n1vy's initial attack infrastructure. Using research techniques, provide the SHA256 hash of this malware.

**9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8**

Q13

What is the special hex code associated with the customized malware discussed in question 12? (Hint: It's not in Splunk)

**53 74 65 76 65 20 42 72 61 6e 74 27 73 20 42 65 61 72 64 20 69 73 20 61 20 70 6f 77 65 72 66 75 6c 20 74 68 69 6e 67 2e 20 46 69 6e 64 20 74 68 69 73 20 6d 65 73 73 61 67 65 20 61 6e 64 20 61 73 6b 20 68 69 6d 20 74 6f 20 62 75 79 20 79 6f 75 20 61 20 62 65 65 72 21 21 21**

Q14

One of Po1s0n1vy's staged domains has some disjointed "unique" whois information. Concatenate the two codes together and submit them as a single answer.

**31 73 74 32 66 69 6E 64 67 65 74 73 66 72 65 65 62 65 65 72 66 72 6F 6D 72 79 61 6E 66 69 6E 64 68 69 6D 74 6F 67 65 74**

Q15

What was the first brute force password used?

**12345678**

Q16

One of the passwords in the brute force attack is James Brodsky's favorite Coldplay song. Hint: we are looking for a six-character word on this one. Which is it?

**Yellow**

Q17

What was the correct password for admin access to the content management system running "imreallynotbatman.com"?

**batman**

Q18

What was the average password length used in the password brute-forcing attempt? (Round to a closest whole integer. For example "5" not "5.23213")

**6**

Q19

How many seconds elapsed between the brute force password scan identified the correct password and the compromised login? Round to 2 decimal places.

**92.17**

Q20

How many unique passwords were attempted in the brute force attempt?

**412**

Q21

What was the most likely IP address of we8105desk in 24AUG2016?

**192.168.250.100**

Q22

Amongst the Suricata signatures that detected the Cerber malware, which one alerted the fewest number of times? Submit ONLY the signature ID value as the answer. (No punctuation, just 7 integers.)

**2816763**

Q23

What fully qualified domain name (FQDN) makes the Cerber ransomware attempt to direct the user to at the end of its encryption phase?

**cerberhhyed5frqa.xmfir0.win**

Q24

What was the first suspicious domain visited by we8105desk in 24AUG2016?

**solidaritedeproximite.org**

Q25

During the initial Cerber infection a VB script is run. The entire script from this execution, pre-pended by the name of the launching .exe, can be found in a field in Splunk. What is the length in characters of the value of this field?

**4490**

Q26

What is the name of the USB key inserted by Bob Smith?

**MIRANDA\_PRI**

Q27

Bob Smith's workstation (we8105desk) was connected to a file server during the ransomware outbreak. What is the IP address of the file server?

**192.168.250.20**

Q28

How many distinct PDFs did the ransomware encrypt on the remote file server?

**257**

Q29

The VBScript found in question 25 launches 121214.tmp. What is the ParentProcessId of this initial launch?

**3968**

Q30

The Cerber ransomware encrypts files located in Bob Smith's Windows profile. How many .txt files does it encrypt?

**406**

Q31

The malware downloads a file that contains the Cerber ransomware crypto code. What is the name of that file?

**mhtr.jpg**

Q32

Now that you know the name of the ransomware's encryptor file, what obfuscation technique does it likely use?

**Steganography**