A pixel art of a christmas wreath

Description automatically generated

# Bournemouth 2600 Xmas Challenge Answers

## Challenge 1 – Posh Christmas Tree

**Steps:**

1. Find the secret QR code in the image
2. Decode the Base64 Code that decodes to an AppAnyRun link
3. Find the PowerShell script that produced a glowing Christmas tree
4. Inspect the PowerShell script and find another base64 code
5. Decode the base64 and find the flag

**Answers:**

* Base64 code: aHR0cHM6Ly9hcHAuYW55LnJ1bi90YXNrcy82YzY5YjA1YS04MDY2LTQxMmEtYjQ0MS0yY2ZlNWE3NjRjZWU=
* AnyRun link: <https://app.any.run/tasks/6c69b05a-8066-412a-b441-2cfe5a764cee>
* 2nd Base64 code: Q29uZ3JhdHMhIFlvdSBmb3VuZCB0aGUgZmxhZzogQnVzaGlkb19pc18xMzM3
* Flag: Bushido\_is\_1337

## Challenge 2 – Packets for Presents

**PCAP ccda62b0-4607-4670-bd19-9823687bdf25**

1. Download the PCAP
2. Search for SMTP packets
3. Follow the tcp stream
4. Find the connections to the domain

A screenshot of a computer

Description automatically generated

Answer: educt[.]shop

**PCAP cbfd7146-bf87-4356-9551-9ecbcdf28344**

1. Download the PCAP
2. Search for FTP packets
3. Follow the tcp stream
4. Find the authentication process for the FTP server and view the credentials

A screenshot of a computer

Description automatically generated

Answer: ro}UWgz#!38E

## Challenge 3 – Ransomware for Christmas

Q1. Which Japanese company was a victim to ransomware in August 2023?

A1. Seiko (Google Search or use Ransomware.live)

* <https://www.bleepingcomputer.com/news/security/seiko-says-ransomware-attack-exposed-sensitive-customer-data/>
* <https://www.ransomware.live/id/U2Vpa28gR3JvdXAgQ29ycG9yYXRpb25AYWxwaHY=>

Q2. Which ransomware group attacked that company?

A2. ALPHV (read articles about the Seiko attack or use Ransomware.live)

* <https://www.ransomware.live/group/alphv>
* <https://www.bleepingcomputer.com/news/security/japanese-watchmaker-seiko-breached-by-blackcat-ransomware-gang/>

Q3. Which initial access broker offered access to the victim company?

A3. AliceWonderland (find the answer in the BleepingComputer article)

* <https://www.bleepingcomputer.com/news/security/japanese-watchmaker-seiko-breached-by-blackcat-ransomware-gang/>

Q4. Which Forum did the initial access broker make post on?

A4. Exploit[.]in (research cybercrime forums and look for initial access brokers and match the format/layout of posts)

## Challenge 4 – Bitcoin Barons

Q1. How much Bitcoin did Akira receive in total from the six addresses associated with them?

<https://www.ransomware.live/group/akira#btc>

Answer:

* Using Blockchain.com and looking at the Total Received amount
* bc1q6dqe4esmqejmxhpj95qadv0j4clsqcxxp4cd94 = 1.72325000 BTC
* bc1qandfxc4knaf943njca77edl9mmegzs83tv8lpx = 2.41407011 BTC
* bc1qr0pqfghr9cksfc5arr2rak3lt2y50v03pc76nh = 38.55847013 BTC
* bc1qpwwtck0zhzrj56fxeayz6wz5546nlp607qzpvh = 3.95475769 BTC
* bc1qghj85gz0dkr9jeucana3z4xu50ujtllj50rvj0 = 2.98600000 BTC
* bc1qcnw5v94y40ast06eatgalnjpluu2p067qewh46 = 3.69315708 BTC
* Total = 53.32970501 BTC (roughly $5m USD)

## Challenge 5 – IOCs for Pudding

Download the list of indicators of compromise (IOCs) from the GitHub

<https://github.com/Bournemouth2600/XmasChallenge>

1. 37.191.122[.]186 - FANCY BEAR - <https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf>
2. 45.85.76[.]10 - APT41 - <https://blog.talosintelligence.com/chinese-hacking-group-apt41-compromised-taiwanese-government-affiliated-research-institute-with-shadowpad-and-cobaltstrike-2/>
3. east-healthy-dress[.]glitch[.]me - CHARMING KITTEN - <https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/>
4. sesorin[.]lol - APT43 - <https://services.google.com/fh/files/misc/apt43-report-en.pdf>
5. 78d75669390e4177597faf9271ce3ad3a16a3652e145913dbfa9a5951972fcb0 - Akira - <https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/>
6. b6e82a4e6d8b715588bf4252f896e40b766ef981d941d0968f29a3a444f68fef - SCATTERED SPIDER - <https://www.crowdstrike.com/en-us/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/>

The rest of the IOCs came from this GitHub repository: <https://github.com/executemalware/Malware-IOCs/>

[VirusTotal - Collections - 4bce0e7f08c56b459c13b770d225fd1456c5b41f2bd62473f28e007f58943324](https://www.virustotal.com/gui/collection/4bce0e7f08c56b459c13b770d225fd1456c5b41f2bd62473f28e007f58943324/iocs)

[VirusTotal Graph](https://www.virustotal.com/graph/gf20bd62dd14145a78d7f4b213eec408fdabea28d661345eebb14172c4a888b53)

[LevelBlue - Open Threat Exchange](https://otx.alienvault.com/pulse/6743340922e24b160d55142a/)