LET HIM COOK: CYBERCHEF WORKSHOP

1 August 2025

Will Thomas
B2600 Goat & Tricycle

1) List all the CVEs from the RansomHub Alert

CyberChef Recipe – see here

RansomHub Alert: #StopRansomware: RansomHub Ransomware | CISA

Key Takeaway: Learning to use Regular Expression (Regex)

---

2) List all the Domains from the CISA Alerts

CyberChef Recipe – see here

RansomHub Alert: #StopRansomware: RansomHub Ransomware | CISA

GRU Alert: Russian GRU Targeting Western Logistics Entities and Technology Companies | CISA

Key Takeaway: Combining Regex with Fang/Defang URLs and Filters

---

3) Extract all IPs from the Shodan Scan Result

CyberChef Recipe – see here

Shodan Scan Results: Bournemouth2600/LetHimCook: CyberChef Workshop

Enrich results in bulk: Domain and IP bulk lookup tool

Key Takeaway: Extracting IPs from “large” files

---

4) Extracting IPs from CERT-UA Alerts and format to Query Language

CyberChef Recipe – see here

CERT-UA Alerts: CERT-UA

Key Takeway: Extracting IPs and using Regex to fit Query Language for SIEM or CTI tool

---

5) Decode Encoded PowerShell Commands run by Malware Part 1

CyberChef Recipe – see here

Malicious PowerShell Script: LetHimCook/mal_powershell.md at main · Bournemouth2600/LetHimCook

Key Takeaway: Decoding obfuscated commands and extracting additional IOCs

---

6) Decoding Encoded PowerShell Commands run by Malware Part 2

CyberChef Recipe – see here

Malicious PowerShell Script: LetHimCook/mal_powershell_2.md at main · Bournemouth2600/LetHimCook

Key Takeaway: Remove null bytes from commands and extracting additional IOCs

---

7) Generate & Parse QR codes

CyberChef Recipe – see here

Malicious QR code phishing PDF file: https://app.any.run/tasks/e0581063-d055-4029-9166-7a74e469d16e

Key Takeaway: Extract links from QR codes instead of scanning/visiting them on endpoints

Try Next: Parsing conference badge QR codes and viewing the data stored there

---

8) Extract EXIF from images/docs

CyberChef Recipe – see here

Image with Exif: LetHimCook/leaf.jpg at main · Bournemouth2600/LetHimCook

Key Takeaway: It is possible to identify which device took the image using the EXIF data

Try Next: Take a picture from your mobile device and upload it to CyberChef to view the EXIF

---

9) Generate Hashes from Files

CyberChef Recipe – see here

ELF Malware Sample: LetHimCook/LIMPOPOx32.bin.zip at main · Bournemouth2600/LetHimCook

Key Takeaway: How to generate unique hashes of files

Try Next: Copying the hashes and searching for them in sites like VirusTotal or AnyRun

---

10) Visualise Entropy

CyberChef Recipe – see here

Key Takeaway: Identify if a file is heavily obfuscated or not

---

11) Create and Test YARA rules for detecting File Content

CyberChef Recipe – see here

YARA Rule: LetHimCook/ELF_malware_sample.yar at main · Bournemouth2600/LetHimCook

Key Takeaway: You can test writing YARA rules using CyberChef

Try Next: Running strings against a file and using those to write a YARA rule and then testing the YARA against a file.

---

12) IOC Extraction from PCAP files

a) CyberChef Recipe – see here

b) CyberChef Recipe - see here

PCAP File: LetHimCook/cbfd7146-bf87-4356-9551-9ecbcdf28344.pcap at main · Bournemouth2600/LetHimCook

Key Takeaway: Speed up analysis of PCAP files without even opening Wireshark

Try Next: Analysing the PCAP in Wireshark and looking for the mentions of the Domain

---

Further Reading

1. https://isc.sans.edu/diary/CyberChef+Entropy/29352
2. https://isc.sans.edu/diary/Excel+4+Emotet+Maldoc+Analysis+using+CyberChef/28830
3. https://isc.sans.edu/diary/CyberChef+Entropy/29352