

The background of the image is a dark, atmospheric scene of a lighthouse at night. The lighthouse is positioned on a rocky shore in the foreground, with its beam of light sweeping across the dark, misty sky and illuminating the peaks of distant mountains. The overall mood is mysterious and guiding.

100 Security Tools - more or less

Tools you use every day, or at least you should be!

by Josh Galvez - aka Zevlag

Josh Galvez

zevlag

- Offensive Security Operator at LogMeln
- In the Security industry for 15 years
- DEFCON 25 Black Badge
- DEFCON 29 Black Badge
- SAINTCON 2014 Black Badge



A dense forest scene with tall, thin trees covered in bright yellow autumn leaves. Sunlight filters through the canopy, creating a warm glow and casting long shadows on the ground. The forest floor is covered with fallen leaves.

Network

Nmap

Network Mapper

```
[zevlag@Z314 ~ % nmap -v -A webplay.hackerschallenge.org
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-20 22:59 MDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:59
Completed NSE at 22:59, 0.00s elapsed
Initiating NSE at 22:59
Completed NSE at 22:59, 0.00s elapsed
Initiating NSE at 22:59
Completed NSE at 22:59, 0.00s elapsed
Initiating Ping Scan at 22:59
Scanning webplay.hackerschallenge.org (54.212.225.228) [2 ports]
Completed Ping Scan at 22:59, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:59
Completed Parallel DNS resolution of 1 host. at 22:59, 0.17s elapsed
Initiating Connect Scan at 22:59
Scanning webplay.hackerschallenge.org (54.212.225.228) [1000 ports]
Discovered open port 22/tcp on 54.212.225.228
Completed Connect Scan at 23:00, 9.22s elapsed (1000 total ports)
Initiating Service scan at 23:00
Scanning 1 service on webplay.hackerschallenge.org (54.212.225.228)
Completed Service scan at 23:00, 0.11s elapsed (1 service on 1 host)
NSE: Script scanning 54.212.225.228.
Initiating NSE at 23:00
Completed NSE at 23:00, 1.22s elapsed
Initiating NSE at 23:00
Completed NSE at 23:00, 0.00s elapsed
Initiating NSE at 23:00
Completed NSE at 23:00, 0.00s elapsed
Nmap scan report for webplay.hackerschallenge.org (54.212.225.228)
Host is up (0.041s latency).
rDNS record for 54.212.225.228: ec2-54-212-225-228.us-west-2.compute.amazonaws.com
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE     SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 2b:39:30:00:08:64:5d:8a:2a:4f:07:7f:ae:f0:89:c9 (RSA)
|   256 f3:42:d3:d8:fd:d5:6c:91:a6:e5:5f:1e:19:96:e8:58 (ECDSA)
|_  256 c0:98:c1:81:c0:62:86:a4:42:d7:24:91:d5:24:e5:b1 (ED25519)
25/tcp    filtered  smtp
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
587/tcp   filtered submission
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 23:00
Completed NSE at 23:00, 0.00s elapsed
Initiating NSE at 23:00
Completed NSE at 23:00, 0.00s elapsed
Initiating NSE at 23:00
Completed NSE at 23:00, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.51 seconds
```

Nmap

Scan for active IP's:
nmap -sn 192.168.0.0/24

Scan for Operating Systems:
nmap -O 192.168.0.164

Scan it all, and do it fast:
nmap -T4 -A 192.168.0.0/24

Be More Verbose:
nmap -v

Wireshark

Wi-Fi: en0

Apply a display filter ...<⌘/>>

Time	Source	Destination	Protocol	Length	Info
801 15.761983	172.20.5.83	142.250.101.108	TCP	78	50746 → 993 [SYN, ECN, CWR] Seq=0 Win=65535 Len=
802 15.762607	172.20.5.83	142.250.101.108	TCP	78	50747 → 993 [SYN, ECN, CWR] Seq=0 Win=65535 Len=
803 15.763073	172.20.5.83	142.250.101.108	TCP	78	50748 → 993 [SYN, ECN, CWR] Seq=0 Win=65535 Len=
804 15.764772	172.20.0.1	172.20.5.83	DNS	158	Standard query response 0x01bb HTTPS www.apache.org
805 15.782763	172.20.5.83	172.20.0.1	DNS	78	Standard query 0x2930 HTTPS gateway.icloud.com
806 15.782929	172.20.5.83	172.20.0.1	DNS	78	Standard query 0xccbb A gateway.icloud.com
807 15.788693	142.250.101.108	172.20.5.83	TCP	74	993 → 50737 [SYN, ACK, ECN] Seq=0 Ack=1 Win=65535
808 15.788787	172.20.5.83	142.250.101.108	TCP	66	50737 → 993 [ACK] Seq=1 Ack=1 Win=131840 Len=0
809 15.789368	172.20.5.83	142.250.101.108	TLSv1.2	240	Client Hello
810 15.792463	142.250.101.108	172.20.5.83	TCP	74	993 → 50739 [SYN, ACK, ECN] Seq=0 Ack=1 Win=65535
811 15.792544	172.20.5.83	142.250.101.108	TCP	66	50739 → 993 [ACK] Seq=1 Ack=1 Win=131840 Len=0
812 15.792975	172.20.5.83	142.250.101.108	TLSv1.2	240	Client Hello
813 15.793128	142.250.101.108	172.20.5.83	TCP	74	993 → 50738 [SYN, ACK, ECN] Seq=0 Ack=1 Win=65535
814 15.793130	142.250.101.108	172.20.5.83	TCP	74	993 → 50745 [SYN, ACK, ECN] Seq=0 Ack=1 Win=65535
815 15.793196	172.20.5.83	142.250.101.108	TCP	66	50738 → 993 [ACK] Seq=1 Ack=1 Win=131840 Len=0
816 15.793196	172.20.5.83	142.250.101.108	TCP	66	50745 → 993 [ACK] Seq=1 Ack=1 Win=131840 Len=0

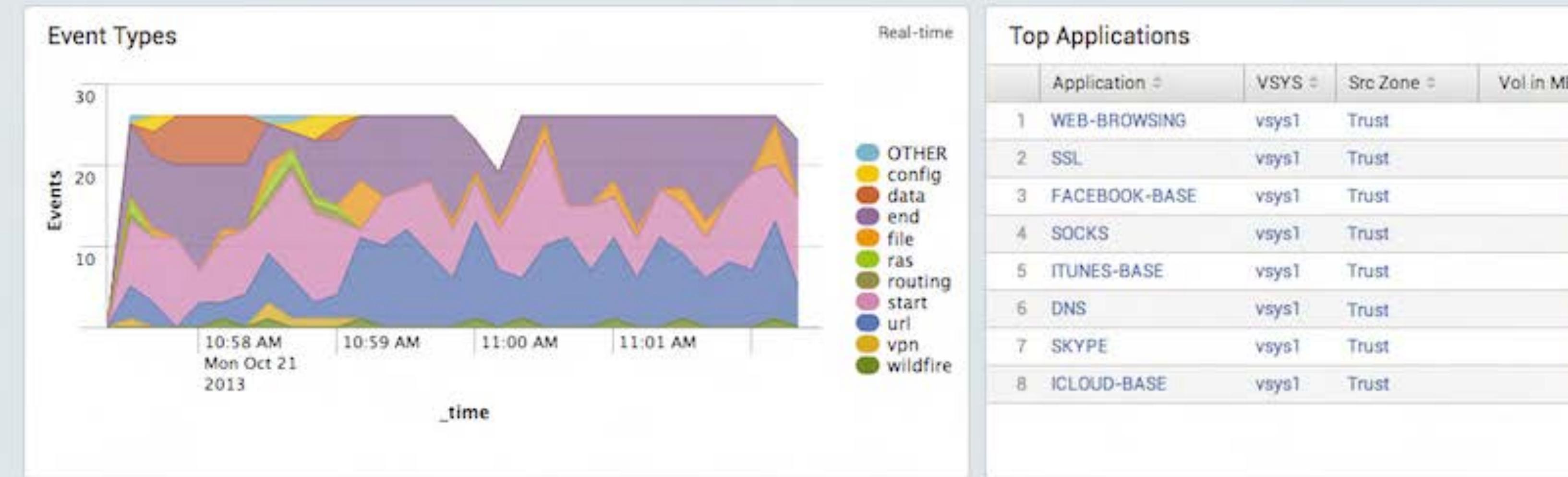
Frame 804: 158 bytes on wire (1204 bits), 158 bytes captured (1204 bits) on interface en0, 10:00:50:e8:04:41 → 00:b3:d4:43:1b (Nomadix_04:41:4d [eth0] > Apple_d4:43:1b [en0])
Ethernet II, Src: Nomadix_04:41:4d (00:50:e8:04:41:4d), Dst: Apple_d4:43:1b (c4:b3:01:d4:43:1b)
Internet Protocol Version 4, Src: 172.20.0.1, Dst: 172.20.5.83
User Datagram Protocol, Src Port: 53, Dst Port: 63182
Domain Name System (response)
 Transaction ID: 0x01bb
 Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 0
 Authority RRs: 1
 Additional RRs: 0
 Queries
 www.apache.org: type HTTPS, class IN
 Name: www.apache.org
 [Name Length: 14]
 [Label Count: 3]
 Type: HTTPS (HTTPS Specific Service Endpoints) (65)
00 c4 b3 01 d4 43 1b 00 50 e8 04 41 4d 08 00 45 00 ..C..P..AM..E.
10 00 90 00 00 40 00 38 11 e4 e0 ac 14 00 01 ac 14 ..@8.....
20 05 53 00 35 f6 ce 00 7c ce 45 01 bb 81 80 00 01 S.5...|..E..
30 00 00 00 01 00 00 03 77 77 77 06 61 70 61 63 68 ..W..WW..APACH..
40 65 03 6f 72 67 00 00 41 00 01 c0 10 00 06 00 01 e..ORG..A..
50 00 00 03 84 00 48 06 6e 73 2d 35 35 38 09 61 77 ..H..N..S-558..AW..
60 73 64 6e 73 2d 30 35 03 6e 65 74 00 11 61 77 73 sdns-05..NET..AWS..
70 64 6e 73 2d 68 6f 73 74 6d 61 73 74 65 72 06 61 dns-host master..A..

wireshark_Wi-FiJVBTB1.pcapng

Packets: 3001 · Displayed: 3001 (100.0%) · Dropped: 0

Defensive

Overview



Autopsy

Digital forensics platform

case1 - Autopsy 3.1.2

File View Tools Window Help

Close Case Add Data Source Generate Report

Directory Listing
Recent Documents
Table Thumbnail

Source File Path Date/Time

Source File	Path	Date/Time
howdy.txt.lnk	C:\Users\Autopsy\Documents\howdy.txt.txt	2014-03-10 12:
100_6259.lnk	C:\Users\Autopsy\Desktop\100_6259.JPG	2014-03-14 16:
1978871_10152107173663113_2060708596.lnk	C:\Users\Autopsy\Desktop\1978871_10152107173663113_2060708...	2014-03-10 14:
840451_1.lnk	C:\Users\Autopsy\Desktop\840451_1.jpg	2014-03-10 17:
ActiveSync.lnk	E:\Mobile Device Forensic Challenge\SEC563-Capstone-WindowsMobil...	2014-03-10 16:
Alouette_14kb.lnk	E:\Mobile Device Forensic Challenge\SEC563-Capstone-WindowsMobil...	2014-03-10 16:
Calendar.lnk	E:\Mobile Device Forensic Challenge\SEC563-Capstone-Nokia-6610\N...	2014-03-10 16:
DCode-v4.02a-build-4.02.0.9306.lnk	C:\Users\Autopsy\Desktop\DCode-v4.02a-build-4.02.0.9306.zip	2014-03-10 16:
E2.lnk	E:\E2.bmp	2014-03-10 12:
E3.lnk	E:\E3.bmp	2014-03-10 12:
My Videos.lnk	E:\Mobile Device Forensic Challenge\SEC563-Capstone-WindowsMobil...	2014-03-10 16:
Nokia 6610 XRY Report.lnk	E:\Mobile Device Forensic Challenge\SEC563-Capstone-Nokia-6610\N...	2014-03-10 16:
Open-count.lnk	E:\Mobile Device Forensic Challenge\SEC563-Capstone-WindowsMobil...	2014-03-10 16:
Removable Disk (E).lnk	E:\	2014-03-10 12:
SEC563-Capstone-Nokia-6610.lnk	E:\Mobile Device Forensic Challenge\SEC563-Capstone-Nokia-6610	2014-03-10 16:
What is Second Life_Second Life.lnk	C:\Users\Autopsy\Desktop\What is Second Life_Second Life.mp4	2014-03-10 16:
XACT Log.lnk	E:\Mobile Device Forensic Challenge\SEC563-Capstone-Nokia-6610\X...	2014-03-10 16:

Hex Strings Metadata Results Text Media Video Triage

Page: 1 of 1 Page Go to Page: []

Hex	Strings	Metadata	Results	Text	Media	Video Triage
0x00000000: 4C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00	L.....					
0x00000010: 00 00 00 46 83 00 20 00 10 00 00 00 40 01 E0 0B	...F.....@..					
0x00000020: 39 98 CD 01 00 58 68 B7 C6 97 CD 01 00 4D DD 0C	9....Xh.....M..					
0x00000030: 39 98 CD 01 00 00 00 00 00 00 00 00 01 00 00 00	9.....					
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 9B 01 14 00					
0x00000050: 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30	P.O. ..i.....+0					
0x00000060: 30 9D 19 00 2F 45 3A 5C 00 00 00 00 00 00 00 00	0.../E:\.....					
0x00000070: 00 00 00 00 00 00 00 00 00 00 8A 00 31 00 001..					
0x00000080: 00 00 00 35 41 B8 A4 10 00 4D 4F 42 49 4C 45 7E	...5A....MOBILE~					
0x00000090: 31 00 00 72 00 09 00 04 00 EF BE 35 41 B8 A4 35	1..r.....5A..5					
0x000000a0: 41 00 38 2E 00 00 00 60 DC 03 00 00 00 00 00 00	A.8.....`.....					
0x000000b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					
0x000000c0: 00 4D 00 6F 00 62 00 69 00 6C 00 65 00 20 00 44	M.o.b.i.l.e..D					
0x000000d0: 00 65 00 76 00 69 00 63 00 65 00 20 00 46 00 6F	e.v.i.c.e..F.o					
0x000000e0: 00 72 00 65 00 6E 00 73 00 69 00 63 00 20 00 43	r.e.n.s.i.c..C					
0x000000f0: 00 68 00 61 00 6C 00 6C 00 65 00 6E 00 67 00 65	h.a.l.l.e.n.g.e					
0x00000100: 00 00 00 18 00 84 00 31 00 00 00 00 00 35 41 B81.....5A..					
0x00000110: A4 10 00 53 45 43 35 36 33 7E 31 00 00 6C 00 09	...SEC563~1..1..					
0x00000120: 00 04 00 EF BE 35 41 B8 A4 35 41 00 38 2E 00 005A..5A.8...					
0x00000130: 00 E0 10 04 00 00 00 00 00 00 00 00 00 00 00 00					

Volatility Memory Forensics

```
volpypy [jelle@lab-linux -]s vol.py linux sshkeys -n sshd
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.ssdt (NameError: global name 'distorm3' i
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No modu
*** Failed to import volatility.plugins.malware.apihooks (NameError: global name
*** Failed to import volatility.plugins.malware.threads (NameError: global name '
```



OpenSSH end to end encryption key dumper
By Jelle Vergeer

Scanning for OpenSSH sshenc structures...

Name	Pid	PPid	Address	Name
	5743	1	0x0000000018fd548	chacha20-poly
	5743	1	0x0000000018fd690	chacha20-poly
sshd [sshd: root@pts/0]	10009	4977	0x00007f1f4871ebd0	aes128-ctr
sshd [sshd: root@pts/0]	10009	4977	0x00007f1f4871ee10	aes128-ctr
sshd [sshd: root@pts/1]	10052	4977	0x00007fea8857b2e0	aes256-ctr
sshd [sshd: root@pts/1]	10052	4977	0x00007fea8857c9d0	aes256-ctr
sshd [sshd: root@pts/3]	10206	4977	0x00007fdc156a6c00	aes128-ctr
sshd [sshd: root@pts/3]	10206	4977	0x00007fdc156a6e40	aes128-ctr
sshd [sshd: root@pts/4]	31148	4977	0x00007f43f2cd1bd0	aes128-ctr
sshd [sshd: root@pts/4]	31148	4977	0x00007f43f2cd1e10	aes128-ctr
sshd [sshd: root@pts/2]	31332	4977	0x00007f13ffcf8a80	aes128-ctr
sshd [sshd: root@pts/2]	31332	4977	0x00007f13ffcf8cc0	aes128-ctr
sshd [sshd: root@pts/5]	31362	4977	0x00007f66a3b36c10	aes128-ctr
sshd [sshd: root@pts/5]	31362	4977	0x00007f66a3b36e50	aes128-ctr

LiME

Linux Memory Extractor

```
r00t@r00t-KitPloit: ~
$ adb push lime.ko /sdcard/lime.ko
$ adb forward tcp:4444 tcp:4444
$ adb shell
$ su
# insmod /sdcard/lime.ko "path=tcp:4444 format=lime"

Now on the host machine, we can establish the connection and ac...
r00t@r00t-KitPloit: ~
$ nc localhost 4444 > ram.lime

Acquiring to sdcard
r00t@r00t-KitPloit: ~
# insmod /sdcard/lime.ko "path=/sdcard/ram.lime format=lime"
```

WinPmem

Windows Memory

Extractor



Nessus Vulnerability Assessment

localhost [Configure](#) [Audit Trail](#)

[Back to My Scans](#)

Hosts 1 | Vulnerabilities 21

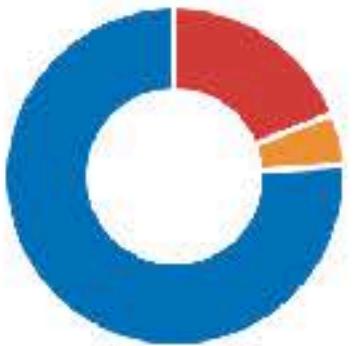
Filter ▾ Search Vulnerabilities: 21 Vulnerabilities

Sev	Name	Family	Count	Actions
CRITICAL	Mozilla Firefox (Multiple Issues)	MacOS X Local Security Checks	36	View Edit
CRITICAL	Microsoft Office (Multiple Issues)	MacOS X Local Security Checks	19	View Edit
CRITICAL	Wireshark (Multiple Issues)	MacOS X Local Security Checks	10	View Edit
CRITICAL	Oracle VM VirtualBox (Multiple Issues)	Misc.	3	View Edit
HIGH	Apple Mac OS X (Multiple Issues)	MacOS X Local Security Checks	5	View Edit
INFO	SSH (Multiple Issues)	General	4	View Edit
INFO	Authenticated Check : OS Name and Installed Package Enumeration	Settings	1	View Edit
INFO	Common Platform Enumeration (CPE)	General	1	View Edit
INFO	Device Hostname	General	1	View Edit
INFO	Device Type	General	1	View Edit

Scan Details

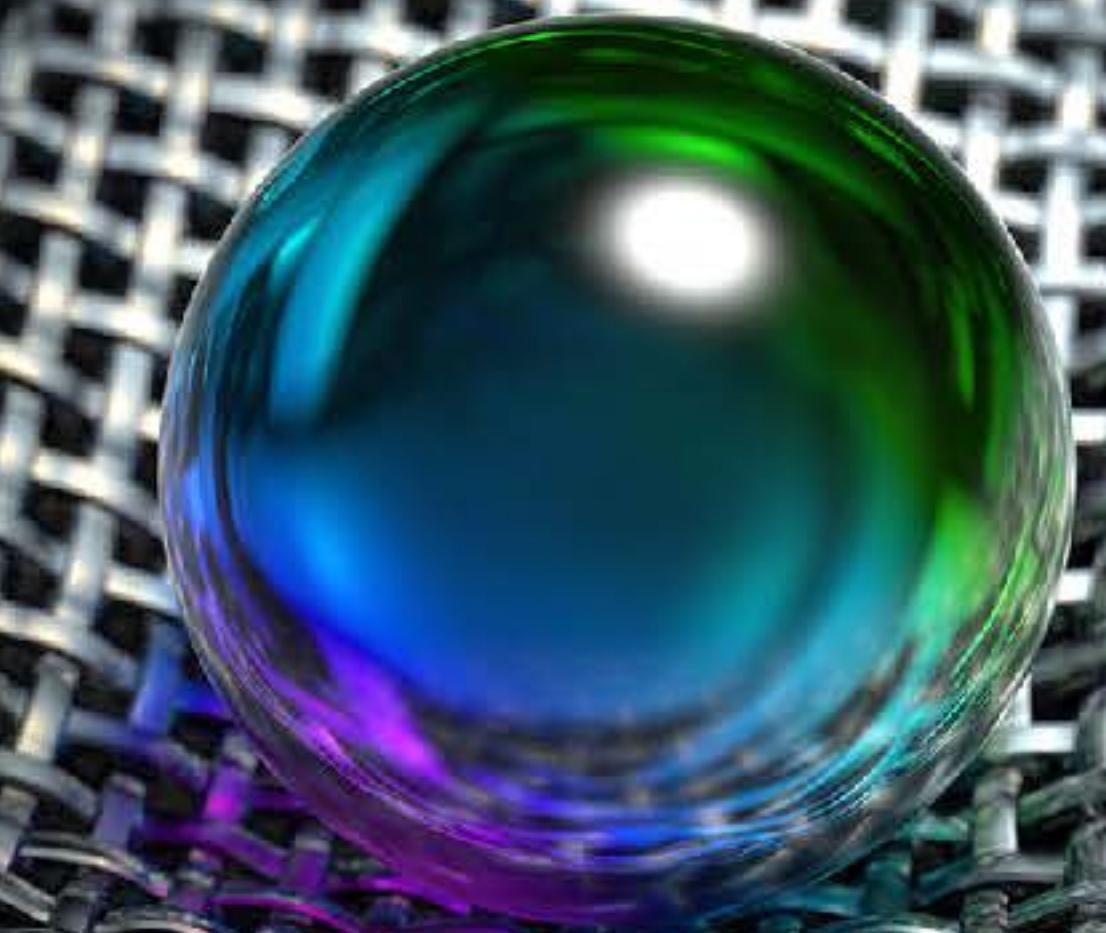
Name:	localhost
Status:	Imported
Policy:	Advanced Scan
Start:	July 3 at 4:09 PM
End:	July 3 at 4:09 PM
Elapsed:	a few seconds

Vulnerabilities



Critical	Red
High	Orange
Medium	Yellow
Low	Green
Info	Blue

Intelligence



Shodan

SHODAN Explore Downloads Pricing ↗ enphase-envoy

TOTAL RESULTS 997

TOP COUNTRIES

United States	723
Netherlands	104
Canada	45
Belgium	32
France	25
More...	

TOP ORGANIZATIONS

Charter Communications Inc	348
CPE Customers NL	35
AT&T Corp.	27
Hawaiian Telcom Services Company, Inc.	21
Comcast Cable Communications, Inc.	15
More...	

67.213.99.243

host-67-213-99-243.pub
lic.eastlink.ca
Amtelecom Cable Inc
Canada, Aylmer

mDNS:
services:
80/tcp enphase-envoy:
txtvers=1
protovers=3.7.31
serialnum=121049456542
Name=envoy
Address=67.213.99.243
answers:
PTR:
[_enphase-envoy._tcp.local](#)

136.26.94.86

136-26-94-86.cab.webp
ass.net
Webpass Inc.
United States, San Diego

mDNS:
services:
80/tcp enphase-envoy:
txtvers=1
protovers=5.0.55
serialnum=121920036082
Name=envoy
Address=136.26.94.86 2604:5500:50cb:0:12ce:
answers:
PTR:
[_enphase-envoy._tcp.local](#)

76.14.61.121

76-14-61-121.sf-cable.a
stound.net
Wave Broadband
United States, Walnut Creek

mDNS:
services:
80/tcp enphase-envoy:
txtvers=1
protovers=3.17.3
serialnum=121345000892
Name=envoy-00069

New Service: Keep track of what you have connected to the Internet

View Report Download Results Historical Trend View

hybrid-analysis.com

Sandbox Quick Scans File Collections Resources Request Info IP, Domain, Hash... Copy SHA256s

Unknown Files Collection

Number of files: 51
Sandbox Reports: 3
Created At: 10/21/2021 13:49:55 (UTC)

malicious

Link Twitter E-Mail

Analysis Overview
Anti-Virus Scanner Results
Files
Back to top

Anti-Virus Results

CrowdStrike Falcon

52.9%
47.1%

clean no-result

No threat found

GET STARTED WITH A FREE TRIAL

MetaDefender

70.6%
29.4%

clean malicious

15 of 51 are detected as malicious

VirusTotal

96.1%
3.8%

malicious clean

2 of 51 are detected as malicious

Files

Show 10 entries Search:

File name	SHA256	Tags	AV Result	Sandbox Report	Verdict
prostart.exe	43659212...d68f44a4	-	5% Trojan.Generic	✓	malicious
bin2dbex.exe	885f5033...e6adf3f3	-	4% Unsafe.AI_Score_99%	✗	malicious
fda32.exe	13f086a0...b012a480	-	4% AI Detect VM.malware1	✓	malicious
mangle.exe	c7d80925...5080ab48	-	4% Trojan.Malware.300983	✗	malicious
topgun.exe	94577813...08a3a707	-	4% Trojan/Generic.ASMalwS	✗	malicious
tproc.exe	c04c0900...388e6b9b	-	3% Trojan.Malware.300983	✗	malicious
uniedit.exe	8cb5da9e...2125a623	-	3% Trojan.Malware.300983	✗	malicious
wcsch.exe	983fd848...d3f89d94	-	3% Unsafe.AI_Score_95%	✗	malicious
cg.exe	0388802b...eab96887	-	3% Trojan.Malware.300983	✗	malicious
dlgmake.exe	4647b9ce...d9bcf545	-	3% Trojan.Malware.300983	✗	malicious

Showing 1 to 10 of 51 entries

Previous 1 2 3 4 5 6 Next

Results

Host Filters

Autonomous System:

- 263 TWC-20001-PACWEST
- 72 CELLCO-PART
- 40 COMCAST-7922
- 25 ATT-INTERNET4
- 20 AS-WAVE-1

More

Location:

- 645 United States
- 46 Canada
- 13 Netherlands
- 9 Belgium
- 7 Australia

More

Service Filters

Service Names:

- 4,787 HTTP
- 566 NTP
- 516 MDNS
- 186 SSH
- 19 FTP

More

Ports:

- 638 80
- 566 123

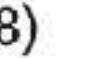
Hosts

Results: 747 Time: 2.18s

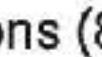
 [5.80.128.229](#)

-  BT-UK-AS BTnet UK Regional network (2856)  England, United Kingdom
-  21/FTP  22/SSH  23/TELNET
-  446/HTTP  447/HTTP  1723/PPTP
-  services.http.response.body: > <td class="hdr_line" valign="middle">
-  services.http.response.body: Serial Number: 121219038787

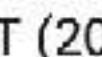
 [12.227.58.20](#)

-  ATT-INTERNET4 (7018)  California, United States
-  80/HTTP
-  services.http.response.body: > <td class="hdr_line" valign="middle">
-  services.http.response.body: Serial Number: 121504017705

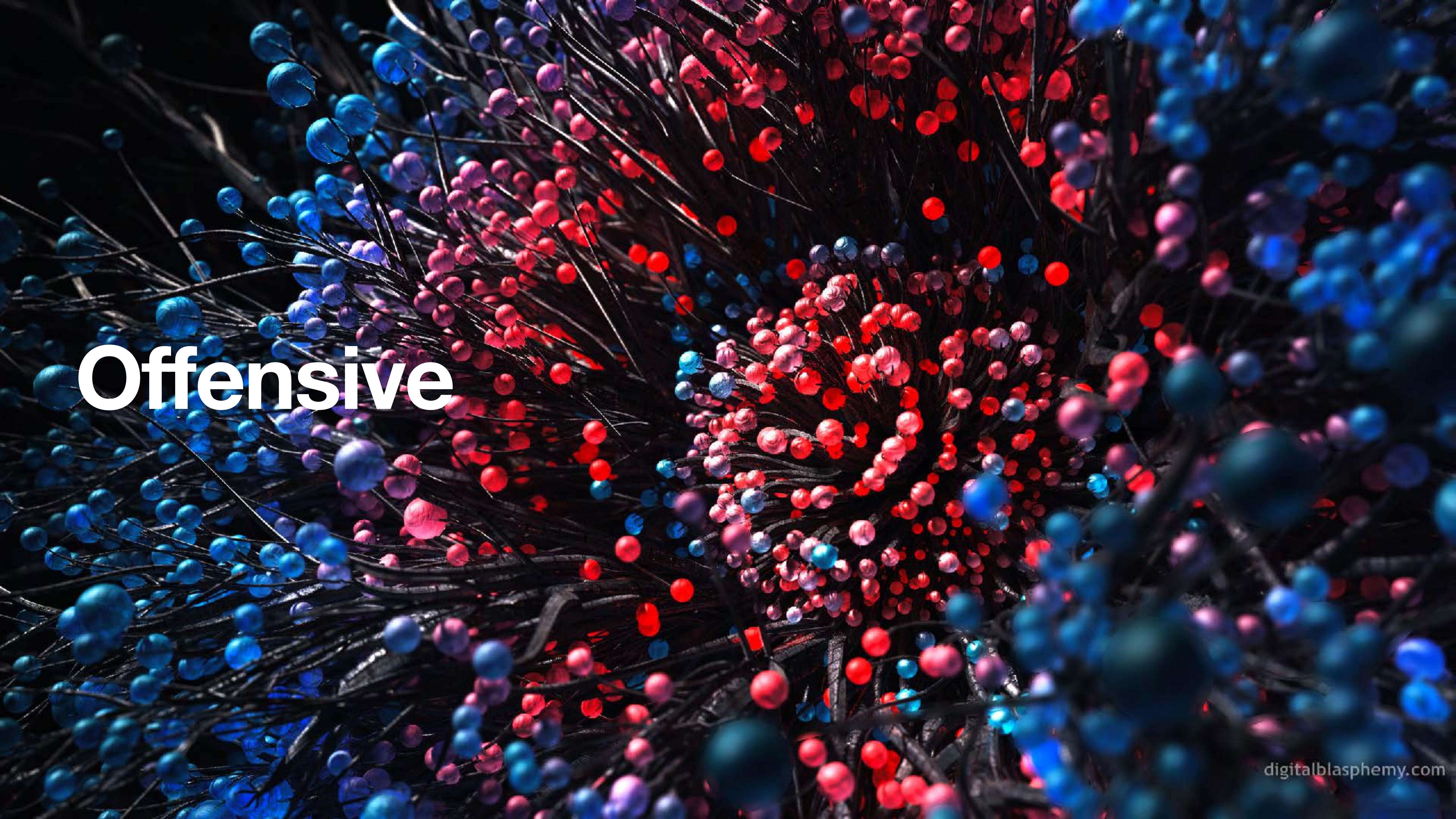
 [23.16.120.70](#)

-  TELUS Communications (852)  British Columbia, Canada
-  80/HTTP  123/NTP  5353/MDNS
-  8192/HTTP  8888/HTTP  9091/HTTP
-  9096/HTTP
-  services.http.response.body: > <td class="hdr_line" valign="middle">
-  services.http.response.body: Serial Number: 121502023085

 [23.240.15.105](#)

-  TWC-20001-PACWEST (20001)  California, United States
-  80/HTTP
-  services.http.response.body: Serial Number: 121501044202

censys.io

A complex, organic-looking structure composed of numerous small, glowing spheres in shades of red, blue, and purple. These spheres are interconnected by a network of thin, dark lines, creating a sense of depth and motion. The overall effect is reminiscent of a microscopic view of a biological tissue or a futuristic digital visualization.

Offensive

WPScan

WordPress

Security Scanner

WordPress Security Scanner
Version 3.8
Sponsored by Automattic - ht
@WPScan_, @ethicalhack3r, @e

URL: http://www.ethicalhack3r.co
Started: Mon Nov 9 15:45:23 202

Interesting Finding(s):

Headers
Interesting Entry: Server: nginx
Found By: Headers (Passive Detection)
Confidence: 100%

Fingerprinting the version - Time: 00:00:05 < (437
[+] WordPress version 4.7.2 identified (Insecure, r
| Found By: Meta Generator (Passive Detection)
| - http://www.ethicalhack3r.co.uk/, Match: 'Word
[!] 56 vulnerabilities identified:
[!] Title: WordPress 3.6.0-4.7.2 – Authenticated
L/UI:R/S:C/

Interesting Finding(s):

- [+] Headers
 - | Interesting Entry: Server: nginx
 - | Found By: Headers (Passive Detection)
 - | Confidence: 100%
- [+] WordPress readme found: http://www.ethicalhack3r.co.uk/readme
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
- [+] A backup directory has been found: http://www.ethicalhack3r.co.uk/backup-db/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 70%
| Reference: https://github.com/wpscanteam/wpscan/issues/422
- [+] This site has 'Must Use Plugins': http://www.ethicalhack3r.co.uk/wp-content/plugins/mu-plugins/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 80%

lities/8765
cvename.cgi
7/03/wordpr
ordPress/co
016/wordpre
017/q1/563

Nikto

Web Server Scanner

```
[zevlag@zevlag ~] $ nikto -host zevlag.com
- Nikto v2.1.6
-----
+ Target IP:          104.131.85.78
+ Target Hostname:   zevlag.com
+ Target Port:        80
+ Start Time:        2021-11-18 10:04:37 (GMT-5)
-----
+ Server: Apache/2.4.43 (FreeBSD) OpenSSL/1.0.2s-freebsd PHP/5.6.32
+ Retrieved x-powered-by header: PHP/5.6.32
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
  some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user to
  force the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /favicon.ico, field
+ OSVDB-39272: favicon.ico file identifies this server as: Wordpress
+ Web Server returns a valid response with junk HTTP methods, this may cause
  problems with some crawlers
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable
+ /error_log: PHP include error may indicate local or remote file inclusion
+ OSVDB-3092: /error_log: This might be interesting...
+ OSVDB-3268: /logs/: Directory indexing found.
+ OSVDB-3092: /logs/: This might be interesting...
+ OSVDB-3268: /temp/: Directory indexing found.
+ OSVDB-3092: /temp/: This might be interesting...
+ OSVDB-3233: /a/: May be Kebi Web Mail administration menu.
+ OSVDB-3268: /mc/: Directory indexing found.
+ OSVDB-3092: /mc/: This might be interesting... potential country code (Mo
+ OSVDB-3092: /tl/: This might be interesting... potential country code (Ti
```

hashcat

Password Cracker

```
hashcat (v6.2.1) starting...

CUDA API (CUDA 11.3)
=====
* Device #1: NVIDIA GeForce RTX 2080 Ti, 10137/11264 MB, 68MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Early-Skip
* Not-Iterated
* Prepended-Salt
* Single-Hash
* Single-Salt
* Brute-Force
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1100 MB

e983672a03adcc9767b24584338eb378:00:hashcat

Session.....: hashcat
Status.....: Cracked
Hash.Name....: SolarWinds Serv-U
Hash.Target...: e983672a03adcc9767b24584338eb378:00
Time.Started...: Sun May 23 11:43:13 2021 (1 sec)
Time.Estimated...: Sun May 23 11:43:14 2021 (0 secs)
Guess.Mask....: ?a?a?a?a?at [7]
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 24620.9 MH/s (32.19ms) @ Accel:32 Loops:1024 Thr:1024 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 31606272000/735091890625 (4.30%)
Rejected.....: 0/31606272000 (0.00%)
Restore.Point...: 0/857375 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:35840-36864 Iteration:0-1024
Candidates.#1...: 4{,erat -> cyr ~}t
Hardware.Mon.#1..: Temp: 62c Fan: 31% Util:100% Core:1920MHz Mem:7000MHz Bus:16

Started: Sun May 23 11:43:12 2021
Stopped: Sun May 23 11:43:15 2021
```

Metasploit

Swiss Army knife of Exploitation

```
;0MMMMMMMMMMMMMMMMMo.          +#+
. dNMMMMMMMMMMMMMMMo      +#+#+#+#+#+#
' oOWMMMMMMMMMo           +#+
.,cdk00K;            +#+  +#+
                           :::::::+:
                                         Metasploit
[metasploit v6.0.30-dev]
[ 2099 exploits - 1129 auxiliary - 357 post]
[ 592 payloads - 45 encoders - 10 nops]
[ 7 evasion]
```

Metasploit tip: To save all commands executed since start up to a file, use the `makerc` command

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.0.3
LHOST => 10.0.0.3
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.0.0.3:4444
```

Burp Suite

Ultimate MITM Proxy

And attack suite

Burp Suite Community Edition v2021.8.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept **HTTP history** WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comments
17	https://hackerschallenge.org	GET	/events			403	6250	HTML		Hackers Challenge	
15	https://use.fontawesome.com	GET	/releases/v5.9.0/webfonts/fa-solid-9...			200	76617			woff2	
14	https://fonts.gstatic.com	GET	/s/latO/v20/S6uyw4BMUTPHjx4wX...			200	24454			woff2	
13	https://saintcon.org	GET	/wp-content/uploads/2021/07/LOG...			200	1410087	XML		svg	
12	https://hackerschallenge.org	GET	/themes/core/static/js/core.min.js?d...		✓	200	326	script	js		
11	https://hackerschallenge.org	GET	/themes/core/static/js/helpers.min.js...		✓	200	5705	script	js		
10	https://hackerschallenge.org	GET	/themes/core/static/js/pages/main.m...		✓	200	51332	script	js		
7	https://hackerschallenge.org	GET	/themes/core/static/js/vendor.bundl...		✓	200	1379336	script	js		
3	https://hackerschallenge.org	GET	/			200	7203	HTML		Hackers Challenge	
2	http://hackerschallenge.org	GET	/			301	354	HTML		301 Moved Permanently	
1	https://hackerschallenge.org	GET	/			200	7203	HTML		Hackers Challenge	

Request

Pretty Raw Hex \n ⌂

```
1 GET / HTTP/1.1
2 Host: hackerschallenge.org
3 Sec-Ch-Ua: ";Not A Brand";v="99", "Chromium";v="94"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "macOS"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61
Safari/537.36
8 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
```

Response

Pretty Raw Hex Render \n ⌂

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Thu, 21 Oct 2021 15:21:30 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 6933
6 Connection: close
7 Set-Cookie: session=e6eae927-c5c2-462d-b9df-33f9c7b5644d.jpDd
8
9 <!DOCTYPE html>
10 <html>
11   <head>
12     <title>
13       Hackers Challenge
14     </title>
15     <meta charset="utf-8">
16     <meta name="viewport" content="width=device-width, initial-scale=1.0, user-scalable=0">
17     <link rel="shortcut icon" href="/themes/core/static/img/favicon.ico">
18     <link rel="stylesheet" href="/themes/core/static/css/font-awesome.css">
19     <link rel="stylesheet" href="/themes/core/static/css/main.css">
20     <link rel="stylesheet" href="/themes/core/static/css/core.css">
21
22     <script type="text/javascript">
23       var init = {
24         'urlRoot': '',
25         'csrfNonce': 'aeed4ce25582a131c29f220c0bde4c4alc263e3',
26         'userMode': 'users',
27         'userId': 0,
28         'start': 1634668496,
29         'end': 1634914800,
30         'theme_settings': null
31       }
32     </script>
33     <style>
34       .navbar-dark{
35         background-color:#ff2aab!important;
36         color:hsl(0,0%,100%);
37       }
38     .navbar-dark.navbar-nav.nav-link{
```

INSPECTOR

Request Attributes

Request Headers

Name

Host

Sec-Ch-Ua

Sec-Ch-Ua-Mobile

Sec-Ch-Ua-Platform

Upgrade-Insecure-Requests

User-Agent

Accept

Sec-Fetch-Site

Sec-Fetch-Mode

Sec-Fetch-User

Sec-Fetch-Dest

Accept-Encoding

Accept-Language

Connection

Response Headers

Fiddler

Telerik Fiddler Web Debugger

File Edit Rules Tools View Help GeoEdge

WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard

#	Result	Protocol	Host	URL
35	200	HTTPS	www.telerik.com	/
36	200	HTTPS	ajax.aspnetcdn.com	/ajax/jquery/jquery-1.12.1.min.js
37	200	HTTPS	cdn.cookie-law.org	/consent/2fffb1c2-c64a-4fcc-bc19-a4adecbc5ebf.js
css38	200	HTTPS	www.telerik.com	/Telerik.Web.UI.WebResource.axd?d=Fwpnh9ive5PG4kWt6X
css39	200	HTTPS	dtzbddy9anri2p.cloudfront.net	/cache/f09825e1707b511d225a91005f91d87505d64f40/teler
40	200	HTTP		Tunnel to dtzbddy9anri2p.cloudfront.net:443
41	200	HTTP		Tunnel to ajax.aspnetcdn.com:443
42	200	HTTP		Tunnel to www.telerik.com:443
css43	200	HTTPS	dtzbddy9anri2p.cloudfront.net	/cache/7e05f6db9d18aebb0ada00323c63b3c5c573c1b8/teler
js44	200	HTTPS	ajax.aspnetcdn.com	/ajax/4.5.1/1/WebForms.js
45	200	HTTP		Tunnel to ajax.aspnetcdn.com:443
46	200	HTTP		Tunnel to ajax.aspnetcdn.com:443
47	200	HTTP		Tunnel to optanon.blob.core.windows.net:443
js48	200	HTTPS	ajax.aspnetcdn.com	/ajax/beta/0911/MicrosoftAjax.js
js49	200	HTTPS	ajax.aspnetcdn.com	/ajax/beta/0910/MicrosoftAjaxWebForms.js
js50	200	HTTPS	www.googletagmanager.com	/gtm.js?id=GTM-6X92
js51	200	HTTPS	s1325.t.eloqua.com	/visitor/v200/srvGP?pps=70&siteid=1325
js52	200	HTTPS	s3.amazonaws.com	/telerik-media/scripts/ribbon.js
css53	200	HTTPS	d6vtbcy3ong79.cloudfront.net	/fonts/1.1.5/css/metric.min.css
44	200	HTTP		Tunnel to d6vtbcy3ong79.cloudfront.net:443
55	200	HTTP		Tunnel to d6vtbcy3ong79.cloudfront.net:443
56	200	HTTPS	d585tldpucybw.cloudfront.net	/sfimages/default-source/homepage/tirk/kendo-ui-r1.jpg?sfvr
57	200	HTTPS	d117h1jjq768j.cloudfront.net	/images/default-source/home/progress-next-logo.png
58	200	HTTP		Tunnel to d585tldpucybw.cloudfront.net:443
59	200	HTTP		Tunnel to d585tldpucybw.cloudfront.net:443
60	200	HTTP		Tunnel to d585tldpucybw.cloudfront.net:443
61	200	HTTP		Tunnel to d585tldpucybw.cloudfront.net:443
62	200	HTTP		Tunnel to d585tldpucybw.cloudfront.net:443
css63	200	HTTPS	d6vtbcy3ong79.cloudfront.net	/telerik-navigation/1.1.2/css/index.min.css
64	200	HTTP		Tunnel to d117h1jjq768j.cloudfront.net:443
js65	200	HTTPS	d6vtbcy3ong79.cloudfront.net	/telerik-navigation/1.1.2/js/index.min.js
js66	200	HTTPS	www.telerik.com	/WebResource.axd?d=loVHAc3af3LMu99qYAVmFA0Y2PAs7O
67	200	HTTPS	d585tldpucybw.cloudfront.net	/sfimages/default-source/homepage/telerik-ninja.png?sfvrsn=

Filters

Statistics

Request Count: 1
Bytes Sent: 2,588
Bytes Received: 62,546

ACTUAL PERFORMANCE

ClientConnected: 12:24:53.572
ClientBeginRequest: 12:24:54.134
GotRequestHeaders: 12:24:54.134
ClientDoneRequest: 12:24:54.134
Determine Gateway: 0ms
DNS Lookup: 0ms
TCP/IP Connect: 0ms
HTTPS Handshake: 0ms
ServerConnected: 12:24:53.861
FiddlerBeginRequest: 12:24:54.134
ServerGotRequest: 12:24:54.134
ServerBeginResponse: 12:24:54.672
GotResponseHeaders: 12:24:54.672
ServerDoneResponse: 12:24:55.202
ClientBeginResponse: 12:24:54.672
ClientDoneResponse: 12:24:55.202

Overall Elapsed: 0:00:01.068

RESPONSE BYTES (by Content-Type)

text/html: 62,122
~headers~: 424

ESTIMATED WORLDWIDE PERFORMANCE

The following are VERY rough estimates of download times from Seattle.

US West Coast (Modem - 6KB/sec)
RTT: 0.10s
Elapsed: 10.10s

Japan / Northern Europe (Modem)
RTT: 0.15s
Elapsed: 10.15s

China (Modem)
RTT: 0.45s
Elapsed: 10.45s

US West Coast (DSL - 30KB/sec)
RTT: 0.10s
Elapsed: 2.10s

[QuickExec] ALT+Q > type HELP to learn more

Show Chart

Capturing Web Browsers 1 / 239 18mb https://www.telerik.com/

Postman

The screenshot shows the Postman application interface. At the top, there's a navigation bar with 'Import', 'Overview', 'New Collection' (with a plus icon), 'New Request' (highlighted in orange), 'New Request Copy' (with a plus icon), and 'No Environment'. A search bar says 'Search Postman' and there are icons for cloud, settings, and sign in.

The main area shows a 'New Collection / New Request' screen. The request method is 'POST' and the URL is 'https://www.hackerschallenge.org/api/v1/awards'. The 'Headers' tab is selected, showing two headers: 'Accept' with value 'application/json' and 'Authorization' with value 'Token b36909ee6bb70766318b58d46ab8b1eecf22...'. There are also 9 hidden headers listed.

The 'Body' tab is selected, showing a JSON response:

```
1 "success": true,
2 "data": {
3     "requirements": null,
4     "team": null,
5     "date": "2021-10-21T16:11:44+00:00",
6     "value": 5,
7     "user_id": 5,
8     "type": "standard",
9     "name": "BadgedIn",
10    "category": null,
11    "team_id": null,
12    "user": 5,
13    "icon": "lightning",
14    "description": "Displayed your score between:",
15    "id": 199
16 }
17
18 }
```

At the bottom right, it says 'Status: 200 OK Time: 299 ms Size: 559 B Save Response'.

ashirt
[https://
github.com/
the paranoid/
ashirt-server/](https://github.com/the paranoids/ashirt-server/)

The screenshot shows the ASHIRT application interface. At the top, there's a header with the ASHIRT logo, a user icon, and navigation links for "Create Finding" and "Create Evidence". Below the header, a project titled "Harry Potter and The C..." is shown as "Planning" with 6 members. A sidebar on the left lists "EVIDENCE" (All Evidence, Locate Chamber), "FINDINGS" (All Findings, Find Heir), and other project details like "Ticket" and "Tags". The main area displays a table of findings:

Title	Category	Ticket	# Evidence	Date Range	Tags
lots o' magic	some-category	Pending	3	04/03/84-04/03/84	Mercury, Earth, Mars, Jupiter, Saturn
this looks fake	alt-category	Ready to Report	2	04/03/84-04/03/84	Mercury, Mars, Jupiter
how to scare spiders	some-category	www.google.com/search	0	N/A	

Reverse Engineering

dnSpy

A Decompiler for .NET

dnSpy v6.0.5 (64-bit, .NET Core)

File Edit View Debug Window Help | C# | ▾ | ⌂ ⌂ | Start |

Assembly Explorer dnSpy (6.0.5.0)

- System.Private.Uri (4.0.5.0)
- System.Linq (4.2.1.0)
- System.Private.Xml (4.0.1.0)
- System.Xaml (4.0.0.0)
- WindowsBase (4.0.0.0)
- PresentationCore (4.0.0.0)
- PresentationFramework (4.0.0.0)
- dnlib (3.2.0.0)
- dnSpy (6.0.5.0)

dnSpy (6.0.5.0)

```
1 // C:\temp\dnspy\dnSpy.dll
2 // dnSpy, Version=6.0.5.0, Culture=neutral, PublicKeyToken=9813e10cffb0cdd6
3
4 // Entry point: dnSpy.MainApp.StartUpClass.Main
5 // Timestamp: <Unknown> (AB4D6BBC)
6
7 using System;
8 using System.Diagnostics;
9 using System.Reflection;
10 using System.Resources;
11 using System.Runtime.CompilerServices;
12 using System.Runtime.Versioning;
13 using System.Security.Permissions;
14
15 [assembly: AssemblyVersion("6.0.5.0")]
16 [assembly: CompilationRelaxations(8)]
17 [assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
18 [assembly: Debuggable(2)]
19 [assembly: TargetFramework(".NETCoreApp,Version=v3.0", FrameworkDisplayName="")]
20 [assembly: AssemblyCompany("dnSpy")]
21 [assembly: AssemblyConfiguration("Release")]
22 [assembly: AssemblyCopyright("Copyright (C) 2014-2019 de4dot@gmail.com")]
```

100 %

Exception Settings

Break When Thrown Category

Break When Thrown	Category
<input checked="" type="checkbox"/> <All Common Language Runtime Exceptions not in this list>	Common Language Runtime Exceptions
<input checked="" type="checkbox"/> Microsoft.JScript.JScriptException	Common Language Runtime Exceptions
<input checked="" type="checkbox"/> System.AccessViolationException	Common Language Runtime Exceptions
<input checked="" type="checkbox"/> System.AggregateException	Common Language Runtime Exceptions
<input checked="" type="checkbox"/> System.AppDomainUnloadedException	Common Language Runtime Exceptions

Ghidra

CodeBrowser: ctf:/boot.bin

File Edit Analysis Graph Navigation Search Select Tools Window Help

I D U L F R V B

Program Trees Listing: boot.bin Decompile: UndefinedFunction

boot.bin ram

// ram
// ram:0000:7c00-ram:0000:7dff
//
assume DF = 0x0 (Default)

Address	OpCode	Operands	Description
0000:7c00	31 c0	XOR AX,AX	
0000:7c02	8e d8	MOV DS,AX	
0000:7c04	8e c0	MOV ES,AX	
0000:7c06	bb 00 80	MOV BX,0x8000	
0000:7c09	fa	CLI	
0000:7c0a	8e d3	MOV SS,BX	
0000:7c0c	89 c4	MOV SP,AX	
0000:7c0e	fb	STI	
0000:7c0f	fc	CLD	
0000:7c10	30 e4	XOR AH,AH	
0000:7c12	b0 03	MOV AL,0x3	
0000:7c14	cd 10	INT 0x10	
0000:7c16	30 c0	XOR AL,AL	
0000:7c18	ea 7a 7c	JMPF LAB_0000_7c7a	
	00 00		
0000:7c1d	eb 5b	JMP LAB_0000_7c7a	
0000:7c1f	60	PUSHA	
0000:7c20	b9 00 00	MOV CX,0x0	
0000:7c23	83 f9 04	CMP CX,0x4	XREF[1]: 0000:7c4
0000:7c26	74 1f	JZ LAB_0000_7c47	
0000:7c28	89 c2	MOV DX,AX	
0000:7c2a	83 e2 0f	AND DX,0xf	
0000:7c2d	80 c2 30	ADD DL,0x30	
0000:7c30	80 fa 39	CMP DL,0x39	
0000:7c33	7e 03	JLE LAB_0000_7c38	
0000:7c35	80 c2 07	ADD DL,0x7	
0000:7c38	bb 54 7c	MOV BX,0x7c54	XREF[1]: 0000:7c3
0000:7c3b	29 cb	SUB BX,CX	
0000:7c3d	88 17	MOV byte ptr [BX],DL	
0000:7c3f	c1 c8 04	ROR AX,0x4	
0000:7c42	83 c1 01	ADD CX,0x1	
0000:7c45	eb dc	JMP LAB_0000_7c23	
0000:7c47	b8 4f 7c	MOV AX,0x7c4f	XREF[1]: 0000:7c2
0000:7c4a	e8 09 00	CALL FUN_0000_7c56	
0000:7c4d	61	POPA	
0000:7c4e	c3	RET	
0000:7c4f	30 78 30	XOR byte ptr [BX + SI + 0x30],BH	

Symbol Tree

- Imports
- Exports
- Functions
- Labels
- Classes
- Namespaces

Filter:

Decompiled C code:

```
1 /* WARNING: Stack frame
2 /* WARNING: This function does not have any visible exits
3
4 void UndefinedFunction()
5 {
6     byte bVar1;
7     code *pcVar2;
8     char cVar3;
9     undefined *puVar4;
10    int iVar5;
11
12    puVar4 = (undefined *)pcVar2;
13    pcVar2 = (*pcVar2)();
14    *(undefined2 *)puVar4 = FUN_0000_7c56();
15    iVar5 = 0;
16    while( true ) {
17        pcVar2 = (code *)swi(
18        cVar3 = (*pcVar2)();
19        if (cVar3 == '\r') {
20            if ('\x1f' < cVar3) {
21                *(char *)((int)&D
22                iVar5 = iVar5 + 1
23                if (iVar5 == 0x20)
24                    *(undefined2 *)puVar4 = FUN_0000_7c73();
25            }
26        }
27        *(undefined2 *)puVar4 = FUN_0000_7c66();
28        iVar5 = 0;
29        do {
30            bVar1 = *(byte *)(
31            if (bVar1 == 0) {
32                *(undefined2 *)puVar4 = FUN_0000_7c56();
33            }
34            code_r0x00007cd3:
35            do {
36                bVar1 = *(byte *)(
37                if (bVar1 == 0) {
38                    *(undefined2 *)puVar4 = FUN_0000_7c56();
39                }
40            }
41            code_r0x00007cd3:
42            do {
43                } while( true );
44            }
45            if ((*byte *)((int)&D
46            *(undefined2 *)puVar4 = FUN_0000_7c56();
47            goto code_r0x0000
48        }
49    }
50 }
```

IDA

Free Version is quite capable
with cloud decompiler

The screenshot shows the IDA Pro interface with the following details:

- Functions List:** On the left, a tree view lists various functions, many of which are prefixed with "github_com_veandco_go_sdl2_sdl_". These include: github_com_veandco_go_sdl2_sdl_, type_eq_6_float32, type_eq_github_com_veandco_g, main_main, main_main_dwrap_3, main_main_dwrap_2, main_main_dwrap_1, main_updateSpecials, main_updateSpecials_dwrap_4, main_updateTics, main_updateTics_dwrap_5, main_blendPixel, main_renderHUD, main_renderSky, main_renderMinimap, main_renderFloors, main_renderWalls, main_imageFormatDecode, main_textureDecoder, runtime_etext, goSetEventFilterCallback, goEventFilterCallback, and goHintCallback.
- Pseudocode View:** The main window displays decompiled pseudocode. The code is written in a C-like syntax with some assembly-style variables (v0, v1, v2, v3, v4, v5, v6, v7, v8, v9) and labels (LABEL_7). It includes function calls like runtime_morestack_noctxt(), runtime_panicIndex(), and github_com_veandco_go_sdl2_sdl_Init().

```
char v7[9]; // [rsp+122h] [rbp-FEh]
int64 v8; // [rsp+12Bh] [rbp-F5h]
char v9[9]; // [rsp+133h] [rbp-EDh]
int64 v10; // [rsp+13Ch] [rbp-E4h]
void *v11; // [rsp+1D8h] [rbp-48h]
int64 v12; // [rsp+1E0h] [rbp-40h]
int128 v13; // [rsp+1F8h] [rbp-28h]
int128 v14; // [rsp+208h] [rbp-18h]
int64 v15; // [rsp+218h] [rbp-8h]

while ( (unsigned __int64)&v6 <= *(_QWORD *) (v1 + 16) )
    runtime_morestack_noctxt();
v15 = v0;
v13 = v2;
v14 = v2;
if ( qword_8D4F48 != 2 )
    goto LABEL_7;
if ( (unsigned __int64)qword_8D4F48 <= 1 )
    runtime_panicIndex();
if ( (*(_QWORD *) (os_Args + 24) != 8LL || **(_QWORD **) (os_Args + 16) != 0x6C61657665722D2D)
    goto LABEL_7;
v9[0] = 0;
*( _QWORD *) &v9[1] = 0x9E57C1A38FAB9DEDLL;
v10 = 0x8DDD7833D9890A26LL;
v7[0] = 102;
*( _QWORD *) &v7[1] = 0xED23AECDA2CCFC81LL;
v8 = 0xA91D41BABC79494LL;
for ( i = 0LL; ; ++i )
{
    if ( i >= 17 )
    {
        runtime_slicebytetostring();
        runtime_convTstring(v5);
        v11 = &unk_660300;
        v12 = v4;
        fmt_Fprintln();
    }
LABEL_7:
    if ( qword_8D4F48 == 2 && (*(_QWORD *) (os_Args + 24) == 1LL && **(_BYTE **) (os_Args + 16) == 0x6C61657665722D2D)
        main_reargate ^= 1u;
        if ( !github_com_veandco_go_sdl2_sdl_Init() )
        {
            *((_QWORD *) &v14 + 1) = &off_6DFED8;
            github_com_veandco_go_sdl2_sdl_CreateWindow();
            runtime_gopanic();
        }
        i = runtime_gopanic();
    }
    v9[1] ^= v7[1];
}
```
- Output Window:** At the bottom, the IDC (Interactive Disassembly Commander) window shows the following output:

```
63B9AU: using guessed type __int64 main_updateSpecials(void);
63BFC0: using guessed type __int64 main_renderHUD(void);
63CF00: using guessed type __int64 main_textureDecoder(void);
6DFED8: using guessed type __int64 (_golang *off_6DFED8)();
8D4F40: using guessed type __int64 os_Args;
8D4F48: using guessed type __int64 qword_8D4F48;
9054CD: using guessed type char main_reargate;
9058E0: using guessed type char main_circular_buffer;
```

Binary Ninja

ch2.elf - Binary Ninja 2.3.2740-dev

The screenshot shows the Binary Ninja interface for the file ch2.elf. The main window displays assembly code for the main function. The assembly code includes various system calls like fgets, scanf, and printf, along with some local variables and control flow logic. A memory dump window below the assembly shows the byte sequence 66-0f 1f 84 00 00 00 00 00 followed by several 'f' characters. The variable references pane shows that the variable var_88 is used in four different locations: its initial assignment at address 0x400075d, its use in the sscanf call at 0x40007bc, its use in the printf call at 0x40007d8, and its comparison in the if statement at 0x4000827. The registers pane on the right shows the current value of var_88 as 0x1898d542.

```
int32_t main(int32_t arg1, char** arg2, char** arg3)

void* fsbase
int64_t rax = *(fsbase + 0x28)
int32_t var_88 = 0
int32_t var_84 = 0
int32_t var_7c = 0x41414141
int32_t var_7c_1 = 0x62637441
void var_78
for (; var_84 == 0; var_84 = sscanf(s: &var_78, format: data_400905, &var_88))
    printf(format: "Password 2: ")
    fgets(buf: &var_78, n: 0x64, fp: *stdin)
int32_t var_7c_2 = 0x1898dd10
printf(format: "\nYou tried: %d\nLet's see if th...", zx.q(var_88))
for (int32_t var_80 = 0; var_80 <= 5; var_80 = var_80 + 1)
    putchar(c: 0xe)
    fflush(fp: *stdout)
    sleep(seconds: 1)
    putchar(c: 0xa)
if (var_88 != 0x1898d542)
    printf(format: "I'm sorry, you have failed.")
else
    printf(format: "Great job! You succeeded.")
if ((rax ^ *(fsbase + 0x28)) == 0)
    return 0
_stack_chk_fail()
noreturn
```

00400867 66-0f 1f 84 00 00 00 00 00 f.....

```
int32_t libc_csu_init(int32_t arg1, char** arg2, char** arg3)
```

>>> current_function.vars
[0].storage
-136
>>> current_function.vars
[0].name
'var_88'

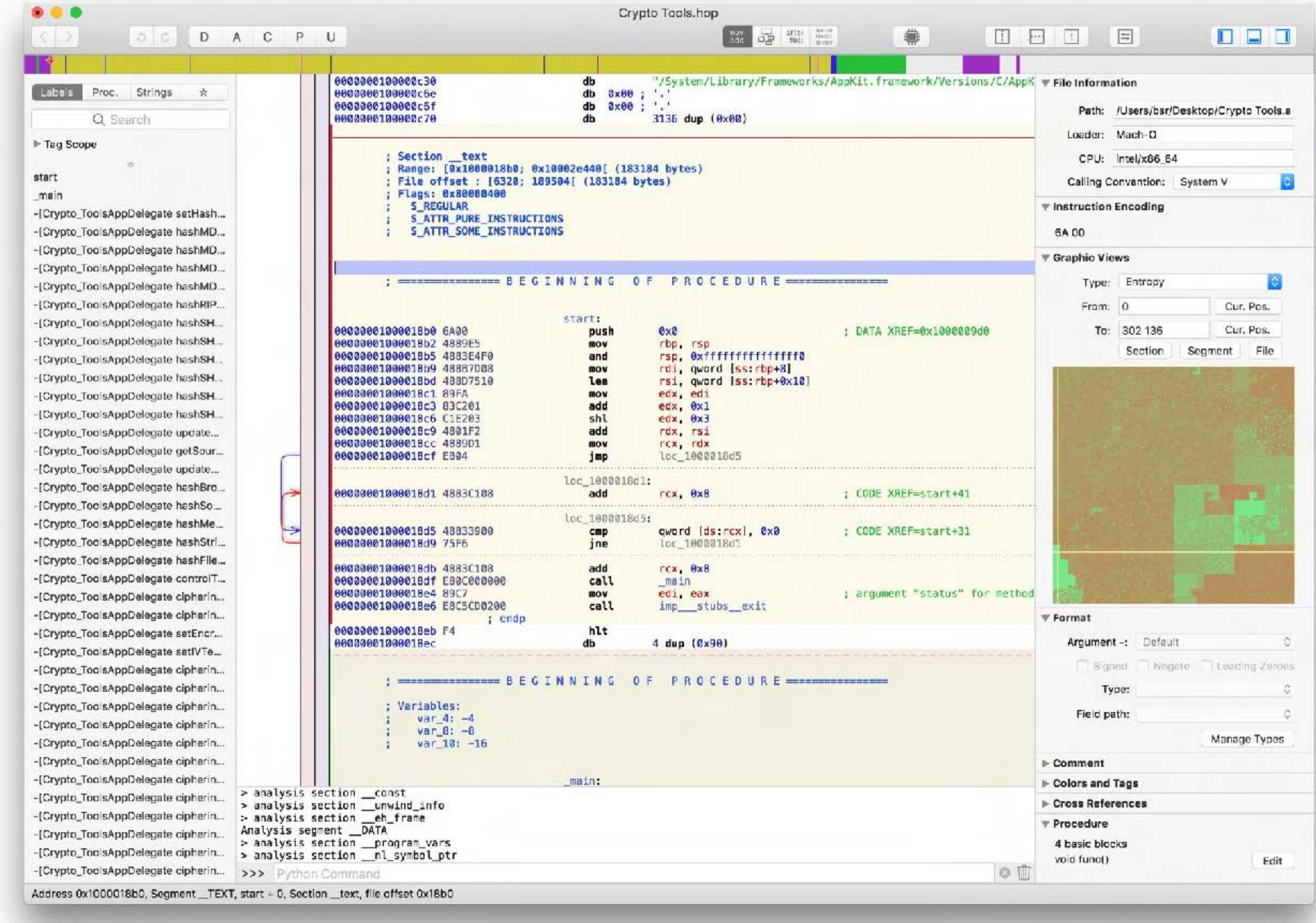
Selection: 0x4000827 to 0x400082a (0x3 bytes) ELF Linear Options

Symbols Tags

Hopper

MacOS Decompiler

Objective C



The background consists of a dense, swirling pattern of black and dark grey lines, resembling a microscopic view of a complex organic structure or a network of veins. These lines are set against a bright, glowing green central area that has a slightly textured, almost liquid appearance. In the center of this green glow, there is a more concentrated, branching structure that looks like a stylized tree or perhaps a microscopic organism. The overall effect is one of depth and motion.

Everything Else

SQL Structured Query Language

```
SELECT incidents.*,
       sub.incidents AS incidents_that_day
  FROM tutorial.sf_crime_incidents_2014_01 incidents
 JOIN ( SELECT date,
               COUNT(incident_num) AS incidents
                  FROM tutorial.sf_crime_incidents_2014_01
                 GROUP BY 1
            ) sub
    ON incidents.date = sub.date
 ORDER BY sub.incidents DESC, time
```

Excel



CyberChef

<https://github.com/mattnotmax/cyberchef-recipes>

The screenshot shows the CyberChef application window with several panels open:

- Unzip**: A panel for unzipping files. It includes a "Password" input field and a checkbox for "Verify result".
- Register**: A panel for creating a regular expression. The "Extractor" field contains the pattern `if\\\\\\\\\\\\\\\\\".*?([a-z]{3})`. Checkboxes for "Case Insensitive", "Multiline matching", and "Dot matches all" are present.
- Find / Replace**: A panel for searching and replacing text. The "Find" field contains `$R0`, and the "Replace" field is empty. Checkboxes for "Global match", "Case insensitive", "Multiline matching", and "Dot matches all" are shown.
- Extract URLs**: A panel for extracting URLs from text. The "Display total" checkbox is checked.
- Regular expression**: A panel for working with regular expressions. It shows a "Built in regexes" section with "User defined" and a "Regex" field containing the pattern `(http|https)://^(?!.*(\.microsoft\.com|\.\openxmlformats\.org|purl\.org|\.\w3\.org)).*`. Checkboxes for "Case insensitive", "Astral support", "Multiline matching", "Dot matches all", "Unicode support", and "Output format List matches" are shown.
- Find / Replace**: A panel for searching and replacing text. The "Find" field contains a single character, and the "Replace" field contains `\n`. Checkboxes for "Global match", "Case insensitive", "Multiline matching", and "Dot matches all" are shown.
- Defang URL**: A panel for defanging URLs. It includes checkboxes for "Escape dots", "Escape http", and "Escape ://". A "Process" button with the text "Valid domains and full URLs" is at the bottom.



base64

|
V

iVBORw0KGgoAAAANSUhEUgAAB8IAAAEICAYAAAk3j7UAAAAG1DQ1BJQ0MgUHJ
vZm1sZQAAStmVVwdUU8kanltSSWiBCEgJvQnSq5QQWgABqYKNkAQSSgwJQcVeFh
VcKyKKFV0Vsa2ugKwFsZdFsPfFgoqyLuqiKCpvQgK67ivn/efMnS/f/
P0305M7A4BWL08qzU01AcjXFMoSIkJYY9PSWaQ0QAYYoAIHYMXjy6Xs+PgYAGWw
/7u8uwEQZX/VSwnrn+P/
VXQFQjkfAGQ8xJkCOT8f4jYA8PV8qawQAKKSt5xSKFXi0RDryWCAEJcrcbYK71T
iTBU+MqCTlMCBuBUAMo3Hk2UDoHkP

...

66Xq3zNYrlSzbc4Erivzhf/
fasc8GD3npvti+uAZ7ZFTtrn3XQSXnWGHb1TJmveBMWZ1Kf09/04yDD2w85d/
gw9T7n3B980P4//tE11adQ0R8AAAAASUVORK5CYII=

curl / wget

curl Protocols:

DICT
FILE
FTP(S)
GOPHER(S)
HTTP(S)
IMAP(S)
LDAP(S)
MQTT
POP3(S)
RTMP(S)
RTSP
SCP
SFTP
SMB(S)
SMTP(S)
TELNET
TFTP

wget Features:

Recursive download

jq

JSON data manipulation

```
zevlag@Z314 ~ % cat users.json | jq '.data[]'  
{  
  "pos": 1,  
  "account_id": 100,  
  "account_url": "/users/100",  
  "account_type": "user",  
  "oauth_id": null,  
  "name": "phaktor",  
  "score": 0  
}  
{  
  "pos": 2,  
  "account_id": 6,  
  "account_url": "/users/6",  
  "account_type": "user",  
  "oauth_id": null,  
  "name": "Santiago",  
  "score": 0  
}  
{  
  "pos": 3,  
  "account_id": 78,  
  "account_url": "/users/78",  
  "account_type": "user",  
  "oauth_id": null,  
  "name": "Legoclones",  
  "score": 0  
}  
{  
  "pos": 4,  
  "account_id": 69,  
  "account_url": "/users/69",  
  "account_type": "user",  
  "oauth_id": null,  
  "name": "cha0swir3",  
  "score": 0  
}
```

WSL
Windows
Subsystem
Linux

proxychains
hooks network functions
and redirects to a proxy

Vmware

Virtualbox

QEMU

grep

**[https://beyondgrep.com/
feature-comparison/](https://beyondgrep.com/feature-comparison/)**

vscode

Notepad++

Sublime Text

BBEdit

Collections

Kali



CommandoVM

Windows-based security
distribution for penetration
testing and red teaming



COMMANDOVM
COMPLETE MANDIANT OFFENSIVE VM

flareVM

**Windows-based security
distribution for malware
analysis, incident response**





And Finally

Play Capture The Flag

Be Curious

Why?

How?

