RUBYCARP: A Detailed Analysis of a Sophisticated Decade-Old Botnet Group

By Sysdig Threat Research Team

Published: 2024-04-09 · Archived: 2026-04-05 15:43:41 UTC

The Sysdig Threat Research Team (Sysdig TRT) recently discovered a long-running botnet operated by a Romanian threat actor group, which we are calling RUBYCARP. Evidence suggests that this threat actor has been

active for at least 10 years. Its primary method of operation leverages a botnet deployed using a variety of public exploits and brute force attacks. This group communicates via public and private IRC networks, develops cyber weapons and targeting data, and uses its botnet for financial gain via cryptomining and phishing. This report explores how RUBYCARP operates and its motivations.

RUBYCARP, like many threat actors, is interested in payloads that enable financial gain. This includes cryptomining, DDoS, and Phishing. We have seen it deploy a number of different tools to monetize its compromised assets. For example, through its Phishing operations, RUBYCARP has been seen targeting credit cards. As we have seen with other threat actors, it has a diversified set of illicit income streams.

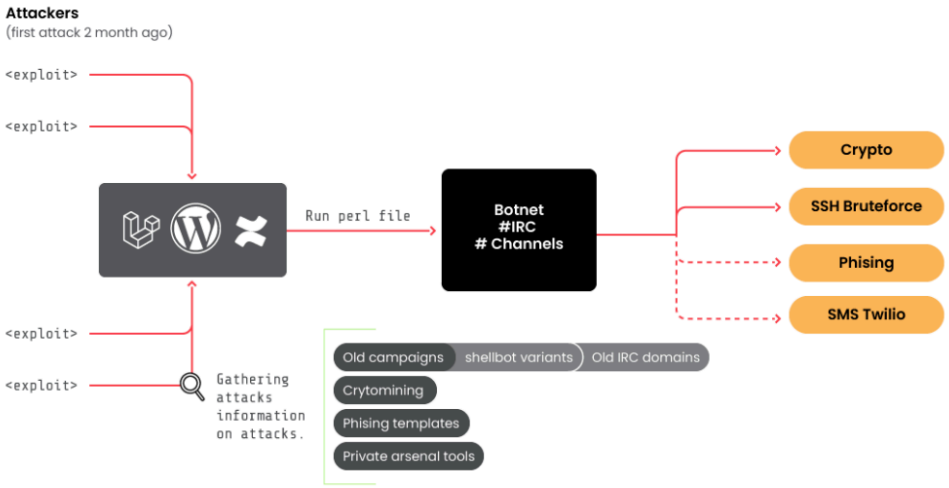
Attribution

RUBYCARP, the name we have given this group, is a financially-motivated threat actor group that is most likely Romanian. RUBYCARP may be related to the Outlaw advanced persistent threat (APT), as it does share many of the same tactics, techniques, and procedures (TTPs). However, since these shared TTPs are common across many botnet operators, we cannot definitively make this conclusion. RUBYCARP leverages Shellbot often during its operations, which can also cause attribution confusion since this tool is a common choice among threat actors.

In the murky world of cybercriminal threat intelligence, there is often a lot of crossover in both tools and targeting. In the recent advisory from CISA, the Androxgh0st threat actor's choice to exploit Laravel is discussed. This is another example of cybercriminal overlap, with RUBYCARP notably targeting the same framework vulnerabilities. Many of these threat actors are fighting it out over the same target space, making it difficult to attribute attacks.

What is RUBYCARP?

For months, Sysdig TRT's has been tracking RUBYCARP through the **targeting and exploitation of Laravel applications vulnerable to CVE-2021-3129**. This led to evidence of SSH Brute forcing as another way the group gained access to its targets. Recently, we also discovered evidence of the threat actor targeting WordPress sites using dumps of usernames and passwords. RUBYCARP continues to add new exploitation techniques to its arsenal in order to build its botnets.



Once access is obtained, a backdoor is installed based on the popular Perl Shellbot. The victim's server is then connected to an IRC server acting as command and control, and joins the larger botnet. During RUBYCARP's reconnaissance phase, we found 39 variants of the Perl file (shellbot), but only eight were in VirusTotal. This means that only a few campaigns were previously detected. The modifications of the files are:

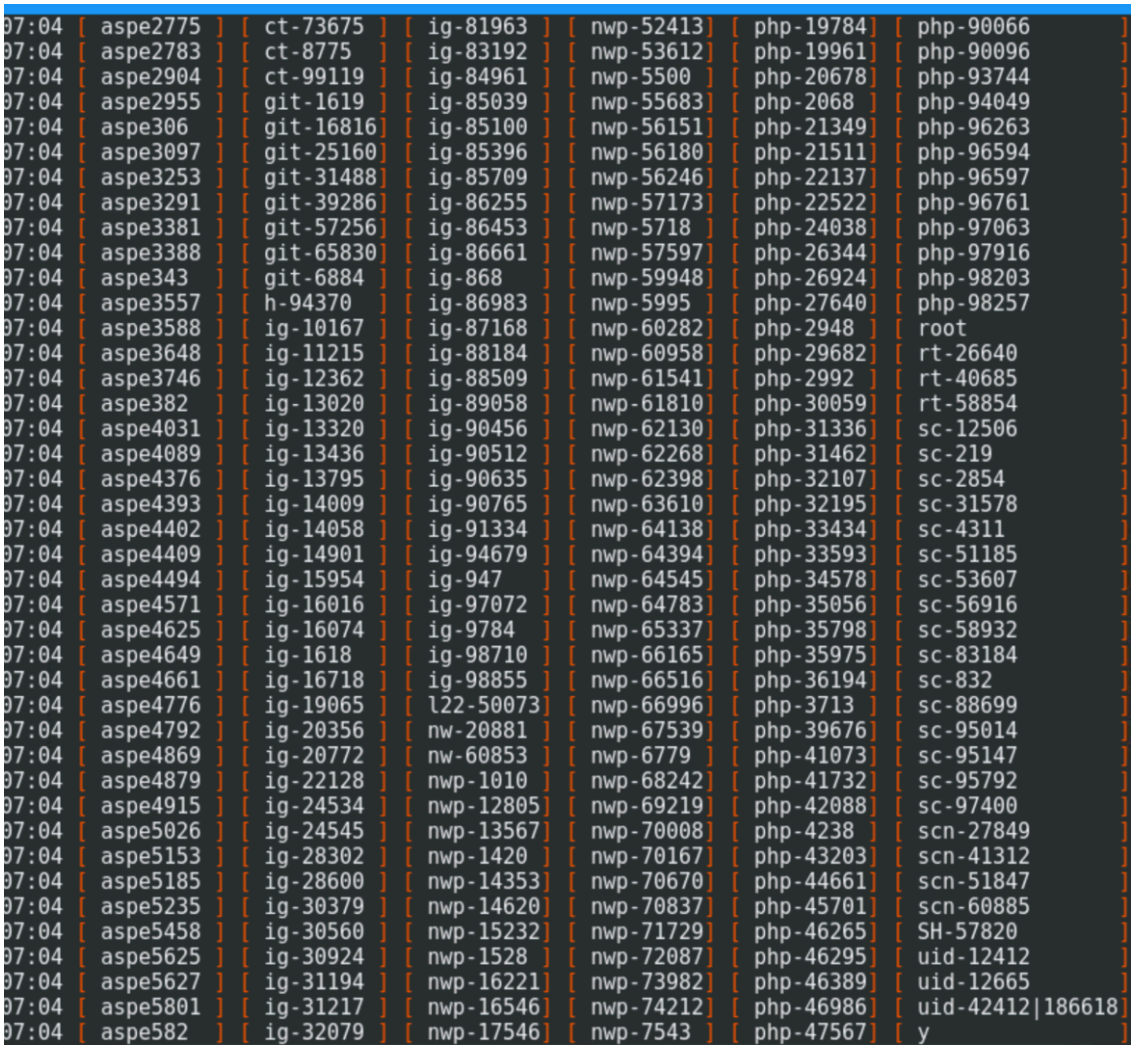
- A nickname is used to join the IRC server
- The channel where the victim joins is often marked by either a platform name (e.g., apache) or a member name (e.g., juice)
- Sometimes auth is added
- The IRC server

Campaigns

After connecting to the IRC server, we discovered the actual number of compromised hosts at over 600. On the other hand, by not properly configuring the connection to the server, RUBYCARP has a detection system to kick out unexpected/unwanted users of the server and ban their IP to prevent new connections. It tries to keep the network hidden as much as possible.

The last active domain of this botnet is chat[.]juicessh[.]pro, and we were able to obtain the information below:

- It was created on Monday, May 1, 2023 at 04:30:05 UTC
- 624 nicks [2 ops, 0 halfops, 0 voices, 622 normal]
- VICTIMS by channel at the moment of writing:
    - #juscan1, 176 victims
    - #cfs, 11 victims
    - #php3, 34 victims
    - #sb, 33 victims



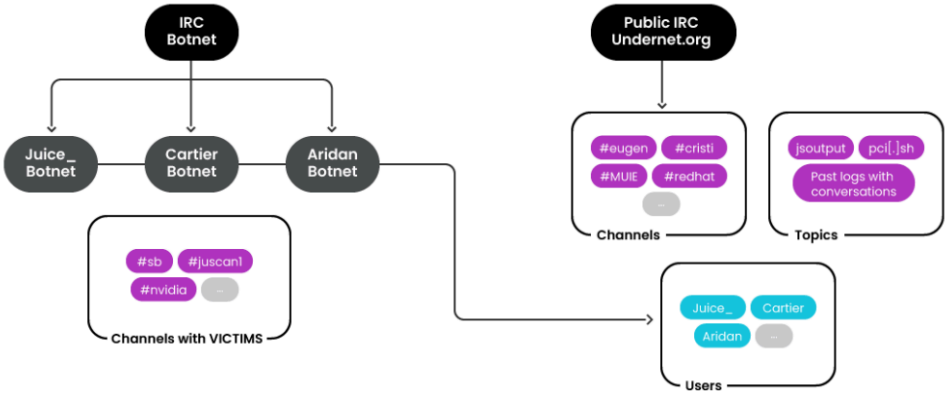
```
07:04 [ aspe2775 ] [ ct-73675 ] [ ig-81963 ] [ nwp-52413] [ php-19784] [ php-90066       ]
07:04 [ aspe2783 ] [ ct-8775  ] [ ig-83192 ] [ nwp-53612] [ php-19961] [ php-90096       ]
07:04 [ aspe2904 ] [ ct-99119 ] [ ig-84961 ] [ nwp-5500  ] [ php-20678] [ php-93744       ]
07:04 [ aspe2955 ] [ git-1619 ] [ ig-85039 ] [ nwp-55683] [ php-2068  ] [ php-94049       ]
07:04 [ aspe306  ] [ git-16816] [ ig-85100 ] [ nwp-56151] [ php-21349] [ php-96263       ]
07:04 [ aspe3097 ] [ git-25160] [ ig-85396 ] [ nwp-56180] [ php-21511] [ php-96594       ]
07:04 [ aspe3253 ] [ git-31488] [ ig-85709 ] [ nwp-56246] [ php-22137] [ php-96597       ]
07:04 [ aspe3291 ] [ git-39286] [ ig-86255 ] [ nwp-57173] [ php-22522] [ php-96761       ]
07:04 [ aspe3381 ] [ git-57256] [ ig-86453 ] [ nwp-5718  ] [ php-24038] [ php-97063       ]
07:04 [ aspe3388 ] [ git-65830] [ ig-86661 ] [ nwp-57597] [ php-26344] [ php-97916       ]
07:04 [ aspe343  ] [ git-6884  ] [ ig-868   ] [ nwp-59948] [ php-26924] [ php-98203       ]
07:04 [ aspe3557 ] [ h-94370   ] [ ig-86983 ] [ nwp-5995  ] [ php-27640] [ php-98257       ]
07:04 [ aspe3588 ] [ ig-10167  ] [ ig-87168 ] [ nwp-60282] [ php-2948  ] [ root           ]
07:04 [ aspe3648 ] [ ig-11215  ] [ ig-88184 ] [ nwp-60958] [ php-29682] [ rt-26640       ]
07:04 [ aspe3746 ] [ ig-12362  ] [ ig-88509 ] [ nwp-61541] [ php-2992  ] [ rt-40685       ]
07:04 [ aspe382  ] [ ig-13020  ] [ ig-89058 ] [ nwp-61810] [ php-30059] [ rt-58854       ]
07:04 [ aspe4031 ] [ ig-13320  ] [ ig-90456 ] [ nwp-62130] [ php-31336] [ sc-12506       ]
07:04 [ aspe4089 ] [ ig-13436  ] [ ig-90512 ] [ nwp-62268] [ php-31462] [ sc-219         ]
07:04 [ aspe4376 ] [ ig-13795  ] [ ig-90635 ] [ nwp-62398] [ php-32107] [ sc-2854        ]
07:04 [ aspe4393 ] [ ig-14009  ] [ ig-90765 ] [ nwp-63610] [ php-32195] [ sc-31578       ]
07:04 [ aspe4402 ] [ ig-14058  ] [ ig-91334 ] [ nwp-64138] [ php-33434] [ sc-4311        ]
07:04 [ aspe4409 ] [ ig-14901  ] [ ig-94679 ] [ nwp-64394] [ php-33593] [ sc-51185       ]
07:04 [ aspe4494 ] [ ig-15954  ] [ ig-947   ] [ nwp-64545] [ php-34578] [ sc-53607       ]
07:04 [ aspe4571 ] [ ig-16016  ] [ ig-97072 ] [ nwp-64783] [ php-35056] [ sc-56916       ]
07:04 [ aspe4625 ] [ ig-16074  ] [ ig-9784  ] [ nwp-65337] [ php-35798] [ sc-58932       ]
07:04 [ aspe4649 ] [ ig-1618   ] [ ig-98710 ] [ nwp-66165] [ php-35975] [ sc-83184       ]
07:04 [ aspe4661 ] [ ig-16718  ] [ ig-98855 ] [ nwp-66516] [ php-36194] [ sc-832         ]
07:04 [ aspe4776 ] [ ig-19065  ] [ l22-50073] [ nwp-66996] [ php-3713  ] [ sc-88699       ]
07:04 [ aspe4792 ] [ ig-20356  ] [ nw-20881 ] [ nwp-67539] [ php-39676] [ sc-95014       ]
07:04 [ aspe4869 ] [ ig-20772  ] [ nw-60853 ] [ nwp-6779  ] [ php-41073] [ sc-95147       ]
07:04 [ aspe4879 ] [ ig-22128  ] [ nwp-1010 ] [ nwp-68242] [ php-41732] [ sc-95792       ]
07:04 [ aspe4915 ] [ ig-24534  ] [ nwp-12805] [ nwp-69219] [ php-42088] [ sc-97400       ]
07:04 [ aspe5026 ] [ ig-24545  ] [ nwp-13567] [ nwp-70008] [ php-4238  ] [ scn-27849     ]
07:04 [ aspe5153 ] [ ig-28302  ] [ nwp-1420 ] [ nwp-70167] [ php-43203] [ scn-41312     ]
07:04 [ aspe5185 ] [ ig-28600  ] [ nwp-14353] [ nwp-70670] [ php-44661] [ scn-51847     ]
07:04 [ aspe5235 ] [ ig-30379  ] [ nwp-14620] [ nwp-70837] [ php-45701] [ scn-60885     ]
07:04 [ aspe5458 ] [ ig-30560  ] [ nwp-15232] [ nwp-71729] [ php-46265] [ SH-57820      ]
07:04 [ aspe5625 ] [ ig-30924  ] [ nwp-1528 ] [ nwp-72087] [ php-46295] [ uid-12412     ]
07:04 [ aspe5627 ] [ ig-31194  ] [ nwp-16221] [ nwp-73982] [ php-46389] [ uid-12665     ]
07:04 [ aspe5801 ] [ ig-31217  ] [ nwp-16546] [ nwp-74212] [ php-46986] [ uid-42412|186618]
07:04 [ aspe582  ] [ ig-32079  ] [ nwp-17546] [ nwp-7543  ] [ php-47567] [ y              ]
```

Based on naming schemes and connection configuration, the apparent group would be composed of users like "juice," "cartier," or "aridan," but there could be more, where each one might be dedicated to a purpose, cryptomining, customized tools, etc. During our investigation, we determined that its IRC server of choice for public and private hosting is undernet.org. The active private IRC networks are **chat[.]juicessh[.]pro** and **sshd[.]run**.

The infrastructure we discovered for RUBYCARP is comprised of a significant number of malicious IPs and domains, rotated regularly and often replaced and emptied of its malicious content as soon as any potential research activity was detected. A full infrastructure list is available here.

How does RUBYCARP Operate?

RUBYCARP uses multiple IRC networks for general communications, but also to manage its botnets and coordinate cryptomining campaigns. An outline of its organization when managing botnets would be as follows:



In one of the logs we acquired, RUBYCARP tends to share the tools it is using, which include many of the tools we have been able to collect through our honeypot, such as:

- Banner
- Masscan
- X (kernel module)
- brute

```
[00:22:51:751] [Eugen-] 11        asterisk   botperl.txt   ip     kk        password   scrr       test     vuln.txt    workedX2.txt
[00:22:51:751] [Eugen-] 22        auto2      brute.php     ip1    list.txt  pmare      search.php u        vv          x
[00:22:51:751] [Eugen-] 3         auto.pl    fileport.py   ip2    logs.txt  pscan2     spawn.sh   umare    wooo        xx
[00:22:51:751] [Eugen-] 3.save    banner     fix           ip3    masscan   pwd        ss         unu.pl   work
[00:22:51:751] [Eugen-] asta ma
```

Communications

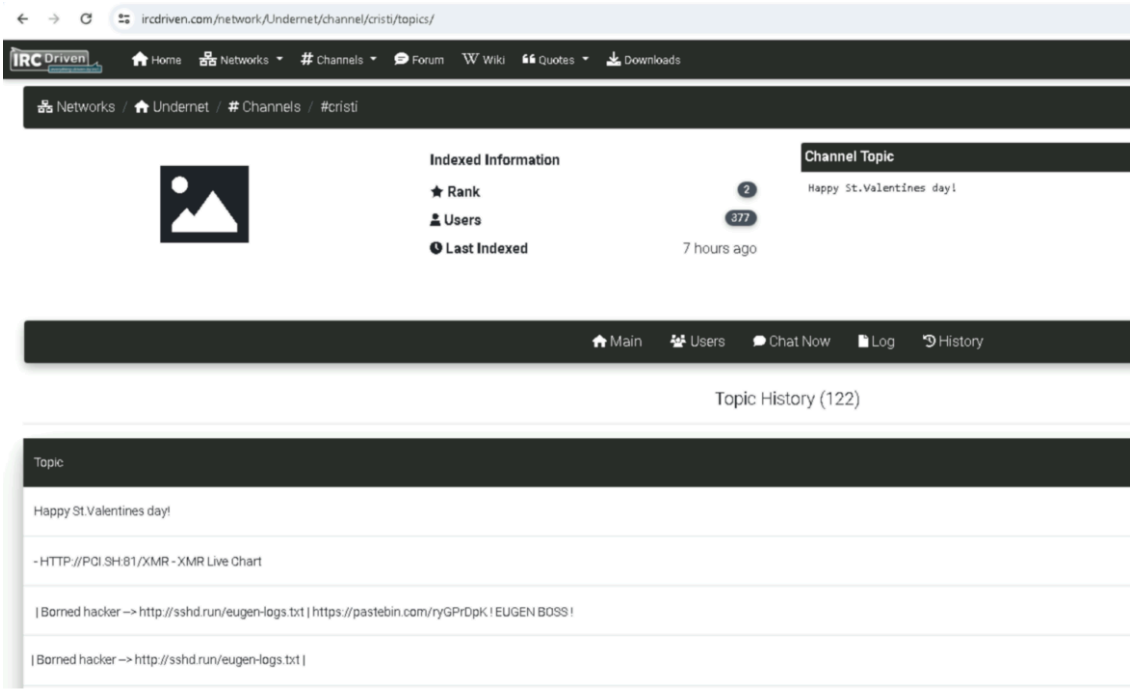
Private IRC

For managing its botnet, RUBYCARP uses a collection of private IRC servers and seems to rotate them regularly. "**Juice.baselinux.net**," "**chat.juicessh.pro**," and others are the latest active ones at the time of writing. Each RUBYCARP campaign gets its own IRC channel and the bots within each channel are then named according to a predefined scheme. We were able to map the observed servers and their respective channels, although, unfortunately, not all of them are still active or accessible.

Public IRC

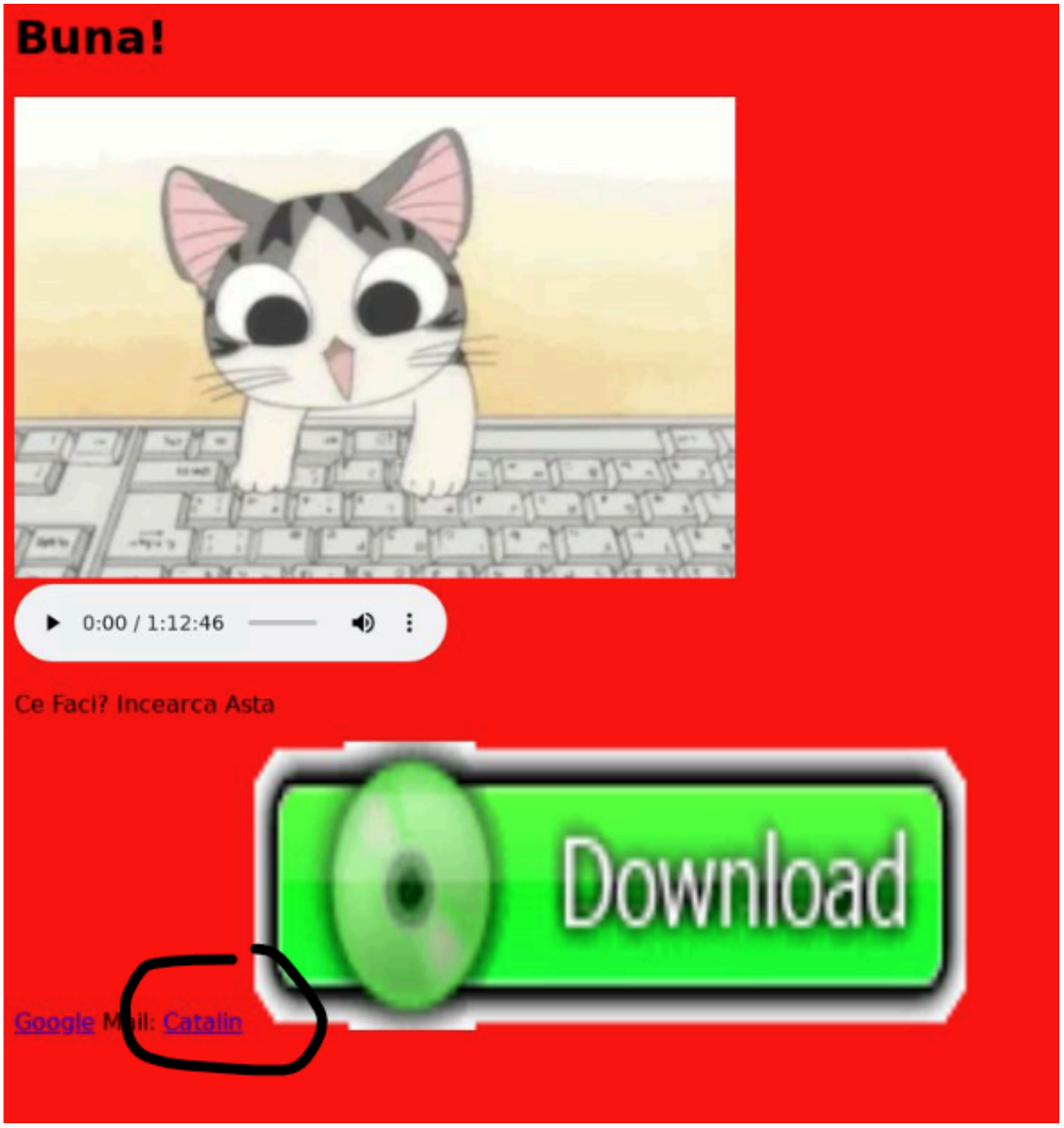
Members

Members of RUBYCARP mainly communicate through an Undernet IRC channel called **#Cristi**. Public logs for the channel show a user (and admin) "**_juice**" interacting with other members of the group in Romanian; we can also see that the channel topic is related to previous or current campaigns, available below.



While we monitored the chats, both actors, juice and Eugen, who own the channel **#Eugen** from which we collected most of the mining setup evidence, were present in channel #Cristi.

Within the user base of the channel #Cristi, which at the time of writing contained 280 users, we identified multiple familiar names of actors who attacked our honeypot. For example, "Catalin" attacked our honeypot on Jan. 8, 2024 from IP **80[.]83[.]124[.]150**. The following image is of the website hosted there at the time of the attack. Notice the attribution to "Catalin" at the bottom.



Another one is "aridan," who we observed in previous attacks with the domain "aridan.men."

The most recurring IRC admins we found within the Shellbot configuration files are "juice," "MUIE," and "Smecher," who also each have their own respective channels for malicious operations. "juice" has been the most prolific in setting up new malicious Shellbot configurations, new servers, and new victim channels. Below is the WHOIS screenshot for the #Cristi channel members we've identified:

juice_, admin

```
15:26 -!- juice_ [~juice@juice.users.undernet.org]
15:26 -!- ircname  : [localhost]
15:26 -!- channels : @#code @#linuxchat @#Alexander @#exploit @#HacKZoNe @#MUIE +#Cristi @#netcat @#hacker @#redhat
15:26 -!- server   : *.undernet.org [The Undernet Underworld]
15:26 -!- away     : Auto away at Sun Jan 21 22:35:27 2024
15:26 -!- account  : juice
15:26 -!- End of WHOIS
```

Smecher, admin

```
15:27 -!- smecher [Foxtrot@kevin-smtp3.livegarneau.info]
15:27 -!-  ircname  : movie
15:27 -!-  server   : *.undernet.org [The Undernet Underworld]
15:27 -!-  away     : Pain looks good on other people.
15:27 -!- End of WHOIS
```

MUIE, admin

```
15:28 -!- MUIE [~zot@GoLaNuL.users.undernet.org]
15:28 -!-  ircname  : zot *
15:28 -!-  channels : #MUIE
15:28 -!-  server   : *.undernet.org [The Undernet Underworld]
15:28 -!-  away     : #MUIE !
15:28 -!-  account  : GoLaNuL
15:28 -!- End of WHOIS
```

Aridan, member

```
- Aridan [Aridan@Aridan.users.undernet.org]
-  ircname  : Aloha
-  channels : +#HacKZoNe #IRCChan #Austria #Location @#MUIE +#Cristi @#Alexander @#Monero @#Owned #Salaj
              #Status @#localhost @#oldhackers @#switch #redhat @#exploit @#darknet @#linuxchat @#SalajOps
              @#global #code @#teen @#hacker @#pepsi @#unix.ro #hero @#u @#security
-  server   : *.undernet.org [The Undernet Underworld]
-  away     : Auto away at Tue Jan 23 16:17:21 2024
-  account  : Aridan
- End of WHOIS
```

Catalin, member

```
!- Catalin [god@bye.users.undernet.org]
!-  ircname  :
!-  channels : @#Eminem +#Cristi
!-  server   : *.undernet.org [The Undernet Underworld]
!-  away     :  alt milog ce face plata pe scannere, detinand permis haxor README.txt. GJ! Esti un schumacher
               al semi-handicapatilor.
!-  account  : bye
!- End of WHOIS
```

Dog, developer

```
dog [dog@dog.shell.oddprotocol.org]
 ircname  :
 channels : #antalya #radiocontact #Allowed
 server   : *.undernet.org [The Undernet Underworld]
End of WHOIS
```

RUBYCARP's Motivations

Cryptomining

RUBYCARP uses its own pools for mining that are hosted on the same domains where it has created the IRC server to control the bots. These custom mining pools allow it to avoid detection from IP-based blocklists, and the usage of common and random ports provides another layer of stealth from simple detection systems. We've also discovered that it has not focused on a single cryptocurrency or mining tool but, instead, has several miners and wallets with activity. All the following IoCs are related to the "juice" threat actor.

Mining Pools:

- juicessh[.]space:443
- juicessh[.]space:4430
- juicessh[.]space:5332
- 91[.]208.206.118:443
- 194[.]163.141.243:4430
- sshd[.]baselinux[.]net
- run[.]psybnc[.]org:443

Known miners

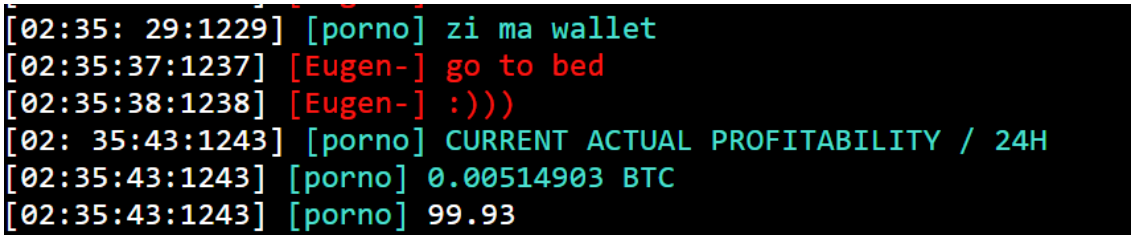
- NanoMiner
- XMrig

Cryptocurrencies

- Monero
- Ethereum
- Ravencoin

The Ravencoin wallet has been particularly prolific. From a wallet checker, its total amount in USD would be over $22,800 received. The wallet has a large number of transactions associated with it and has been active since February 2022, and the last available transaction was mined on March 12, 2024.

There are also several exchanges of wallet information among the members, in an attempt to show how much they have gained from these malicious campaigns. In the excerpt below, user "porno" claimed to have gained 0.00514903 BTC, around $360 USD, within 24 hours.



C3Bash

On top of the already known miners we observed above, we also encountered a custom command-line miner set up called simply "miner," which we named "C3Bash" due to the self-labeling we found. The script in question is signed by "Juice" and it allows a potential user to set up its wallet address with a command line argument, as well as any miner of choice.

Once the user has set up its configurations, the script takes care of downloading, installing, and running the miners in the background, also alerting the user if the script gets killed by an antivirus or simply removed. It also suggests what the CPU usage should be compared to the host, probably to avoid detection. On a victim device, this may result in the running of multiple miners at the same time, effectively reducing both the time it takes for the

attacker to execute the malicious payload and the chances of it being detected, as the execution will now rely on a single script.

The script at the moment supports miners XMRig/Monero, and the script itself was hosted on a now-dead domain "**download[.]c3bash[.]org**."

```
# printing intentions

echo "I will download, setup and run in background Monero CPU miner."
echo "juice c3bash. miners"
echo "If needed, miner in foreground can be started by /var/tmp/c3bash/miner.sh script."
echo "/var/tmp/c3bash/miner.sh script."
echo "Mining will happen to $WALLET wallet."
echo "configure $WALLET done"
if [ ! -z $EMAIL ]; then
  echo "(and $EMAIL email as password to modify wallet options later)"
fi
echo
```

Phishing

We found evidence that RUBYCARP also executes phishing operations to steal financially valuable assets, such as credit card numbers. Based on logs, it appears that it is using this to fund its infrastructure but it is reasonable to think RUBYCARP also uses these for other purposes, or possibly to sell.

In one of the attacks we received against our honeypot in December 2023, we identified a phishing template (letter.html) targeting Danish users and impersonating the Danish logistics company "Bring."

Kære modtager,

Du kan nu hente din pakke hos Netkiosken Aalborg.

Medbring ID og oplys pakkenummer 370730338633121141 og hentekode LM87.
Netkiosken (Kayerødsgade 6, 9000 Aalborg)

For at undgå mest mulig trængsel i pakkeshoppen anbefaler vi, at du henter din pakke i de mindre travle perioder på dagen. Du kan se åbningstider og hvornår der er mindst travlt hos Netkiosken Aalborg via linket nedenfor.

Du kan ansøge om en ny levering på følgende webadresse:

Spor pakke

Venlig hilsen
Bring

I Bring gør vi hverdagen enklere og verden mindre. Vi er 6.000 medarbejdere i Norden, og vi arbejder døgnet rundt for at bringe din pakke hurtigt og sikkert frem på den mest bæredygtige måde. Til glæde for både dig og miljøet. Har du spørgsmål, kan du formentlig finde svar på dem her, hvor du også kan kontakte vores kundeservice.

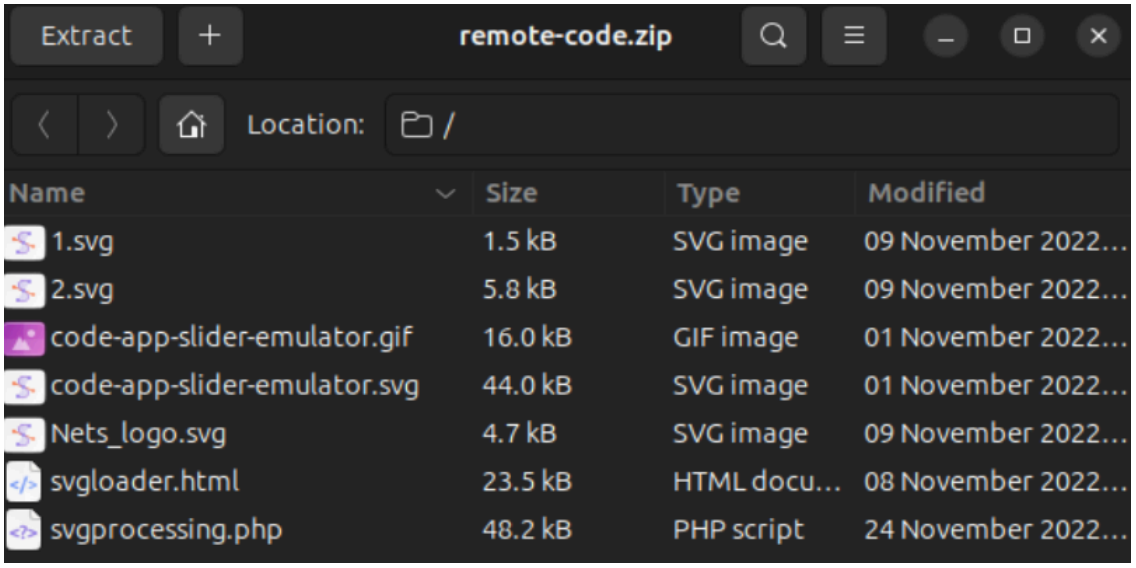
We also discovered a PHP script, named "`ini.inc`," used to send those phishing emails. An email.txt file was found that contained two potential compromised email accounts from which the attackers would send emails: "test@lufaros[.]com" and "maria@cenacop[.]com." At the time of this writing, the domain "lufaros[.]com" is marked as Malicious on VirusTotal.

Analyzing the shellbot code shows that it has specific commands to send emails, and it is likely that this is the template used in the campaigns:

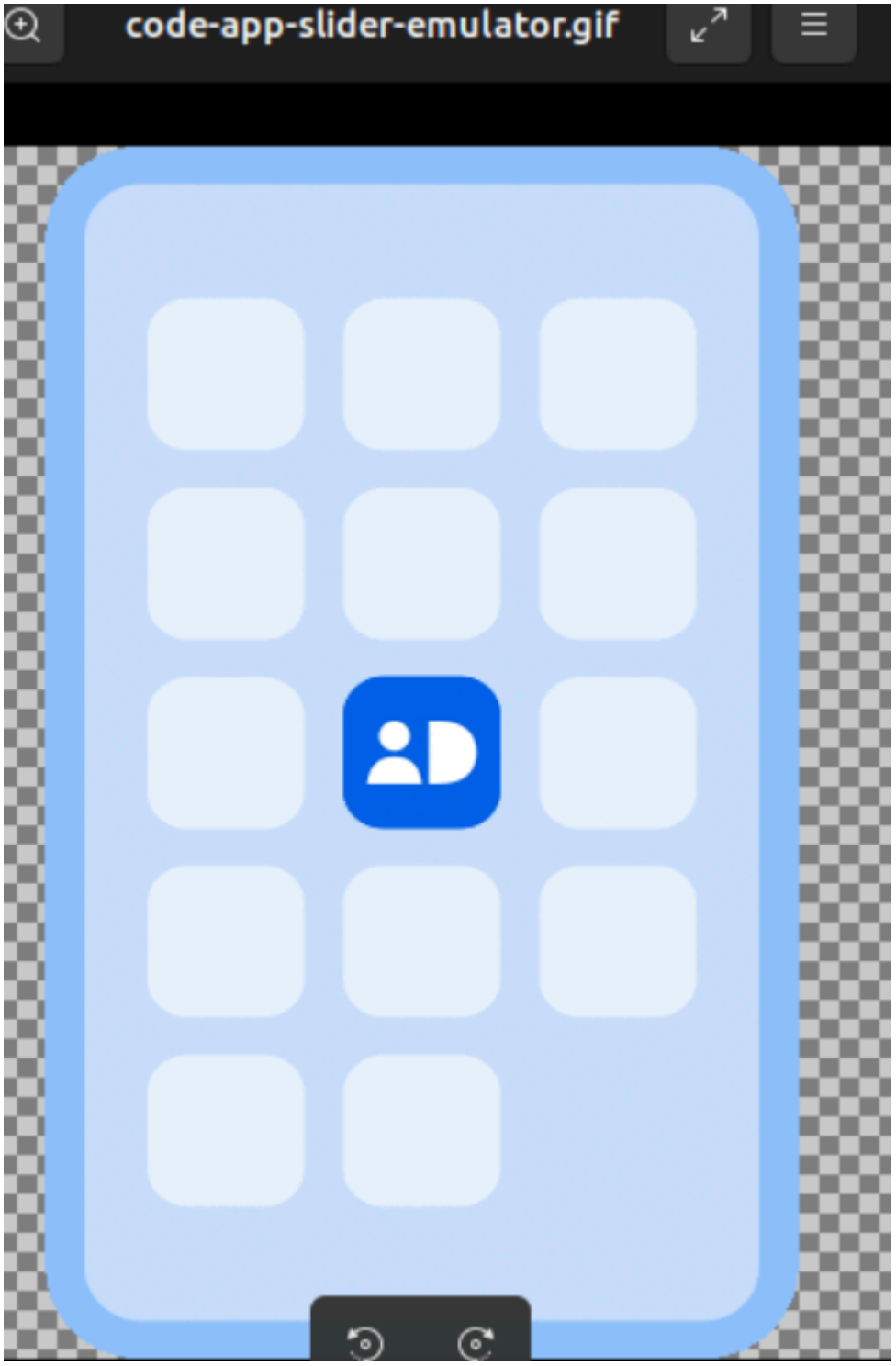
```
sendraw($IRC_cur_socket, "PRIVMSG $printl :!u sendmail <subject> <sender> <recipient> <message>");
```

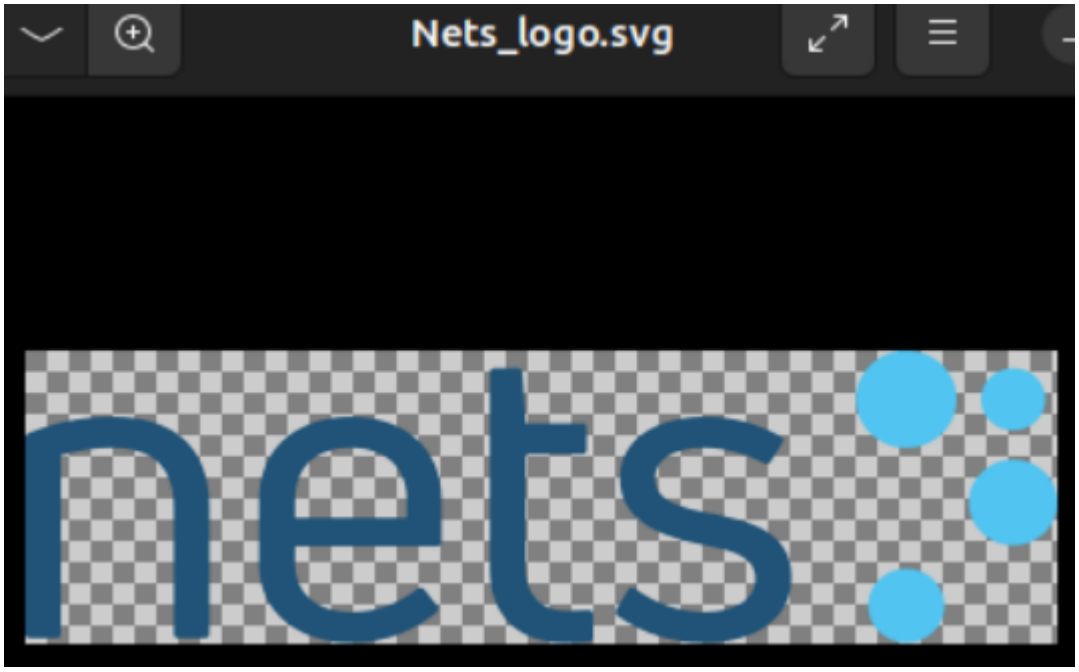
We identified 36 text files containing hundreds of Danish email addresses, some of which were present in both old and recent data leaks. It is reasonable to think that the email addresses may have been the target of the phishing template shown above.

Within the same data, we also identified a Zip file named "**remote_code.zip**." Once extracted, the archive contains a logo image of the European bank Nets. Within the same folder, there are also SVG files containing an "ID Check" verification image and a Visa logo. More images were also found containing a mobile phone layout, as shown below, effectively emulating a Nets home banking application. These would be used to build a convincing phishing landing page.



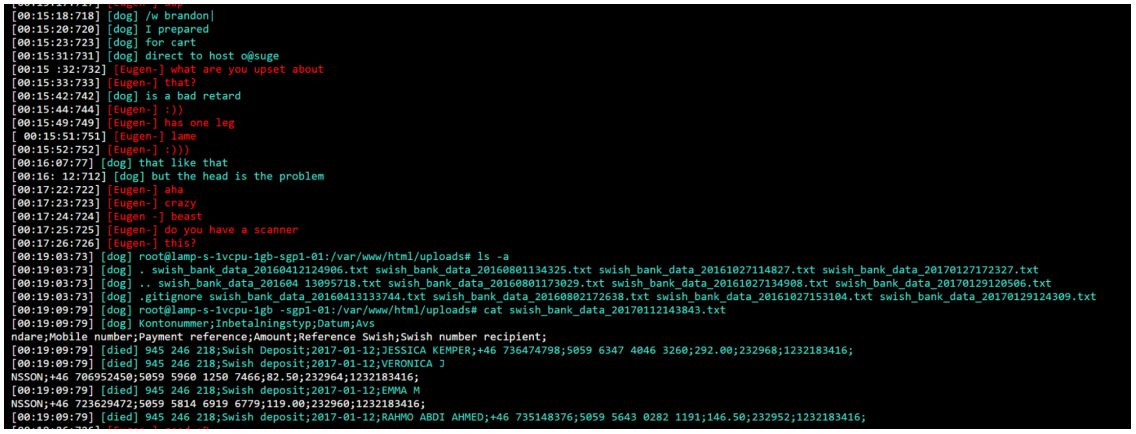
Archives

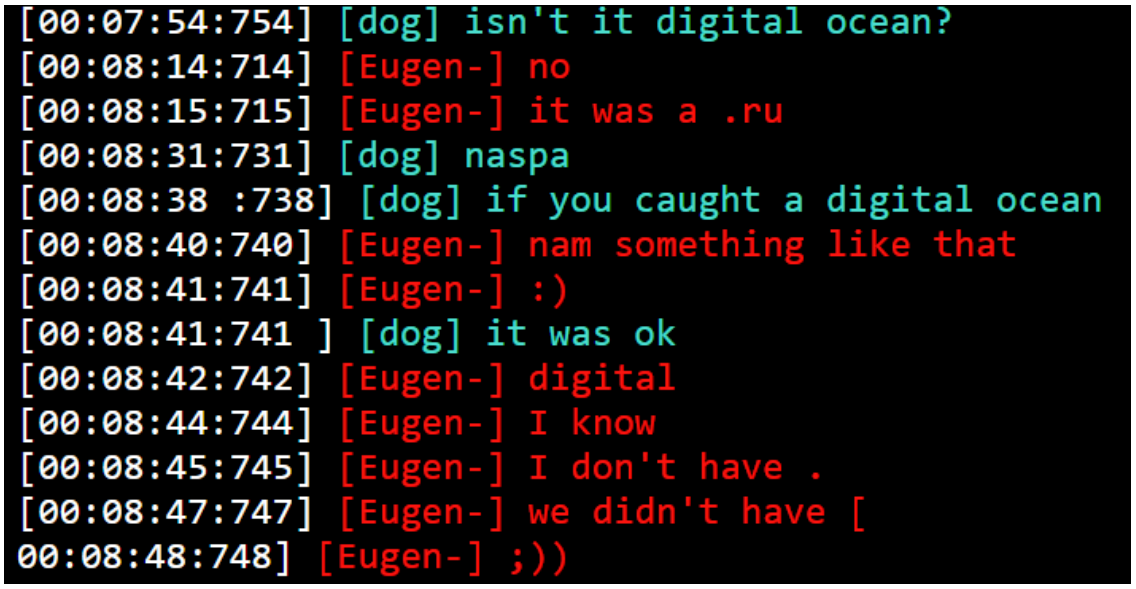

code-app-slider-emulator.gif

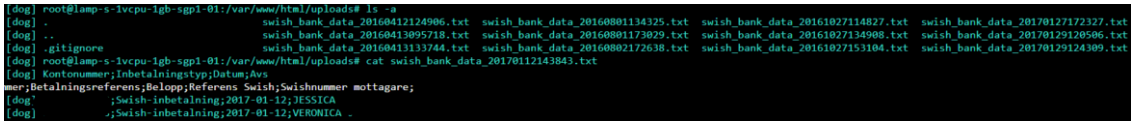


Archive content

Finally, we also found direct evidence of a new domain purchase. In an excerpt below, it is possible to see how the user "dog"/"cartier" is preparing to purchase a new potential domain with stolen credit card data.







The screenshot above shows a conversation where user "dog" lists files which we believe it has stolen. The filenames seem a clear reference to Swedish bank Swish, and the timestamp in the filenames suggests they may have been stolen in 2016. "Dog" also provided credit card information to be used, presumably, by other members. These were printed in clear text within the channel, and have been redacted as they contained payment information.

Given the evidence above, it is plausible that the attackers may rely on phishing templates to collect payment information. It is safe to assume the phishing targets European entities, such as Swish Bank, Nets Bank, and Bring Logistics, among others.

Conclusion

RUBYCARP is a group of Romanian threat actors who have been active for almost a decade. Attribution is always difficult, but they are most likely Romanian and may have some crossover with the "Outlaw APT" group and

others who leverage the Perl Shellbot. These threat actors are also involved in the development and sale of cyber weapons, which isn't very common. They have a large arsenal of tools they have built up over the years which gives them quite a range of flexibility when conducting their operations.

Communications between threat actors hasn't changed very much over the years, with IRC still being very popular. There is also a community aspect to RUBYCARP which is interesting, as they help mentor people who are new to the scene. This does provide some financial benefits to the group since it can then sell them the toolset that it has made.

While RUBYCARP targets known vulnerabilities and conducts brute force attacks, what makes it more dangerous is its post-exploitation tools and the breadth of its capabilities (i.e., Phishing). Defending against this group requires diligent vulnerability management, a robust security posture, and runtime threat detection.

About the author

Test drive the right way to defend the cloud with a security expert

---