Apr 14 2024

NETMANAGEIT

Intelligence Report

A Detailed Analysis of a Sophisticated Decade-Old Botnet Group

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report provides an analysis of a financially motivated Romanian threat actor group called RUBYCARP, which has been active for over 10 years. The group uses botnets, exploits, brute force attacks, and custom tools to infect victims and leverage them for cryptomining, phishing, and selling cyberweapons. The report explores RUBYCARP's tactics, techniques, infrastructure, and motivations.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name
sshd.baselinux.net
Pattern Type
stix
Pattern
[hostname:value = 'sshd.baselinux.net']
Name
run.psybnc.org
Pattern Type
stix
Pattern
[hostname:value = 'run.psybnc.org']
Name
physics.uctm.edu

Pattern Type
stix
Pattern
[hostname:value = 'physics.uctm.edu']
Name
chat.juicessh.pro
Pattern Type
stix
Pattern
[hostname:value = 'chat.juicessh.pro']
Name
juice.baselinux.net
Pattern Type
stix
Pattern
[hostname:value = 'juice.baselinux.net']
Name
download.c3bash.org

Pattern Type
stix
Pattern
[hostname:value = 'download.c3bash.org']
Name
sshd.run
Pattern Type
stix
Pattern
[domain-name:value = 'sshd.run']
Name
juicessh.space
Pattern Type
stix
Pattern
[domain-name:value = 'juicessh.space']
Name
91.208.206.118

Description

ISP: ALEXHOST SRL **OS:** Ubuntu ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC5CoIRtt4DHCwl1I9Ctt5Ed0r+yKd8C9uoMsXPYaVcwGUsXUutaPOqOH2tw6o12mr++HXm5s/vGyfKCzWNiqQ66He7mPKmkIyraZvR81AqfWOb7qhOl1rNKRM0qVaoOMcGHa7l9a00EBUrI4zEfS6p+7JD13FlEvUM2pLf9vAQwUF6DgfhOjd+hgjQQ+u6PgAlQnt7KFmQ9FRDdf9SW46/1q4bJRsHgDH3QoJPk9CDiKUndWVEh7pHPj0jXJgVni8Q9CZlJ+c22zZLVNwGXxNOdG6tHXCSwvfQj65jzK605n3Mamt/w33TahTMuypqoyiv2CvaIqW/Z3Ft49tqcAzn Fingerprint: c8:8b:82:bb:69:9c:b3:6f:03:1f:07:17:72:d7:14:dd Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Mon, 18 Mar 2024 06:39:50 GMT Server: Apache/2.4.29 (Ubuntu) Vary: Accept-Encoding Content-Length: 1148 Content-Type: text/html; charset=UTF-8 ``` ---------- **113:** ``` 113,51296:USERID:UNIX:oident ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.208.206.118']

Name

80.83.124.150

Description

ISP: Bradler & Krantz GmbH & Co. KG **OS:** - ---------- Services: **21:** ``` 500 OOPS: cannot read user list file:/etc/vsftpd.userlist\r\n500 OOPS: priv_sock_get_cmd\r\n ``` ---------- **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDkv4EZ6p/+zuDcG798fbVX2hkLkTUt+IKAHTSDwyFrbk4u LN8/e8Vnu564dzgeuop3PjtyEKnjA7ZBsL5IwkUV16AMEN6Oqaw1Ae8v7B3Cbw2rDhAcrKnpXv1U 7AUG107mSSS+ypd2jGAQ2dbQhwNomgZYo5dIhuzZeD6nMyKgroZ/P54cOaQNHkJHyFbglKdmLTFf 5pSQNufLPkGuR8Uvl2p8SInEcgEbgfz9670vXAvByn+Lu6UuQDfic4B3q8bO0g+Vn6gNOB0/uFoX NAwm35Fj2n1T5kh2VKuQ19XpbbZyD7xDTtXxmQvDTUwvV7HvXxhJWoDBa5+uqH2oj9yf Fingerprint: 4f:90:98:45:d3:f3:70:93:45:5b:5a:2a:97:ac:00:ad Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Thu, 04 Apr 2024 07:23:19 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Wed, 15 Jan 2020 18:05:03 GMT ETag: "25c-59c318c3f0d64" Accept-Ranges: bytes Content-Length: 604 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **113:** ``` 113,51426:USERID:UNIX:oident ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.83.124.150']

Name

194.163.141.243

Description

ISP: Contabo GmbH **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDVmt9ZhlEC7tMIF7LkXgTruyNg2X8V26rzsCq9dmA8zEtl2kHpoo5FzmDVNHWefG5zGw/cpj2w0BKTqjqhz3XGVTuqj4dmJQzvpt0nQ91duYuKdYMVgC0K1e4vAGqh37HBFcX7PJiXl6r+au7927kQKMWuWOKeUnm/xEAzq9IUISXaoxBhwg8R+q73dIe20H0urypr IoqWqh3dcNEuJipqavSCrytCzI1hTTmKPcSmo7rbUb/yPSbguUpESzdfnlv+MRqJ0DoDBgpoQh484/5mHavNaydqf16QsGhNuwzr0+MtRiXiXkXYfNrzuYatRhaHV7VXxNEmVqc72vfT34mzEIHThnt6snz+pbn7bgxe15oN2cR4ebnjNIBSsSA7kvIo0whRH9U7O7lmrKAURcbLvwPyHgYtDDMLl0amdOqa 0xNLaYgmm876Xhssx2ZozPyxvuYreiuasoPp0C4Ycb9d9TwKhgojfgSX76XBoVJZUSJnZ9GkCpo+cKmL7SVQIqk= Fingerprint: 8d:da:44:81:11:29:ee:37:b2:16:74:16:36:2b:e4:01 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 19 Mar 2024 07:22:07 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Location: https://gitlab.twinsdigitallabs.tech:443/ ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Tue, 09 Apr 2024 02:08:20 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Cache-Control: max-age=0, private, must-revalidate Content-Security-Policy: Etag: W/"c0f042b77dcaad40699c13f97e13c738" Link: ; rel=preload; as=style; type=text/css,; rel=preload; as=style; type=text/css,; rel=preload; as=style; type=text/css Permissions-Policy: interest-cohort=() Pragma: no-cache Set-Cookie: _gitlab_session=c7df3436002043f0e83301f01cfcb345; path=/; expires=Tue, 09 Apr 2024 04:08:20 GMT; secure; HttpOnly; SameSite=None X-Content-Type-Options: nosniff X-Download-Options: noopen X-Frame-Options: SAMEORIGIN X-Permitted-Cross-Domain-Policies: none X-Request-Id: 01HV09T27MXDR62E2XRBZA77TR X-Runtime: 0.140176 X-Ua-Compatible: IE=edge X-Xss-Protection: 1; mode=block Strict-Transport-Security: max-age=63072000 Referrer-Policy: strict-origin-when-cross-origin ``` HEARTBLEED: 2024/04/09 02:08:26 194.163.141.243:443 - SAFE ----------

Pattern Type

stix

Pattern
[ipv4-addr:value = '194.163.141.243']

Malware

Name
C3Bash

Name
Shellbot

Intrusion-Set

Name
RUBYCARP

Vulnerability

Name
CVE-2021-3129
Description
Laravel Ignition contains a file upload vulnerability that allows unauthenticated remote attackers to execute malicious code due to insecure usage of file_get_contents() and file_put_contents().

Attack-Pattern

Name
T1573
ID
T1573
Description
Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.
Name
T1078
ID
T1078
Description
Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems

within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

Name

T1496

ID

T1496

Description

Adversaries may leverage the resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster. (Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://

attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR) Alternatively, they may engage in proxyjacking by selling use of the victims' network bandwidth and IP address to proxyware services.(Citation: Sysdig Proxyjacking)

Name

T1059

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

T1566

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1133

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential

authentication for these services. Services such as [Windows Remote Management] (https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Name

T1583

ID

T1583

Description

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090), including from residential proxy services.(Citation: amnesty_nso_pegasus)(Citation: FBI Proxies Credential Stuffing) (Citation: Mandiant APT29 Microsoft 365 2022) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

Country

Name
Sweden

Name
Denmark

Region

Name
Northern Europe

Name
Europe

Sector

Name
Banking
Description
Credit institutions whose business consists in receiving repayable funds from the public and granting credit. As the bank of banks, central banks are included in this scope.
Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

Hostname

Value
sshd.baselinux.net
run.psybnc.org
physics.uctm.edu
juice.baselinux.net
download.c3bash.org
chat.juicessh.pro

Domain-Name

Value
sshd.run
juicessh.space

IPv4-Addr

Value
91.208.206.118
80.83.124.150
194.163.141.243

External References

- https://sysdig.com/blog/rubycarp-romanian-botnet-group/
- https://otx.alienvault.com/pulse/6616d292df2b5184f84c106d