To the moon and hack: Fake SafeMoon app drops malware to spy on you

welivesecurity.com/2021/10/06/moon-hack-fake-safemoon-cryptocurrency-app-drops-malware-spy/

October 6, 2021

Cryptocurrencies rise and fall, but one thing stays the same – cybercriminals attempt to cash in on the craze

Martina López
6 Oct 2021 - 11:30AM

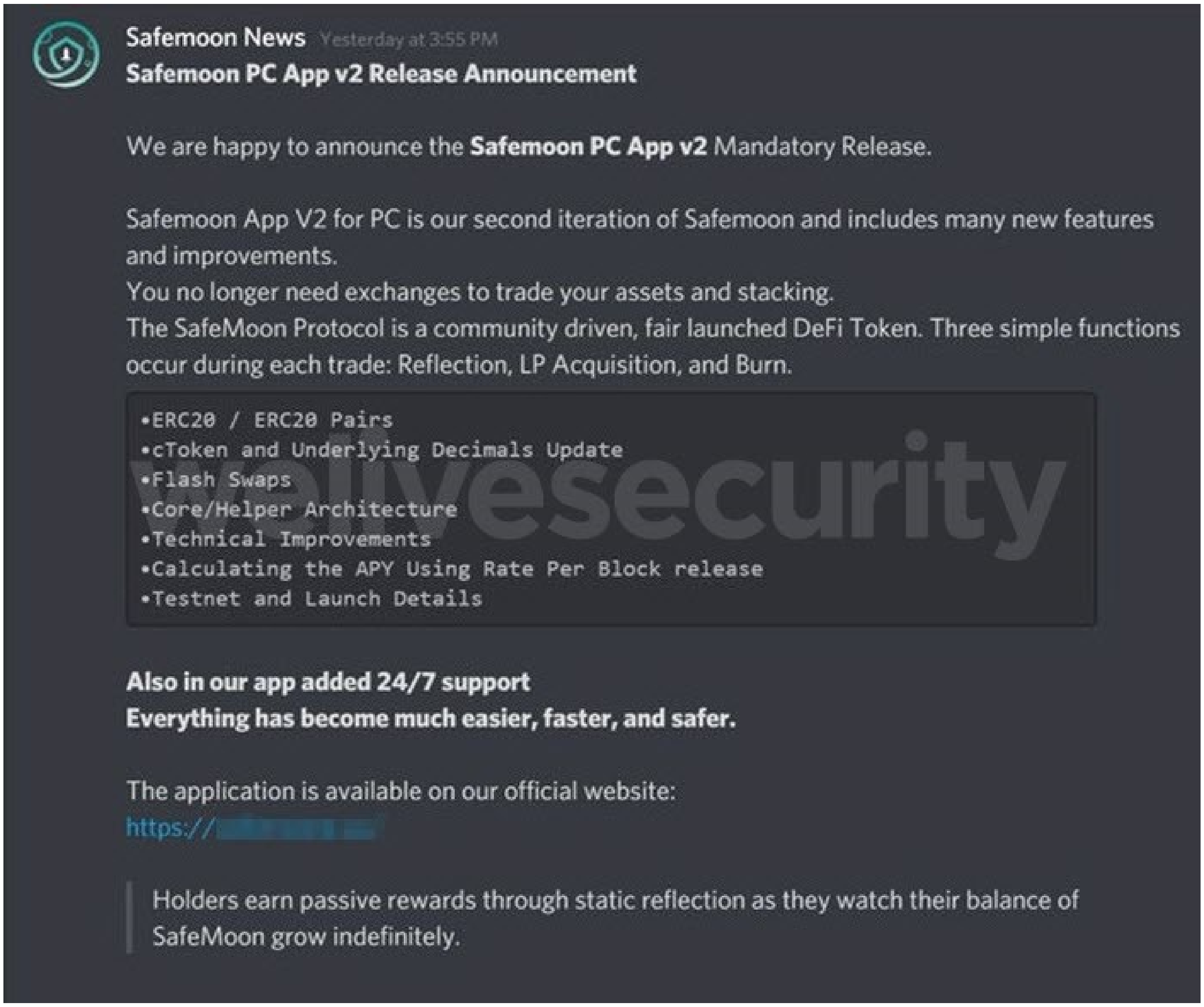
Cryptocurrencies rise and fall, but one thing stays the same – cybercriminals attempt to cash in on the craze

Cybercriminals are trying to capitalize on “the next big thing” in the turbulent cryptocurrency space in an attempt to take remote control of people’s computers and then steal their passwords and money. A campaign spotted recently impersonates the SafeMoon cryptocurrency app and uses a fake update to lure Discord users to a website that distributes a well-known remote access tool (RAT).

SafeMoon is one of the latest altcoins to, well, shoot for the moon. Ever since its inception six months ago, SafeMoon has been highly popular (and duly volatile), with the craze propelled by influencers and numerous enthusiasts on social media. The buzz hasn't escaped the notice of scammers, as swindles targeting cryptocurrency users – including fraud that namedrops celebrities to give it some extra allure – have been running rampant for years.

Houston, we have a problem

The ruse exploiting SafeMoon's sudden popularity begins with a message (Figure 1) that scammers have sent to a number of users on Discord. Posing as the official SafeMoon account, the fraudsters promote a new version of the app.



Safemoon News Yesterday at 3:55 PM
Safemoon PC App v2 Release Announcement

We are happy to announce the **Safemoon PC App v2** Mandatory Release.

Safemoon App V2 for PC is our second iteration of Safemoon and includes many new features and improvements.
You no longer need exchanges to trade your assets and stacking.
The SafeMoon Protocol is a community driven, fair launched DeFi Token. Three simple functions occur during each trade: Reflection, LP Acquisition, and Burn.

```
•ERC20 / ERC20 Pairs
•cToken and Underlying Decimals Update
•Flash Swaps
•Core/Helper Architecture
•Technical Improvements
•Calculating the APY Using Rate Per Block release
•Testnet and Launch Details
```

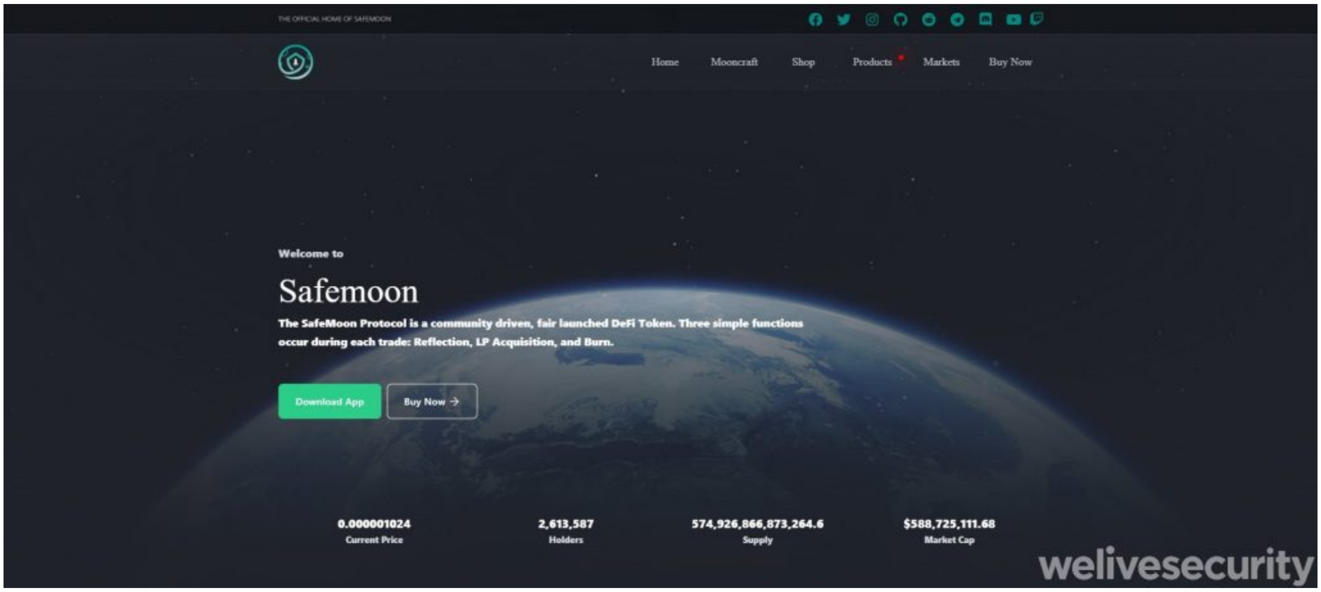
Also in our app added 24/7 support
Everything has become much easier, faster, and safer.

The application is available on our official website:
https://[redacted]

> Holders earn passive rewards through static reflection as they watch their balance of SafeMoon grow indefinitely.

Figure 1. The message impersonating SafeMoon

If you were to click on the URL in the message, you would land on a website (Figure 2) that is apparently designed to look the part of SafeMoon's official site – its old version, to be exact. First reported by a Reddit user in August 2021, the domain name also mimics its legitimate counterpart, except that it adds an extra letter at the end in the hopes that the difference will go unnoticed by most people in their haste to obtain the required "update". As of the time of writing, the malicious site is still up and running.

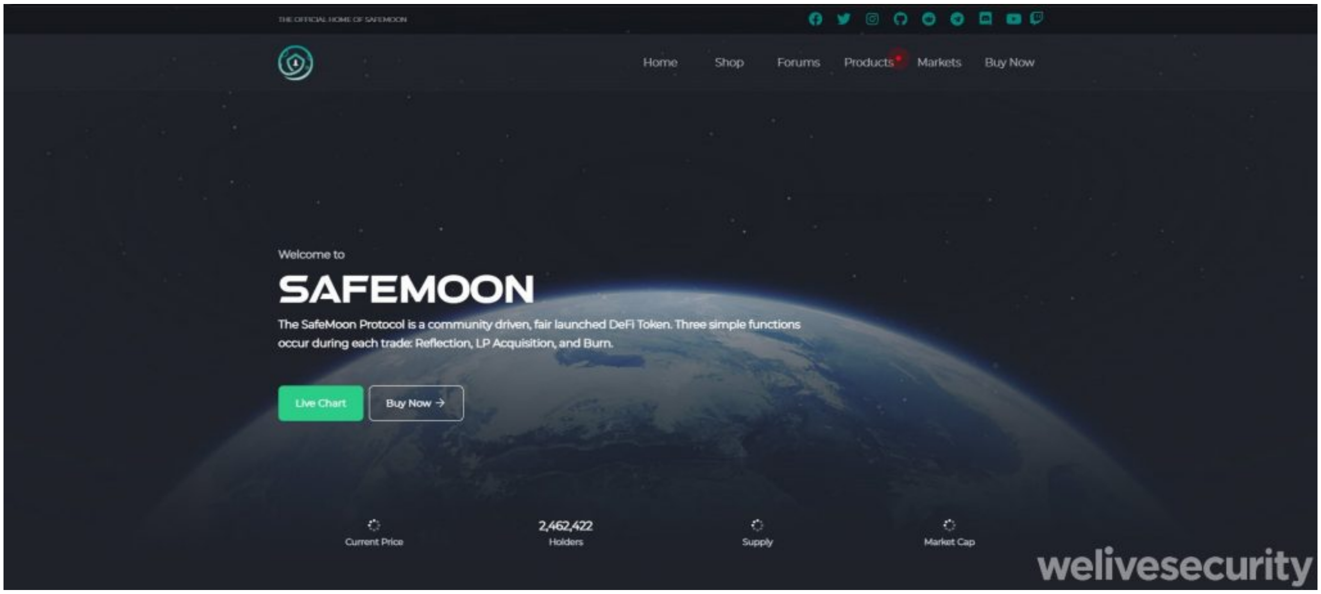


Welcome to

Safemoon

The SafeMoon Protocol is a community driven, fair launched DeFi Token. Three simple functions occur during each trade: Reflection, LP Acquisition, and Burn.

0.000001024	2,613,587	574,926,866,873,264.6	$588,725,111.68
Current Price	Holders	Supply	Market Cap



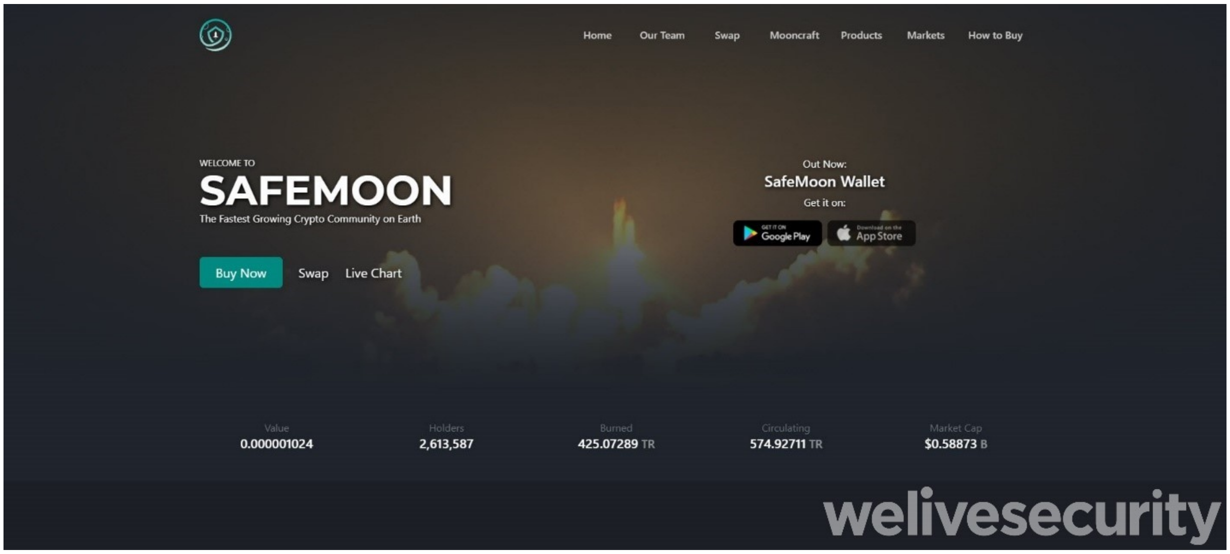
Welcome to

SAFEMOON

The SafeMoon Protocol is a community driven, fair launched DeFi Token. Three simple functions occur during each trade: Reflection, LP Acquisition, and Burn.

	2,462,422		
Current Price	Holders	Supply	Market Cap

Figure 2. The fake (L) versus the legitimate (R) SafeMoon website, August 2021 (source: web.archive.org)



WELCOME TO

SAFEMOON

The Fastest Growing Crypto Community on Earth

Out Now:

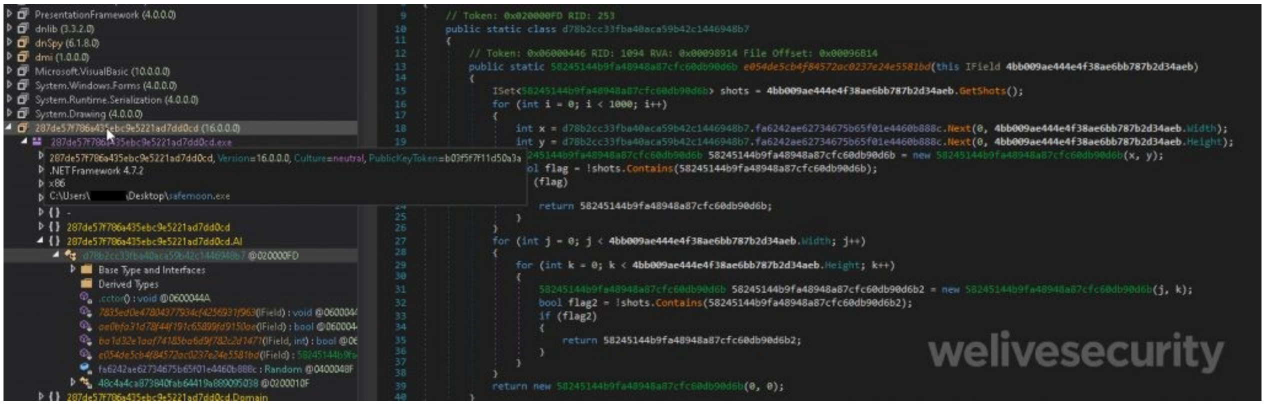
SafeMoon Wallet

Get it on:

Value	Holders	Burned	Circulating	Market Cap
0.000001024	2,613,587	425.07289 TR	574.92711 TR	$0.58873 B

Figure 3. The official SafeMoon website, early October 2021

All external links on the site are legitimate, except for the arguably most important one – the link that prompts you to download the “official” SafeMoon app from the Google Play Store. Instead of the SafeMoon app for Android devices, it downloads a payload that includes rather common, off-the-shelf Windows software that can be used both for legitimate and nefarious ends.



```
PresentationFramework (4.0.0.0)
dnlib (3.3.2.0)
dnSpy (6.1.8.0)
dmi (1.0.0.0)
Microsoft.VisualBasic (10.0.0.0)
System.Windows.Forms (4.0.0.0)
System.Runtime.Serialization (4.0.0.0)
System.Drawing (4.0.0.0)
287de57f786a435ebc9e5221ad7dd0cd (16.0.0.0)
  287de57f786a435ebc9e5221ad7dd0cd.exe
    287de57f786a435ebc9e5221ad7dd0cd, Version=16.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
    .NET Framework 4.7.2
    x86
    C:\Users\[redacted]\Desktop\safemoon.exe
    {} -
    {} 287de57f786a435ebc9e5221ad7dd0cd
    {} 287de57f786a435ebc9e5221ad7dd0cd.AI
      d78b2cc33fba40aca59b42c1446948b7 @020000FD
        Base Type and Interfaces
        Derived Types
        .cctor() : void @0600044A
        7835ed0e47804377934cf4256931f963(IField) : void @060004
        ae0bfa31d78f44f191c65899fd9150ae(IField) : bool @060004
        ba1d32e1aaf74185ba6d9f782c2d1477(IField, int) : bool @06
        e054de5cb4f84572ac0237e24e5581bd(IField) : 58245144b9fa
        fa6242ae62734675b65f01e4460b888c : Random @0400048F
      48c4a4ca873840fab64419a889095038 @0200010F
    {} 287de57f786a435ebc9e5221ad7dd0cd.Domain
```

```
// Token: 0x020000FD RID: 253
public static class d78b2cc33fba40aca59b42c1446948b7
{
    // Token: 0x06000446 RID: 1094 RVA: 0x00098914 File Offset: 0x00096B14
    public static 58245144b9fa48948a87cfc60db90d6b e054de5cb4f84572ac0237e24e5581bd(this IField 4bb009ae444e4f38ae6bb787b2d34aeb)
    {
        ISet<58245144b9fa48948a87cfc60db90d6b> shots = 4bb009ae444e4f38ae6bb787b2d34aeb.GetShots();
        for (int i = 0; i < 1000; i++)
        {
            int x = d78b2cc33fba40aca59b42c1446948b7.fa6242ae62734675b65f01e4460b888c.Next(0, 4bb009ae444e4f38ae6bb787b2d34aeb.Width);
            int y = d78b2cc33fba40aca59b42c1446948b7.fa6242ae62734675b65f01e4460b888c.Next(0, 4bb009ae444e4f38ae6bb787b2d34aeb.Height);
            245144b9fa48948a87cfc60db90d6b 58245144b9fa48948a87cfc60db90d6b = new 58245144b9fa48948a87cfc60db90d6b(x, y);
            ol flag = !shots.Contains(58245144b9fa48948a87cfc60db90d6b);
             (flag)

                return 58245144b9fa48948a87cfc60db90d6b;
            }
        }
        for (int j = 0; j < 4bb009ae444e4f38ae6bb787b2d34aeb.Width; j++)
        {
            for (int k = 0; k < 4bb009ae444e4f38ae6bb787b2d34aeb.Height; k++)
            {
                58245144b9fa48948a87cfc60db90d6b 58245144b9fa48948a87cfc60db90d6b2 = new 58245144b9fa48948a87cfc60db90d6b(j, k);
                bool flag2 = !shots.Contains(58245144b9fa48948a87cfc60db90d6b2);
                if (flag2)
                {
                    return 58245144b9fa48948a87cfc60db90d6b2;
                }
            }
        }
        return new 58245144b9fa48948a87cfc60db90d6b(0, 0);
    }
```

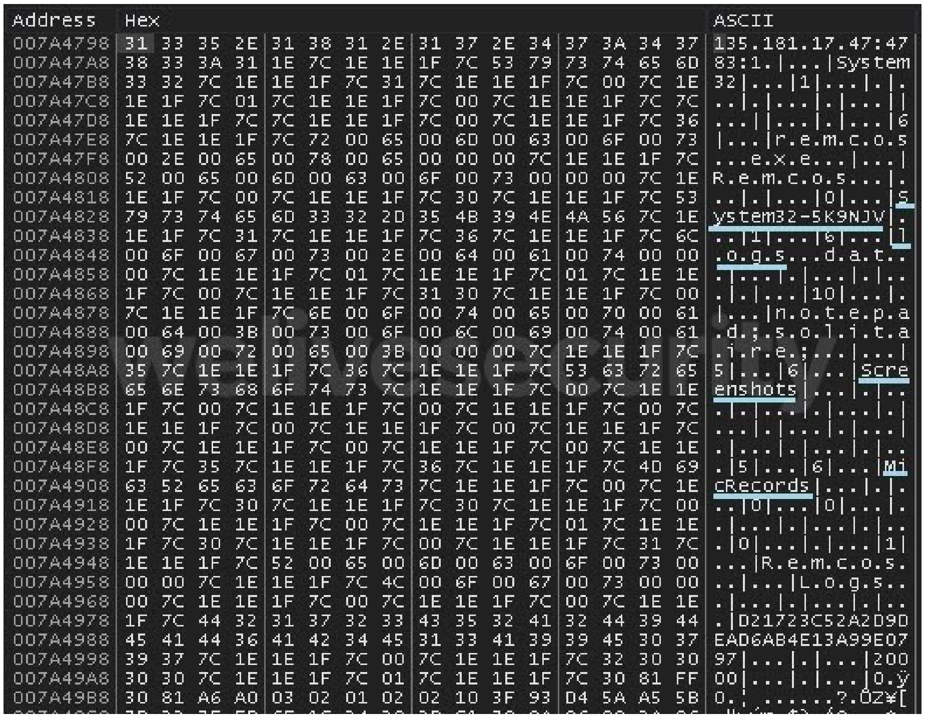
Figure 4. The development section of the obfuscated malicious app

Upon execution, the installer (Safemoon-App-v2.0.6.exe) will drop several files on the system, including a RAT called Remcos. While touted as a legitimate tool, this RAT is also being peddled for sale in underground forums, which also earned it an official alert from US authorities shortly after the tool was released. If used for evil ends, a RAT is often understood to stand for a “remote access trojan” instead.

Remcos has since been deployed in a number of campaigns, both by cybercrime and cyberespionage groups. Indeed, just a few months ago ESET researchers spotted Remcos in what they nicknamed “Operation Spalax”, where threat actors took aim at a slew of organizations in Colombia.

As is customary with RATs, Remcos gives the attacker a backdoor into the victim’s computer and is used to gather sensitive data from the victim. It is operated via a command and control (C&C) server whose IP address is injected into the downloaded files. Remcos’s capabilities include theft of login credentials from various web browsers, logging keystrokes, hijacking the webcam, capturing audio from the victim’s microphone, downloading and executing additional malware on the machine … the whole nine yards, really.

A cursory look at the RAT’s configuration file (Figure 5) provides an idea of its extensive functionality.



```
Address   Hex                                                  ASCII
007A4798  31 33 35 2E 31 38 31 2E 31 37 2E 34 37 3A 34 37  135.181.17.47:47
007A47A8  38 33 3A 31 1E 7C 1E 1E 1F 7C 53 79 73 74 65 6D  83:1.|...|System
007A47B8  33 32 7C 1E 1E 1F 7C 31 7C 1E 1E 1F 7C 00 7C 1E  32|...|1|...|.|.
007A47C8  1E 1F 7C 01 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 7C  ..|.|...|.|...||
007A47D8  1E 1E 1F 7C 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 36  ...||...|.|...|6
007A47E8  7C 1E 1E 1F 7C 72 00 65 00 6D 00 63 00 6F 00 73  |...|r.e.m.c.o.s
007A47F8  00 2E 00 65 00 78 00 65 00 00 00 7C 1E 1E 1F 7C  ...e.x.e...|...|
007A4808  52 00 65 00 6D 00 63 00 6F 00 73 00 00 00 7C 1E  R.e.m.c.o.s...|.
007A4818  1E 1F 7C 00 7C 1E 1E 1F 7C 30 7C 1E 1E 1F 7C 53  ..|.|...|0|...|S
007A4828  79 73 74 65 6D 33 32 2D 35 4B 39 4E 4A 56 7C 1E  ystem32-5K9NJV|.
007A4838  1E 1F 7C 31 7C 1E 1E 1F 7C 36 7C 1E 1E 1F 7C 6C  ..|1|...|6|...|l
007A4848  00 6F 00 67 00 73 00 2E 00 64 00 61 00 74 00 00  .o.g.s...d.a.t..
007A4858  00 7C 1E 1E 1F 7C 01 7C 1E 1E 1F 7C 01 7C 1E 1E  .|...|.|...|.|..
007A4868  1F 7C 00 7C 1E 1E 1F 7C 31 30 7C 1E 1E 1F 7C 00  .|.|...|10|...|.
007A4878  7C 1E 1E 1F 7C 6E 00 6F 00 74 00 65 00 70 00 61  |...|n.o.t.e.p.a
007A4888  00 64 00 3B 00 73 00 6F 00 6C 00 69 00 74 00 61  .d.;.s.o.l.i.t.a
007A4898  00 69 00 72 00 65 00 3B 00 00 00 7C 1E 1E 1F 7C  .i.r.e.;...|...|
007A48A8  35 7C 1E 1E 1F 7C 36 7C 1E 1E 1F 7C 53 63 72 65  5|...|6|...|Scre
007A48B8  65 6E 73 68 6F 74 73 7C 1E 1E 1F 7C 00 7C 1E 1E  enshots|...|.|..
007A48C8  1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C  .|.|...|.|...|.|
007A48D8  1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C  ...|.|...|.|...|
007A48E8  00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E  .|...|.|...|.|..
007A48F8  1F 7C 35 7C 1E 1E 1F 7C 36 7C 1E 1E 1F 7C 4D 69  .|5|...|6|...|Mi
007A4908  63 52 65 63 6F 72 64 73 7C 1E 1E 1F 7C 00 7C 1E  cRecords|...|.|.
007A4918  1E 1F 7C 30 7C 1E 1E 1F 7C 30 7C 1E 1E 1F 7C 00  ..|0|...|0|...|.
007A4928  00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 01 7C 1E 1E  .|...|.|...|.|..
007A4938  1F 7C 30 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 31 7C  .|0|...|.|...|1|
007A4948  1E 1E 1F 7C 52 00 65 00 6D 00 63 00 6F 00 73 00  ...|R.e.m.c.o.s.
007A4958  00 00 7C 1E 1E 1F 7C 4C 00 6F 00 67 00 73 00 00  ..|...|L.o.g.s..
007A4968  00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E  .|...|.|...|.|..
007A4978  1F 7C 44 32 31 37 32 33 43 35 32 41 32 44 39 44  .|D21723C52A2D9D
007A4988  45 41 44 36 41 42 34 45 31 33 41 39 39 45 30 37  EAD6AB4E13A99E07
007A4998  39 37 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 32 30 30  97|...|.|...|200
007A49A8  30 30 7C 1E 1E 1F 7C 01 7C 1E 1E 1F 7C 30 81 FF  00|...|.|...|0.ÿ
007A49B8  30 81 A6 A0 03 02 01 02 02 10 3F 93 D4 5A A5 5B  0.¦.......?.ÔZ¥[
```

Figure 5. Part of the Remcos configuration file binary showing some of what the RAT is after

Strap yourself in

A few basic precautions will go a long way towards staying safe from these scams:

- Be wary of any out-of-the-blue communications, be it via email, social media, texts or other channels
- Don't click on links in such messages, especially when they come from an unverified source
- Be alert to irregularities in URLs – you're better off typing it in yourself
- Use strong and unique passwords or passphrases and, wherever available, two-factor authentication (2FA)
- Use comprehensive security software

When it comes to investing in cryptocurrencies, you need to proceed with caution, and not just because the market is rife with investment fraud, fake giveaways and other scams. But surely you know the drill by now.

Indicators of Compromise (IoCs)

SHA-256 hash	ESET detection name
035041983ADCFB47BBA63E81D2B98FA928FB7E022F51ED4A897366542D784E5B	A Variant of MSIL/Injector.VQB

The files downloaded later as part of the Remcos "package" are detected by ESET products as Win32/Rescoms.B.

6 Oct 2021 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion