Tax Customer Campaign Infects Targets with RAT

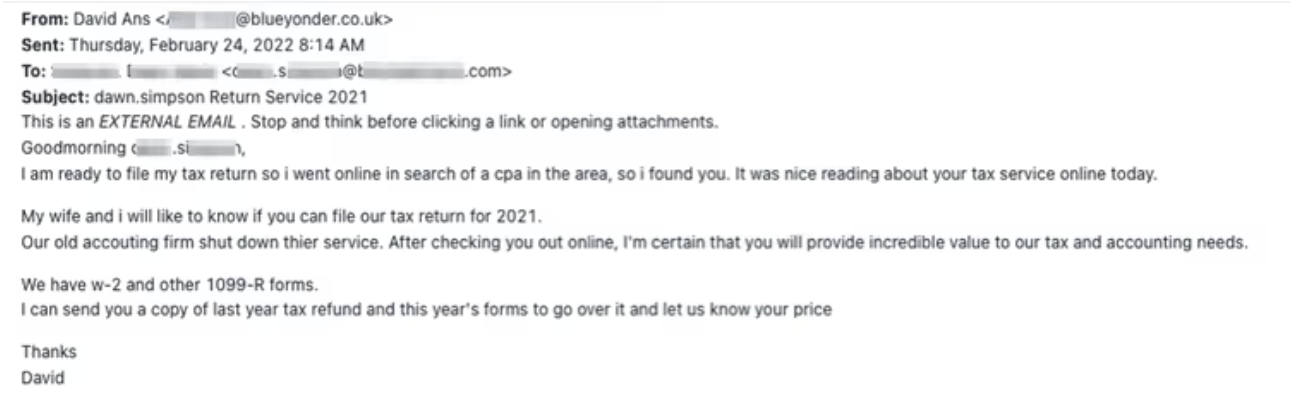
Published: 2022-04-06 · Archived: 2026-04-02 10:57:20 UTC

With the US tax deadline looming, inboxes everywhere are awash in a sea of messages advising their users to exercise caution and due diligence to prevent fraud and identity theft.

If receiving and downloading files is necessary for business functions, it becomes difficult to avoid downloading a malicious file. Some measure of risk is unavoidable, especially if data must be received early in the process of establishing a new client relationship—as is the case for CPAs and tax preparation service providers.

The threat intelligence team at Abnormal Security recently observed a timely campaign targeting accounting and tax professionals.

Between February 24, 2022, and March 4, 2022, we identified more than 130 emails from threat actors posing as potential clients. The emails claimed the sender was attempting to locate a CPA ahead of April's deadline and obtain individual or business tax filing services for this year. However, each email delivered not the promised tax documents but instead an obfuscated version of the remote access tool (RAT) Sorillus.



From: David Ans <[redacted]@blueyonder.co.uk>
Sent: Thursday, February 24, 2022 8:14 AM
To: [redacted]
Subject: dawn.simpson Return Service 2021
This is an *EXTERNAL EMAIL* . Stop and think before clicking a link or opening attachments.
Goodmorning [redacted],
I am ready to file my tax return so i went online in search of a cpa in the area, so i found you. It was nice reading about your tax service online today.

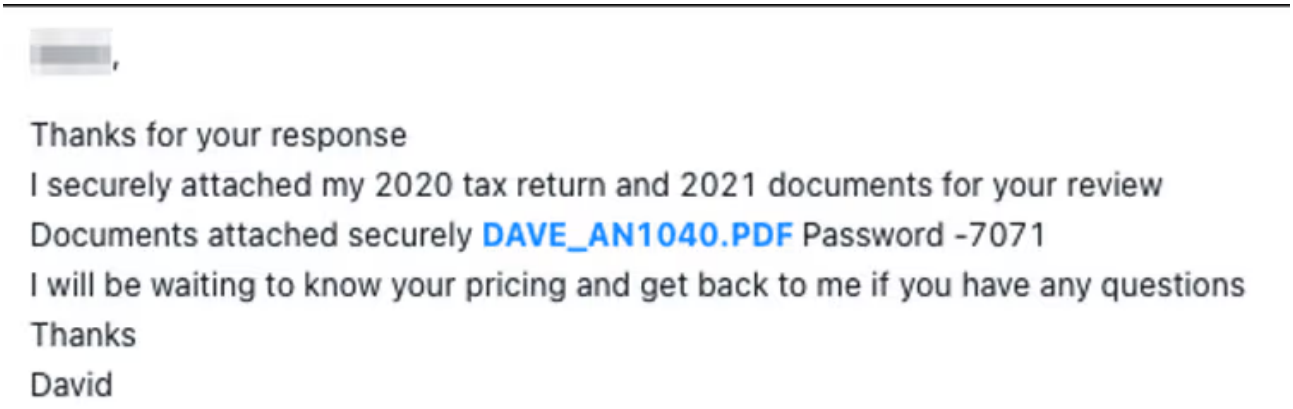
My wife and i will like to know if you can file our tax return for 2021.
Our old accouting firm shut down thier service. After checking you out online, I'm certain that you will provide incredible value to our tax and accounting needs.

We have w-2 and other 1099-R forms.
I can send you a copy of last year tax refund and this year's forms to go over it and let us know your price

Thanks
David

Initial contact by bad actors with potential victim

After initial contact with the service provider was made, the actors sent follow-up messages containing a mega[.]nz file share link to Sorillus RAT. The link was hiding underneath the text, pretending to be a simple PDF file attachment.

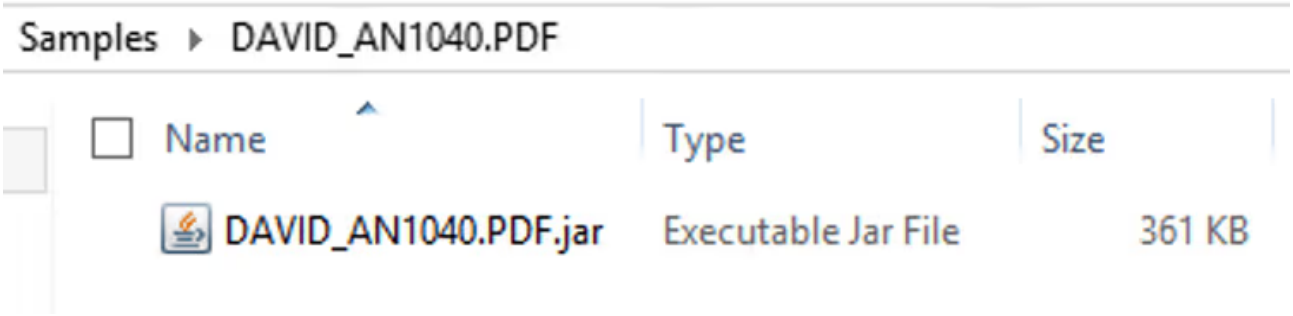


Email with "DAVE_AN1040.PDF" text hiding suspicious mega[.]nz file-sharing link

Emails were sent from 10 different addresses but were easily identifiable because the subject lines of the emails followed a similar pattern. Each referenced business and individual tax documents appropriate for the service supposedly being offered.

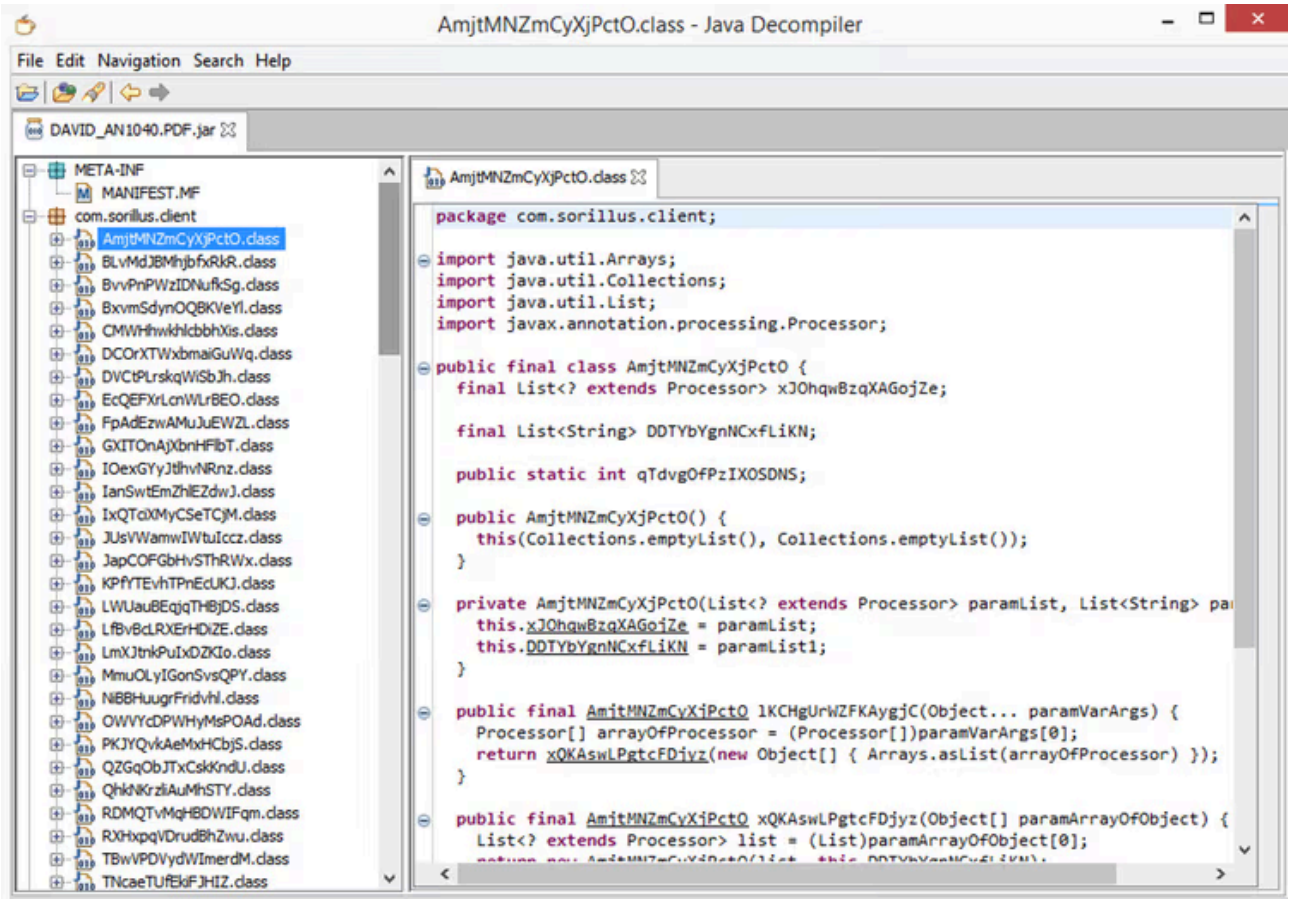
Threat Analysis

Mega[.]nz was used to send the malicious file as an anti-detection technique, and upon visiting the supplied link, a file masquerading as a PDF named "DAVE_AN1040.PDF" was downloaded. In reality, though, the file was a .ZIP archive containing a .JAR file.



Malicious .JAR file inside ZIP archive posing as a PDF

The .JAR file had two packages, obfuscated with what appears to be the Zelix obfuscator.



Even with the obfuscation, the name of the first package is in clear text, *com.sorillus.client*. Sorillus is a RAT that runs in Windows, Linux, and Mac OS, as we can see after some deobfuscation.

```
public static mmMlJzCNxqlmAiLP uOeRpAHTQxWAwldm(Object[] paramArrayOfObject) {
  if (PFOoATOMIjeEpeMA == null) {
    String str = System.getProperty("os.name").toLowerCase();
    if (str.contains("win")) {
      PFOoATOMIjeEpeMA = mmMlJzCNxqlmAiLP.jOrdZnciYiHbbaeP;
    } else if (str.contains("nix") || str.contains("nux") || str.contains("aix")) {
      PFOoATOMIjeEpeMA = mmMlJzCNxqlmAiLP.GGLIXFtPTiHsoILH;
    } else if (str.contains("mac")) {
      PFOoATOMIjeEpeMA = mmMlJzCNxqlmAiLP.MmqAbbJsuHwSEmnO;
    }
  }
```

Java class identifying different compatible operating systems

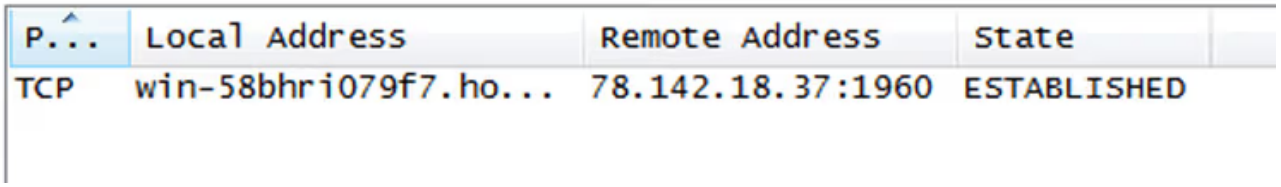
The tool is able to collect the victim's system information including hardware ID, username, language, webcam, and OS.

```
package com.sorillus.client;

import ililililiiliiiiiiiiili.xTuIRejxTuvsfpTC;
import java.awt.GraphicsEnvironment;
import java.net.InetAddress;
import java.util.Locale;

@UWSKfdMdLMCpZSAT(V = 0)
public class OWVYcDPWHyMsPOAd extends sdAmkKL1kVGvyZfI {
  @xTuIRejxTuvsfpTC("hardwareID")
  public String NydmLyjSGLEUIoTB;

  @xTuIRejxTuvsfpTC("username")
  public String wrChghqyJOhLDFYF;

  @xTuIRejxTuvsfpTC("country")
  public String NVolquGzDGsQObtb;

  @xTuIRejxTuvsfpTC("language")
  public String iecmaQcPZVqFxQFU;

  @xTuIRejxTuvsfpTC("webcam")
  public int IgHAnFuAcBxVirSG;

  @xTuIRejxTuvsfpTC("headless")
  public boolean VbRqLGhWIzHGCURu;

  @xTuIRejxTuvsfpTC("operatingSystem")
  public String yoHIgTgYVxRzDruR;

  @xTuIRejxTuvsfpTC("clientVersion")
  public float BzDhrqbWrKmqNgqC;

  public OWVYcDPWHyMsPOAd() {
    String str1;
    String str2 = System.getProperty("user.name");
    boolean bool1 = yTeCQxWBIbbHIECh.LdPYHOgHpRZaeciA;
    boolean bool2 = GraphicsEnvironment.isHeadless();
    try {
      str1 = InetAddress.getLocalHost().getHostName() + "/" + str2;
    } catch (Exception exception) {
      str1 = str2;
    }
    try {
      this.NydmLyjSGLEUIoTB = PKJYQvkAeMxHCbjS.bbVlBIkhxIlukVMs(new Object[0]);
      this.wrChghqyJOhLDFYF = str1;
      this.NVolquGzDGsQObtb = jtUewubkmXOhEiRN.xacpaFASONdycPdm;
      this.iecmaQcPZVqFxQFU = jtUewubkmXOhEiRN.OzaGzkWoxFFiAswB;
      this.IgHAnFuAcBxVirSG = 0;
      this.VbRqLGhWIzHGCURu = bool2;
      this.yoHIgTgYVxRzDruR = System.getProperty("os.name");
      this.BzDhrqbWrKmqNgqC = LfBvBcLRXErHDiZE.vJmnmbCxaXaRpIUi;
      Locale.setDefault(Locale.ENGLISH);
      if (bool1) {
        try {
```

Java class with the parameters to collect

When deployed against a victim, Sorillus establishes the connection with its command and control (C2). In this case, the IP address was 78[.]142[.]18[.]37. The purpose of this C2 connection is to give the threat actor full control of the victim's operating system.

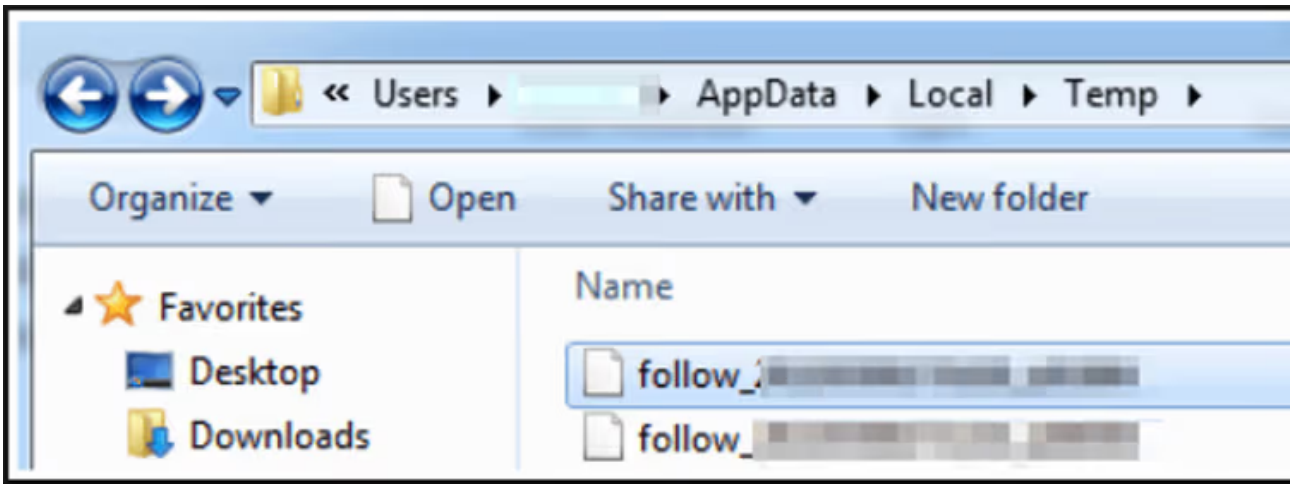
According to VirusTotal, the C2 IP address is associated with HostSlick, a web hosting company based in Germany, and has previously been linked to five other malicious samples similar to the Sorillus RAT we analyzed. Currently, the domain justinblairinc[.]com, which may be impersonating a US-based manufacturer and distributor of shoe store supplies, is also hosted on this IP address.



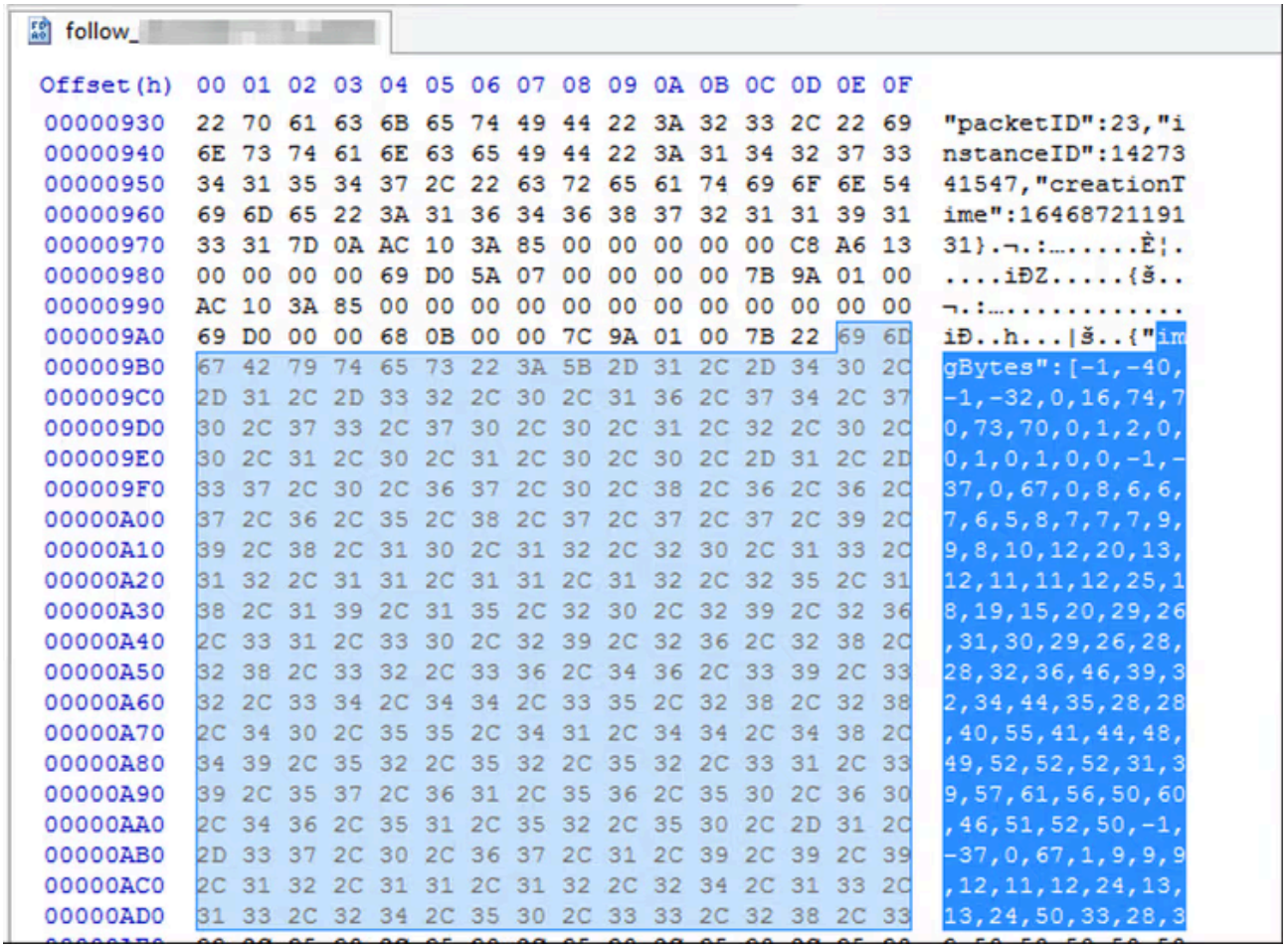
Sorillus RAT connection to C2 IP address

Example of network traffic

Once the malware has successfully connected to the C2, remote access is established and the threat actor is able to start stealing information. Stolen information is encrypted and stored in the victim's Temp directory until it is extracted by the attacker.

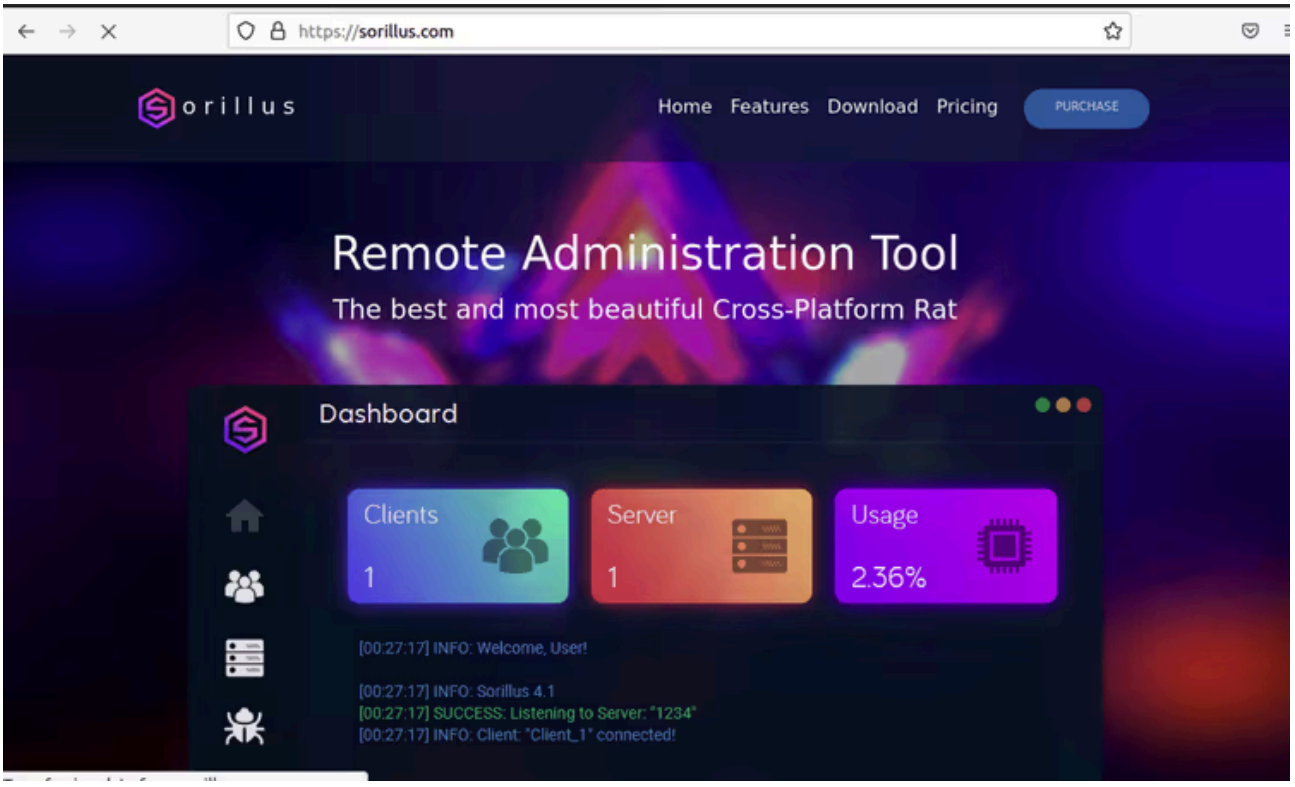


Stolen information stored in the Temp directory



Example of encrypted stolen information

What Is the Sorillus RAT?

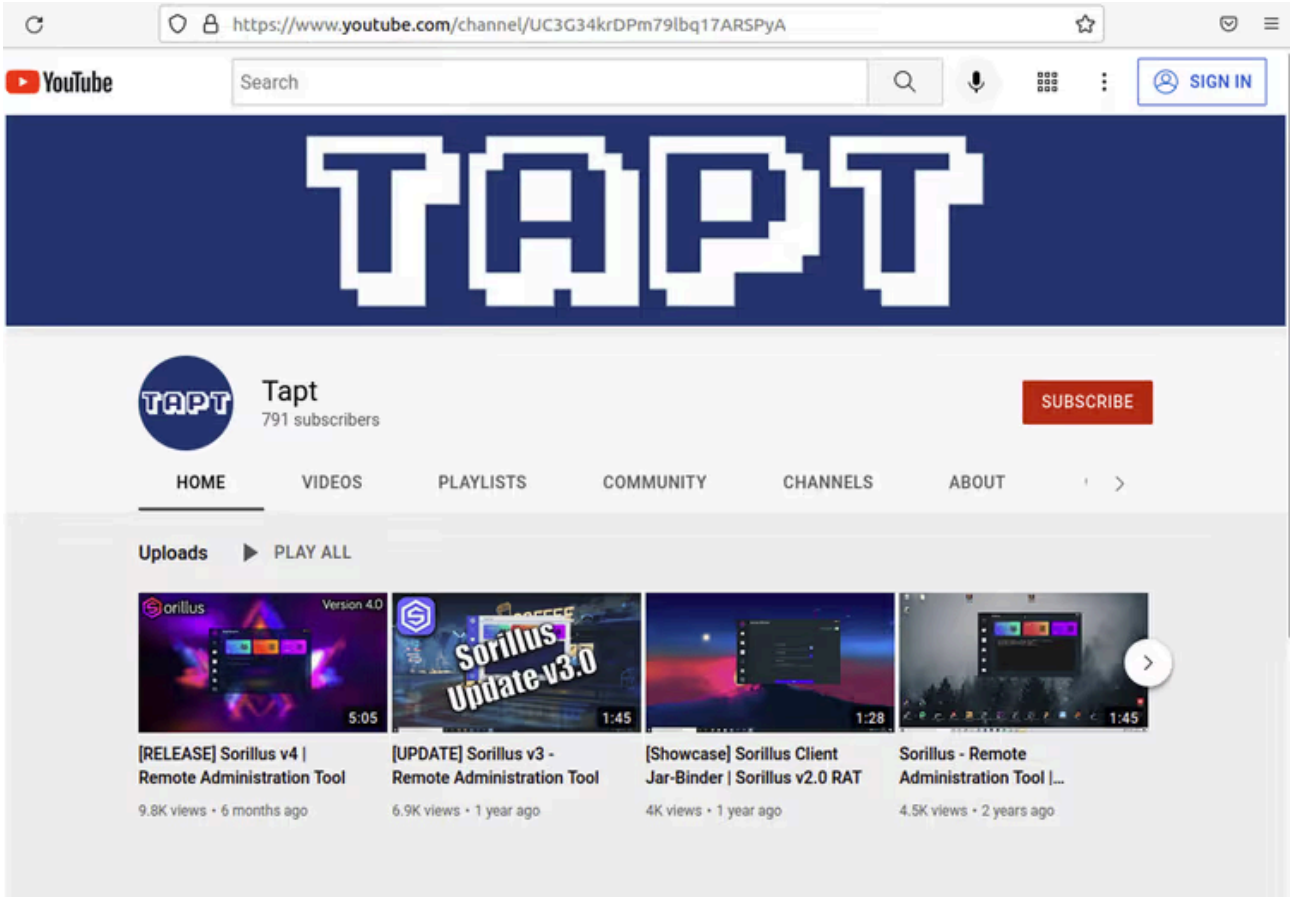


Sorillus is a paid remote access tool (RAT) that offers obfuscation and encryption capabilities. While it was first created in 2019, interest in the tool has increased considerably in the last six months since the previous update.

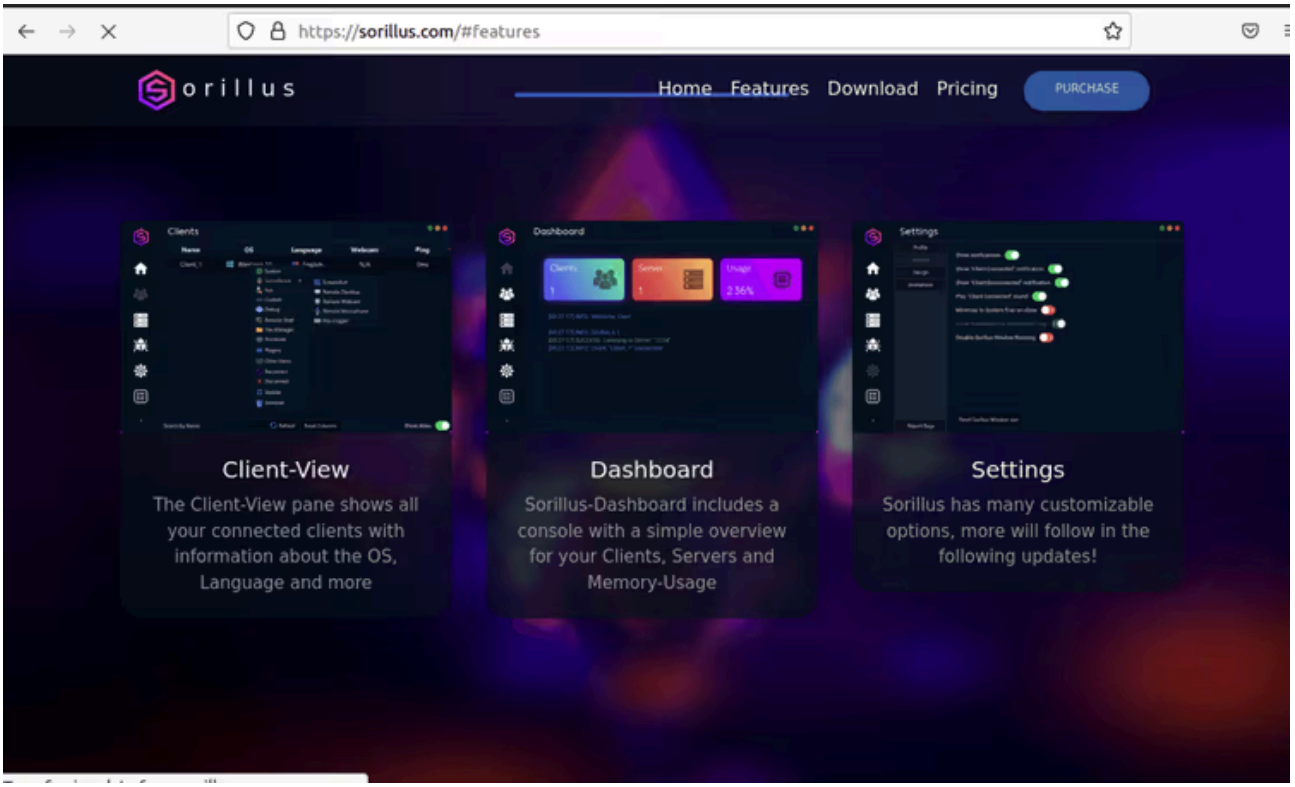
Beginning on January 18, 2022, different obfuscated client versions of the tool started to be uploaded to VirusTotal. Sorillus' features are described in detail on its website. The tool's creator and distributor, a YouTube user known as "Tapt", asserts that the tool is able to collect the following information from its target:

- HardwareID
- Username
- Country
- Language
- Webcam
- Headless
- Operating system
- Client Version

Active on YouTube since April 2015, all of Tapt's recent posts are exclusively videos describing Sorillus RAT and its functions. Overall, their channel has received almost 75K views, and the timing of their videos is consistent with updates made to the tool.

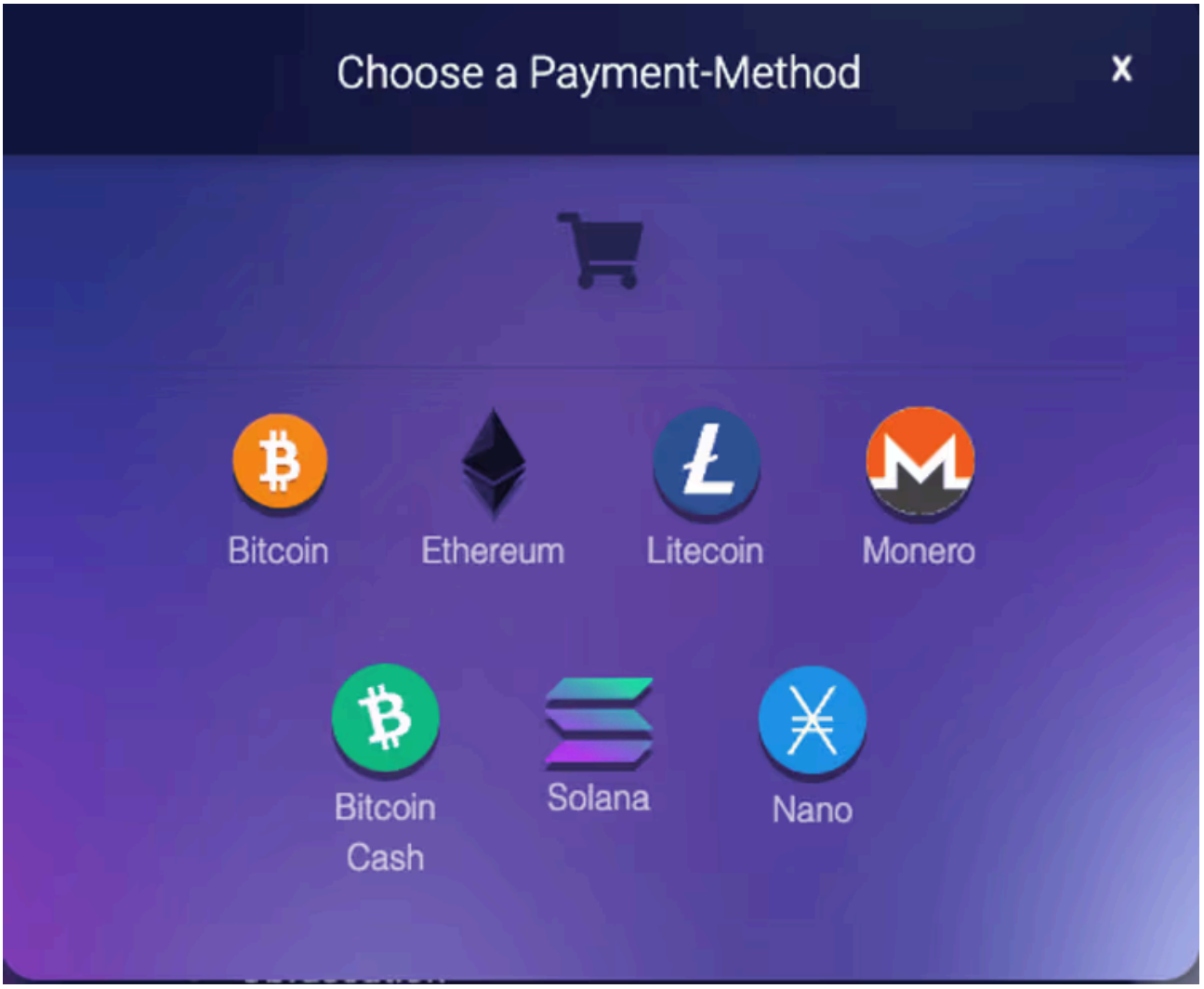


The recently-identified malicious activities associated with this RAT are related mainly to information stealing. However, due to Sorillus' ability to bundle its client code with any other java code, the range of malicious actions the tool can take is broad.



Screenshot showing three different Sorillus tool interfaces

The tool supposedly costs 49.99€ for lifetime access but is currently available at a discounted 19.99€. Conveniently, the Sorillus can be purchased via a variety of cryptocurrencies.



Payment methods for Sorillus

Protecting Yourself From the Sorillus RAT

For accounting and tax professionals, digital file sharing is a necessity. If you primarily receive documents via email (as opposed to having clients upload them to a secure portal), you must take precautions to reduce your risk of downloading malicious files.

One simple step is to avoid opening any attachments or links in emails sent from new or prospective clients until you (or a member of your staff) have spoken with the client directly.

Indicators of Compromise (IOCs)

1c7e5f54c879637967ec6937dee9f18afe33a7be71449d4ecdca8c8903e2a97b	jar
70a8cdbf0aacd885ec30d3c7632cf7fd4f4fe5814504c0dc7da92feb9ee37861	zip
78[.]142[.]18[.]37	C2
ilililililiiliililili	string
davidans1[@]delveroiin[.]com	email
rayjames1101[@]gmail[.]com	email
dexatri[.]com	domain
begrino[.]com	domain
delveroiin[.]com	domain

Source: https://abnormalsecurity.com/blog/tax-customers-sorillus-rat