Operation ElectroRAT: Attacker Creates Fake Companies to Drain Your Crypto Wallets

intezer.com/blog/research/operation-electrorat-attacker-creates-fake-companies-to-drain-your-crypto-wallets/

January 5, 2021

Get Free Account

Join Now

Already with thousands of victims.

Intro

With Bitcoin on the rise and a market exceeding billions of dollars, cryptocurrency has attracted threat actors wishing to leverage these capitals for their own financial gain.

In December, we discovered a wide-ranging operation targeting cryptocurrency users, estimated to have initiated in January 2020. This extensive operation is composed of a full-fledged marketing campaign, custom cryptocurrency-related applications and a new Remote Access Tool (RAT) written from scratch.

The campaign includes: Domain registrations, websites, trojanized applications, fake social media accounts and a new undetected remote access trojan that we have named **ElectroRAT**. ElectroRAT is written in Golang and compiled to target multiple operating systems: Windows, Linux and MacOS.

It is rather common to see various information stealers trying to collect private keys to access victims' wallets. However, it is rare to see tools written from scratch and used to target multiple operating systems for these purposes.

The attacker behind this operation has lured cryptocurrency users to download trojanized applications by promoting them in dedicated online forums and on social media. We estimate this campaign has already infected thousands of victims—based on the number of unique visitors to the pastebin pages used to locate the command and control servers.

The Operation

The attacker has created three different trojanized applications, each with a Windows, Linux and Mac version. The binaries are hosted on websites built specifically for this campaign.

These applications are directly related to cryptocurrency. "*Jamm*" and "*eTrade*" are cryptocurrency trade management applications and "*DaoPoker*" is a cryptocurrency poker app. Figures 1 and 2 are the homepages of the "*Jamm*" and "*eTrade*" websites. Figure 3 shows what the "*eTrade"* application looks like once it runs on an Ubuntu desktop.

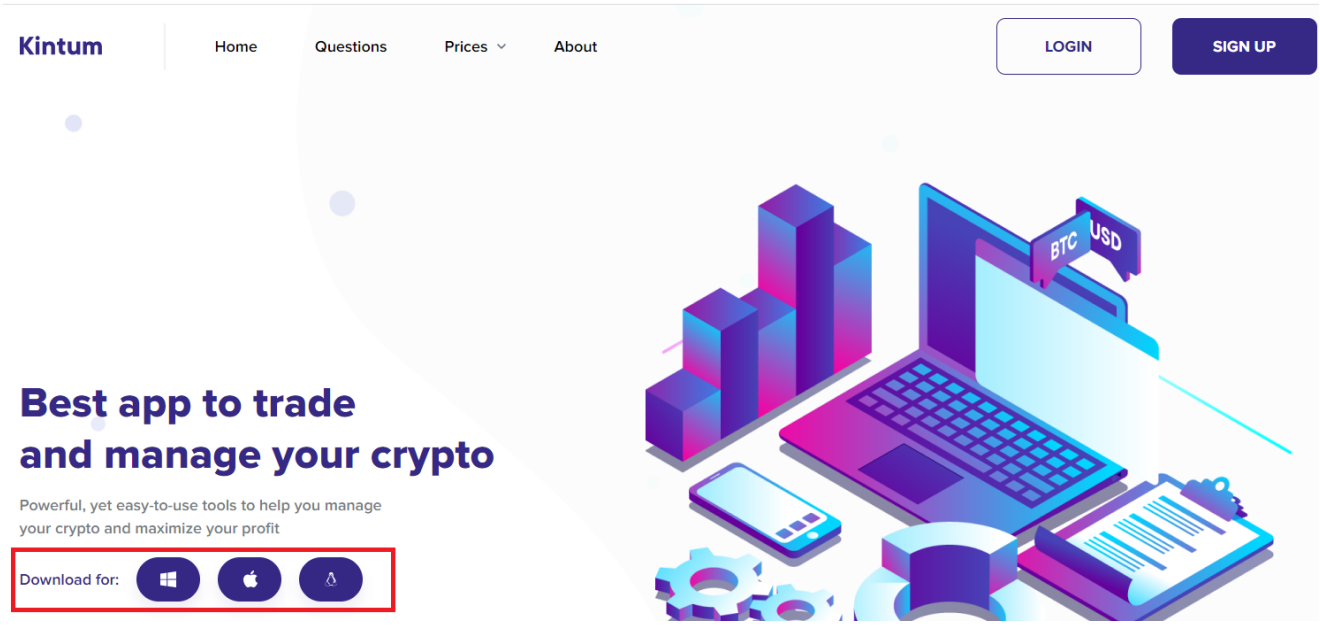


Figure 1: "Kintum" homepage which hosts eTrade's Windows, Linux and MacOS trojans

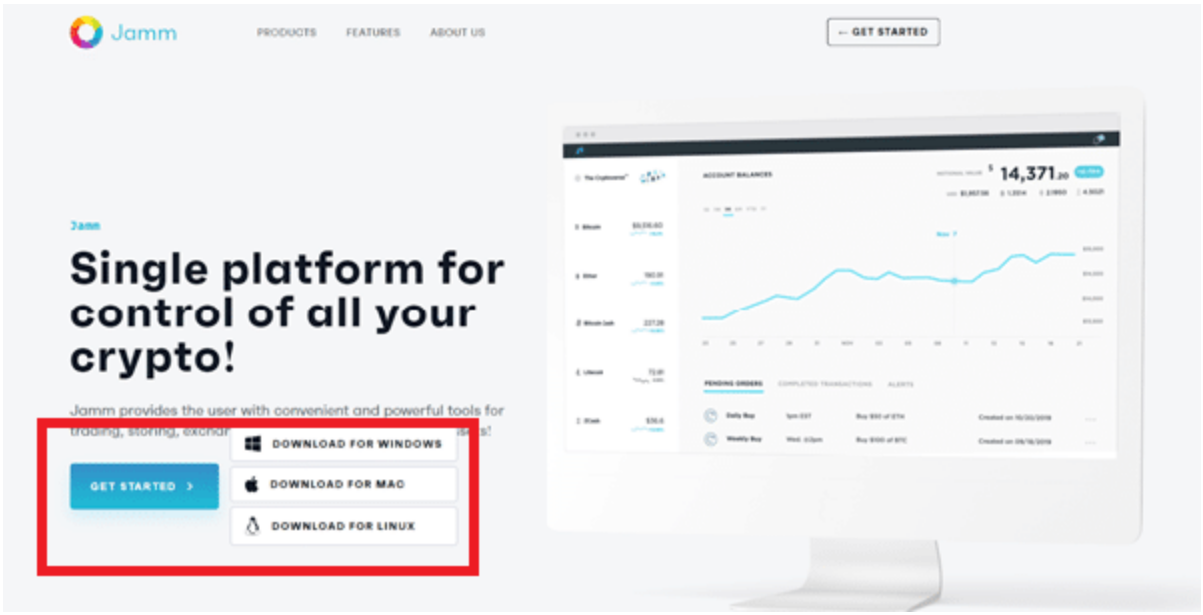


Figure 2: "Jamm" homepage which hosts Jamm's Windows, Linux and MacOS trojans

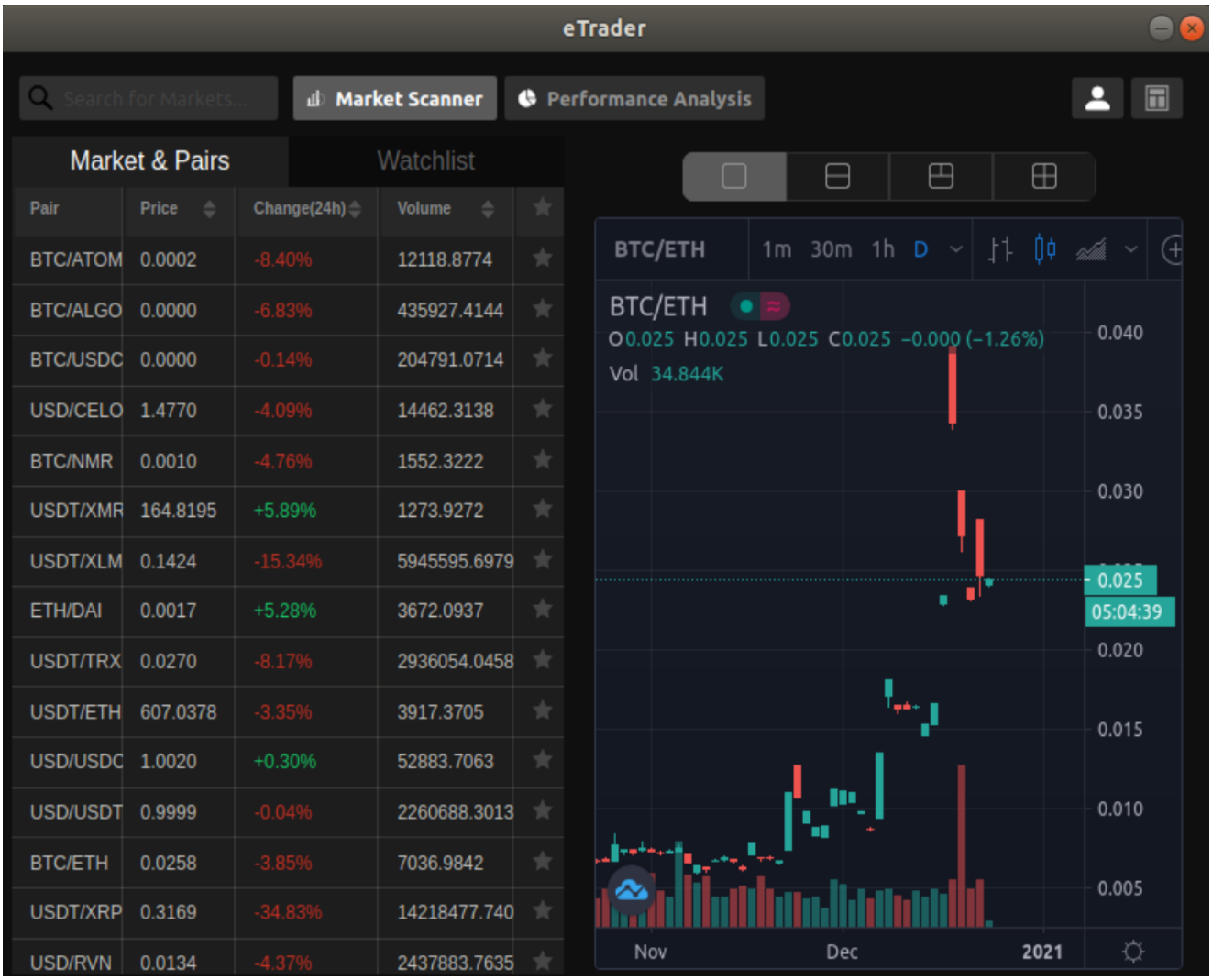
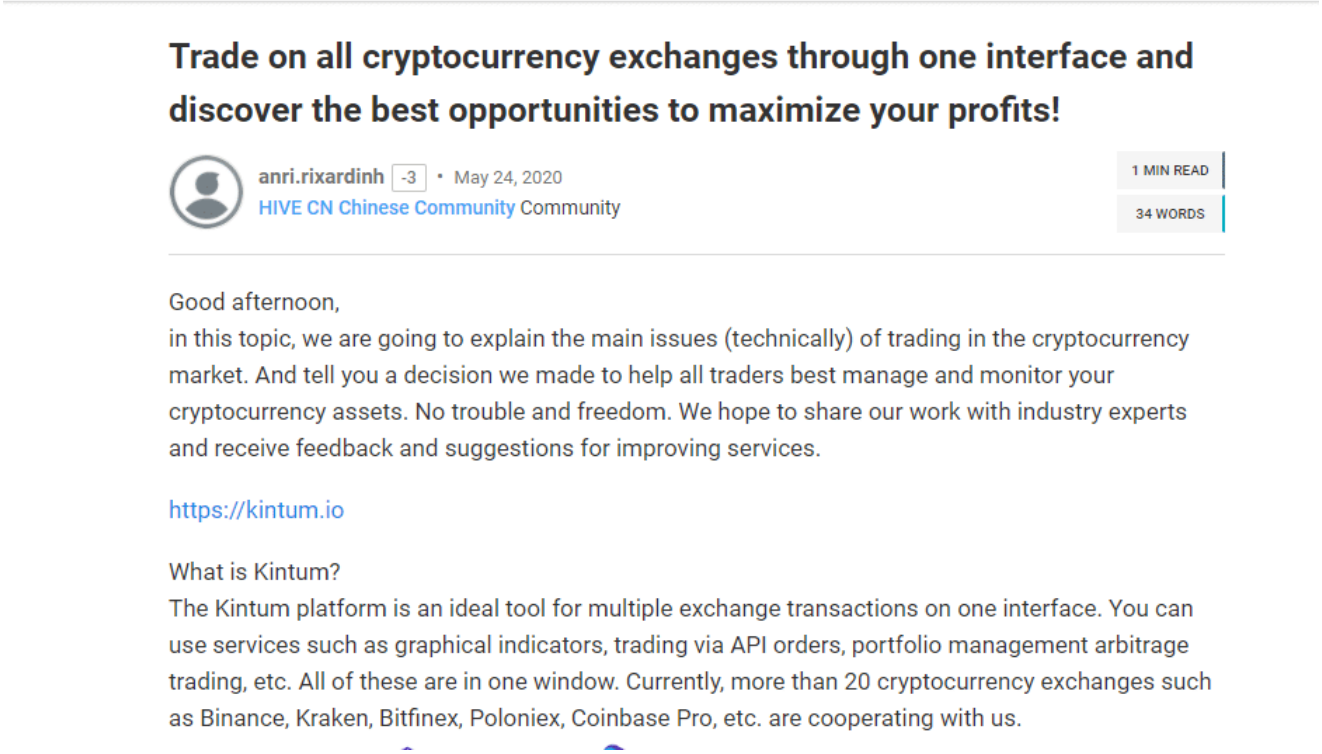


Figure 3: eTrade (Kintum) application on Ubuntu desktop

These applications were promoted in cryptocurrency and blockchain-related forums such as bitcointalk and SteemCoinPan. The promotional posts, published by fake users, tempted readers to browse the applications' web pages, where they could download the application without knowing they were actually installing malware.Figures 4 and 5 are examples of the promotions posted in these forums.



Trade on all cryptocurrency exchanges through one interface and discover the best opportunities to maximize your profits!

anri.rixardinh -3 • May 24, 2020
HIVE CN Chinese Community Community

1 MIN READ
34 WORDS

Good afternoon,
in this topic, we are going to explain the main issues (technically) of trading in the cryptocurrency market. And tell you a decision we made to help all traders best manage and monitor your cryptocurrency assets. No trouble and freedom. We hope to share our work with industry experts and receive feedback and suggestions for improving services.

https://kintum.io

What is Kintum?
The Kintum platform is an ideal tool for multiple exchange transactions on one interface. You can use services such as graphical indicators, trading via API orders, portfolio management arbitrage trading, etc. All of these are in one window. Currently, more than 20 cryptocurrency exchanges such as Binance, Kraken, Bitfinex, Poloniex, Coinbase Pro, etc. are cooperating with us.

Figure 4: The user "anri.rixardinh" posting in a Chinese Hive forum in PeakD promoting "eTrade" application

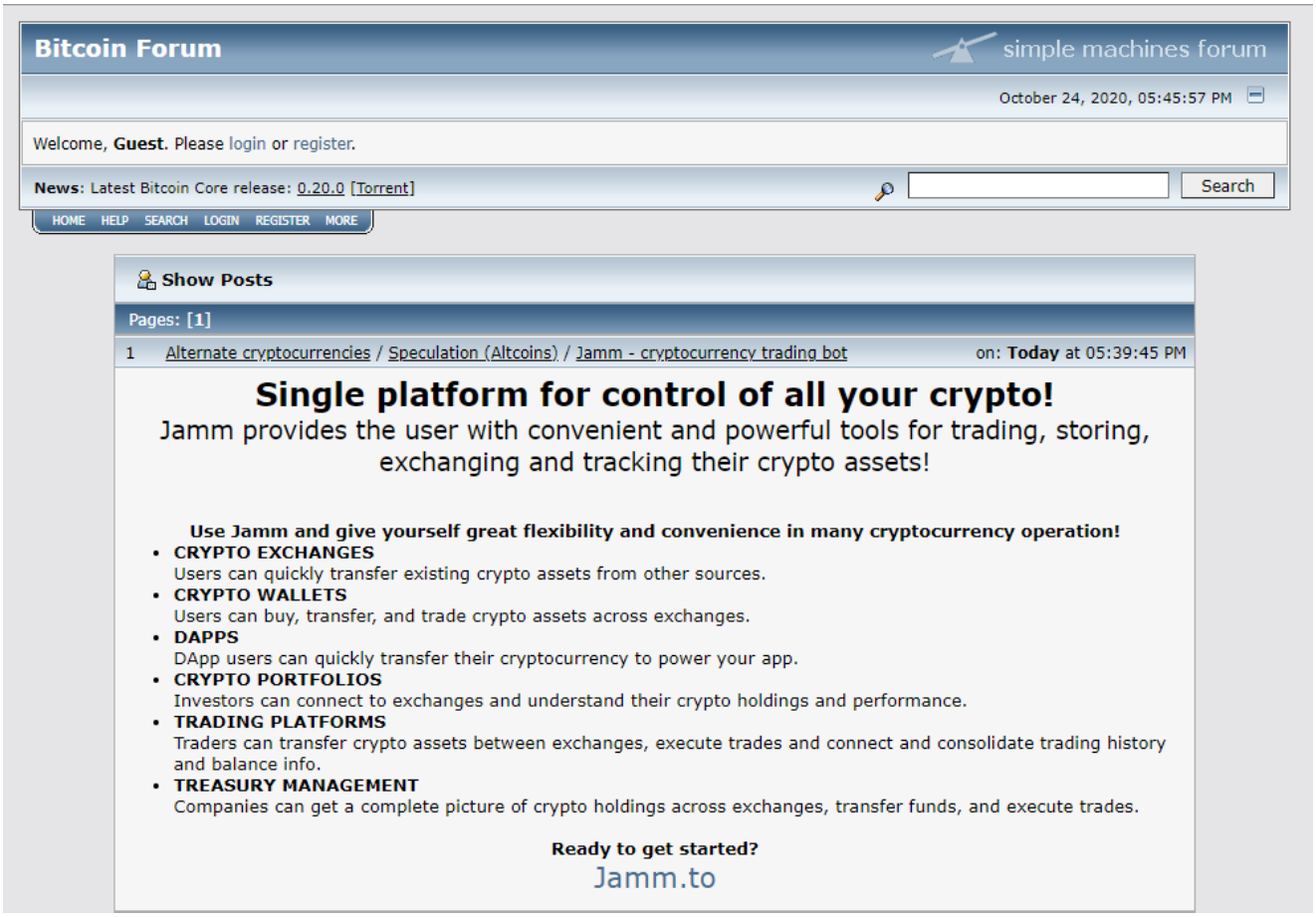


Figure 5: "Jamm" application promoted in bitcointalk forum

The attacker went the extra mile to create Twitter and Telegram personas for the "*DaoPoker*" application, in addition to paying a social media influencer for advertisement. Figure 6 shows the *DaoPoker* Twitter page. Figure 7 shows *eTrade* promoted by a social media advertiser with over 25K followers on Twitter.

Figure 6: DaoPoker's Twitter page

Victims of the Operation

As part of its behavioral flow, ElectroRAT contacts raw pastebin pages to retrieve the C&C IP address. The pastebin pages are published by the same user called "Execmac". Browsing the user's page, we have more visibility into the number of victims subject to this campaign. In Figure 8, we can see that the amount of unique visitors to the user's pastes is approximately 6.5K [at the time of this writing]. We can also see the first pastebin pages were posted on January 8 2020, which indicates the operation has been active for at least a year.

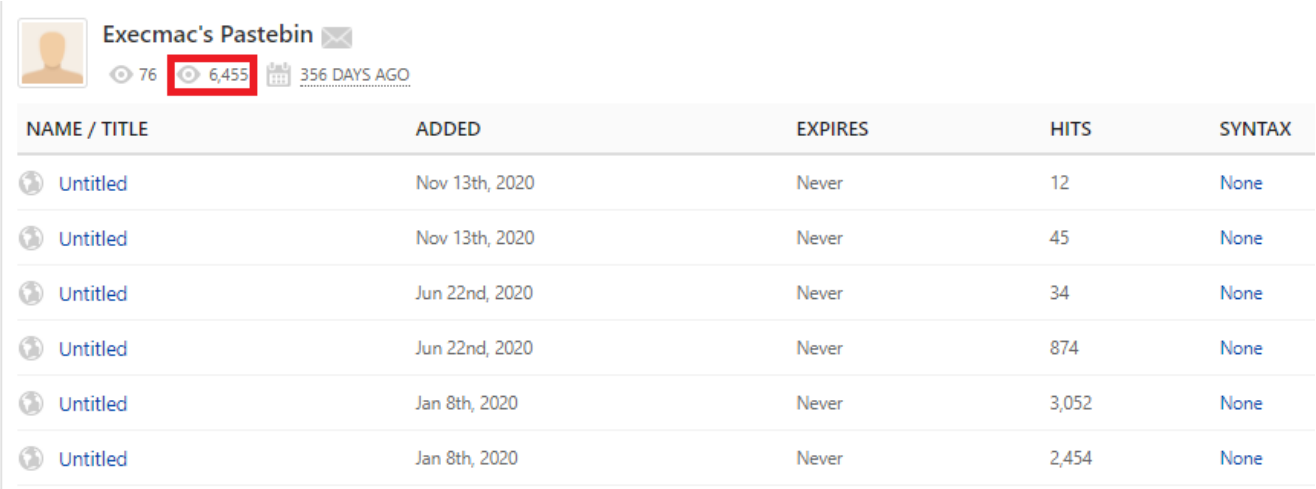


Figure 8: https[:]//pastebin[.]com/u/execmac pastebin page

We also saw evidence of victims who were compromised by these applications commenting on posts related to MetaMask. See Figures 9 and 10.

Figure 9: A user commenting on a MetaMask Tweet

Figure 10: A user alerting on DaoPoker

Opening a Can of Stealers

The above-mentioned pastebin page reveals more insights. Other pastes published by the same user contain C&Cs directly tied to Amadey and KPOT. These malware are stealers mainly purchased on the Dark Web as off-the-shelf malware. ElectroRAT shares similar

functionalities to these well-known trojans, however, it's written from scratch in Golang. We assume a reason for this is to target multiple operating systems, since Golang is incredibly efficient for multi-platform use. Writing the malware from scratch has also allowed the campaign to fly under the radar for almost a year by evading all Antivirus detections.

Technical Analysis

Jamm, DaoPoker and eTrade were built using Electron, an app building platform. ElectroRAT is embedded inside each application. Once a victim runs the application, an innocent GUI will open, while ElectroRat runs hidden in the background as "mdworker". Figure 3 above shows eTrade app GUI upon runtime on an infected Ubuntu desktop machine. Figure 11 shows what the infection looks like behind the scenes using Intezer's Cloud Workload Protection Platform, Intezer Protect.

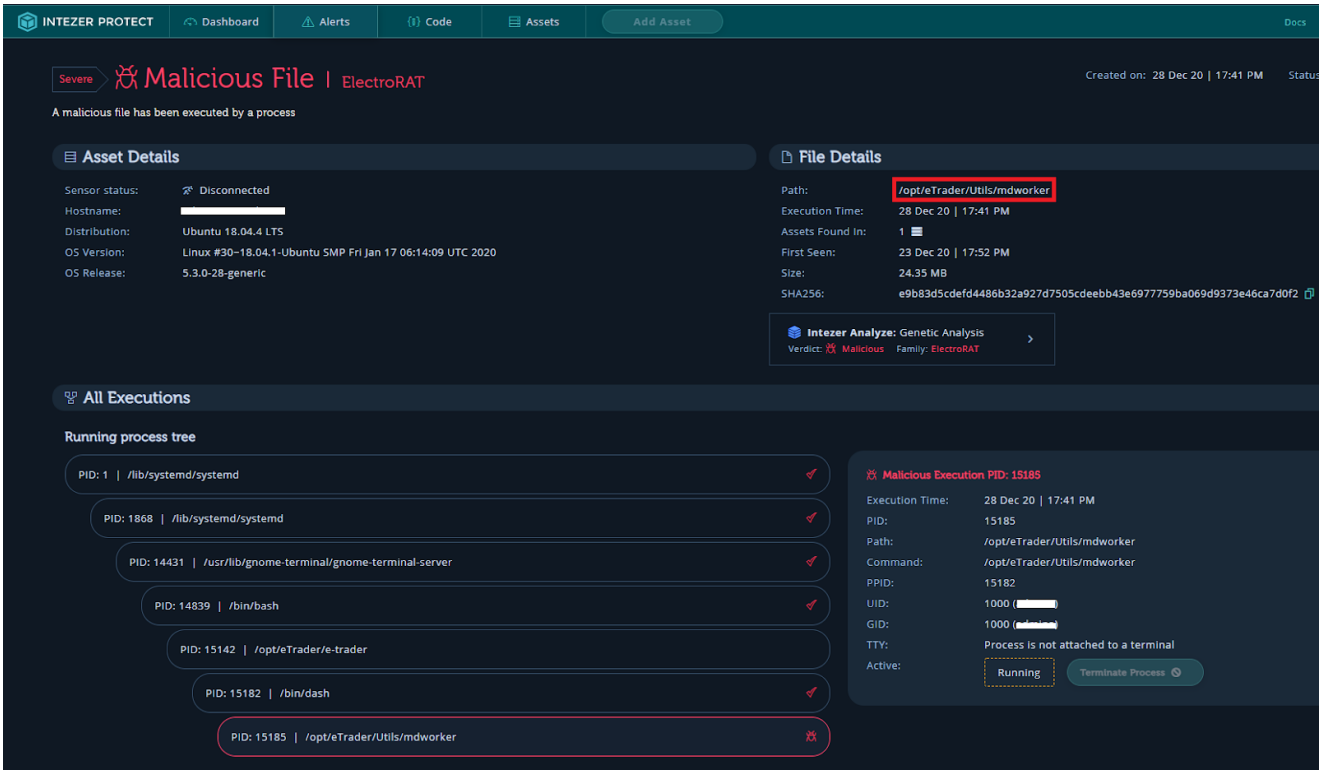


Figure 11: ElectroRAT alert in Intezer Protect

The trojanized application and the ElectroRAT binaries are either low detected or completely undetected in VirusTotal at the time of this writing. Figure 12 shows the signed DaoPoker application's detection rate in VirusTotal.

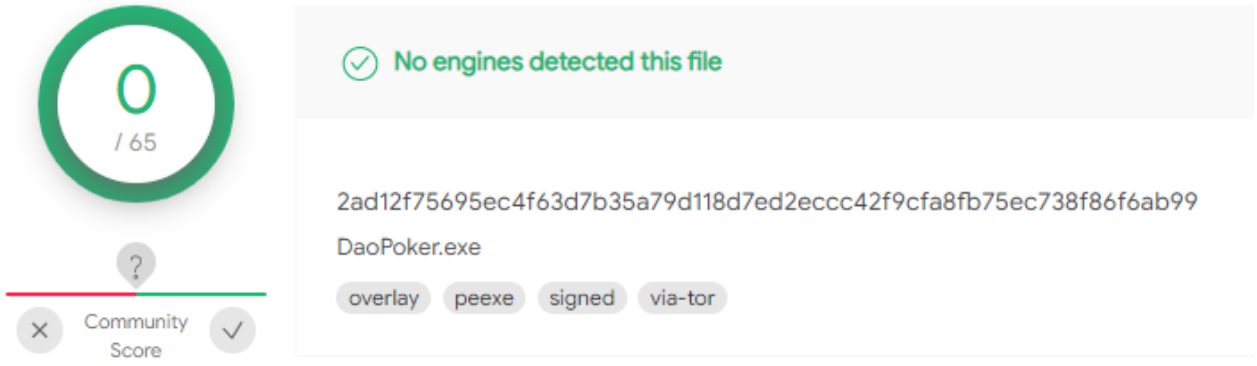


Figure 12: DaoPoker application in VirusTotal (2c35bfabc6f441a90c8cc584e834eb59)

ElectroRAT is extremely intrusive. It has various capabilities such as keylogging, taking screenshots, uploading files from disk, downloading files and executing commands on the victim's console. The malware has similar capabilities for its Windows, Linux and MacOS variants.

For more technical information, browse the following Tweet:

> [1/7] Operation #ElectroRAT is a new campaign that takes sizable measures to steal crypto wallets. For more information about the operation – https://t.co/CWLnOevKir
>
> The following is a technical analysis->@IntezerLabs
>
> — Avigayil Mechtinger (@AbbyMCH) January 5, 2021

Detection & Response

Detect if a Machine in Your Network Has Been Compromised

You can quickly detect if your machine, or a machine in your network, has been compromised by malware using Intezer Protect and Intezer Analyze Endpoint Scanner:

Linux Machines

Linux threats are on the rise. Use Intezer Protect to gain full runtime visibility over the code in your Linux-based systems and get alerted on any malicious or unauthorized code. We have a free community edition.

Figure 10 above emphasizes an Intezer Protect alert on a compromised machine. The alert provides you with full context about the malicious code including threat classification, binary's path on the disk, process tree, command and hash.

Windows Machines

Running Intezer's Endpoint Scanner will provide you with visibility into the type and origin of all binary code that resides in your machine's memory. Figure 13 shows an example of an endpoint infected with ElectroRAT.

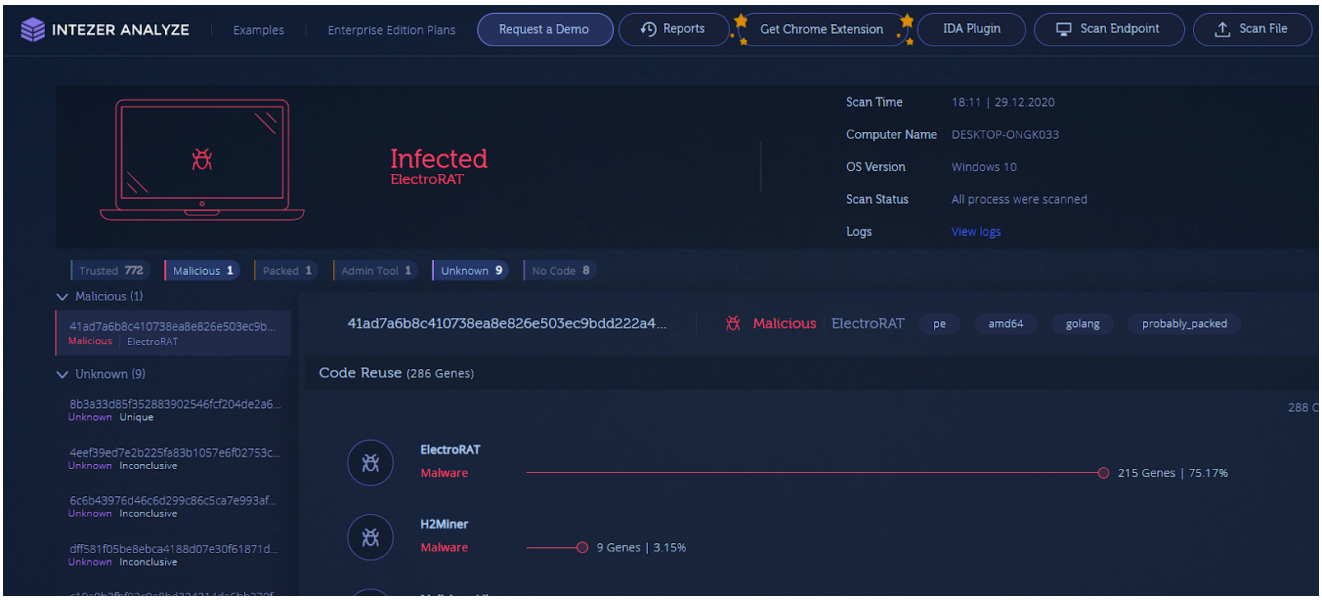


Figure 13: Endpoint infected with ElectroRAT

Response

If you were, or suspect that you are a victim of this scam, take the following steps:

1. Kill the process and delete all files related to the malware.
2. Make sure your machine is clean and running 100% trusted code using Intezer's tools mentioned above.
3. Move your funds to a new wallet.
4. Change all of your passwords.

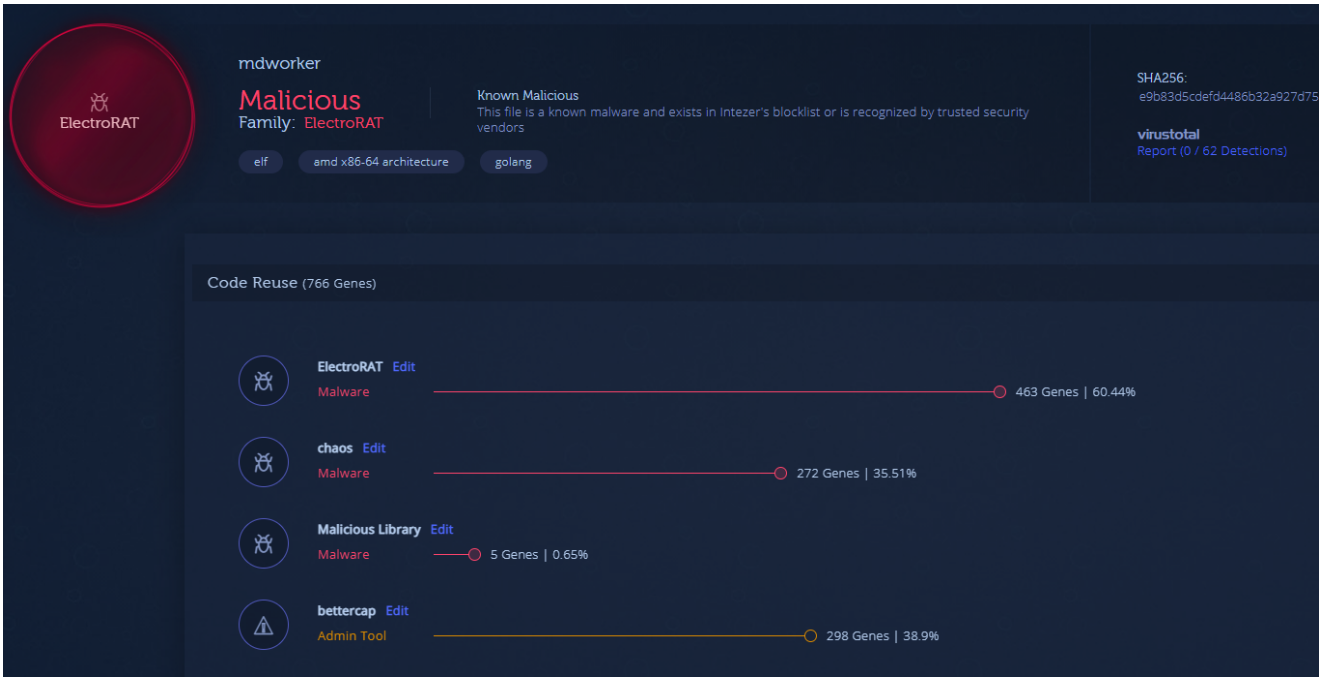
You can also run this YARA rule against in-memory artifacts to detect ElectroRAT.

Wrap-Up

It is very uncommon to see a RAT written from scratch and used to steal personal information from cryptocurrency users. It is even more rare to see such a wide-ranging and targeted campaign that includes various components such as fake apps/websites and marketing/promotional efforts via relevant forums and social media.

ElectroRAT is the latest example of attackers using Golang to develop multi-platform malware. We touched upon this trend in the Top Linux Cloud Threats of 2020.

ElectroRAT's PE and ELF versions are indexed in Intezer Analyze so that you can quickly classify any samples that are genetically similar.



IoCs

C&C

193[.]38[.]55[.]131
193[.]38[.]55[.]4
213[.]226[.]100[.]140
kintum[.]io
daopoker[.]com
jamm[.]to
pastebin.com/raw/r12wBrC7
pastebin.com/raw/DF8Gikrk
pastebin.com/raw/bfQiiqyv
pastebin.com/raw/UbTZx6kd
pastebin.com/raw/U45SvK4K
pastebin.com/raw/zrZA4L3e

ElectroRAT

Windows

170cb5ea1a6b4af3c27358ba267a1309ed5118481619fc874f717262cb91fb77
881be95a9632fa44deeeca23e4e19390d600ad817b2f66671d3f21453a16c7b7
41ad7a6b8c410738ea8e826e503ec9bdd222a490db097b643cd94bbd62a12276
a4a68a51ed0a6ecf9146f75d405e50cfc58473d20220915b489b5fece03c4f55
ddd15dcc89416a61001c10ed9002df854fb4d92089e5388264b8af02654c778e
568326883f9157fe8f1a7c681e2df341973a75205cf81d627040d101ce24f1bb
2ad12f75695ec4f63d7b35a79d118d7ed2eccc42f9cfa8fb75ec738f86f6ab99
13ac090fa99b1dce7f45e4aed07a0359b73815fc38dbe02bf976e088060990a8
da7c4975d75ffe17d6ff1352e239c6841d4b1523f9ea43c8124d732c48dfabba
1416f8c40663d51191e8bd03c885e1f4f1c6b7c63d3068721bf386d621783917
c1aaf691608f1f2a0517e2c57cc4c6ff4e46d3ae1b592e939a0bc9b89a3a04cf
cf77727aa2cfcd3d6dd85cb492ddee28ff9191def60a9e00ea08ccddf817d143
a32ef780ba235f8222c05302f7537b4123c41b048449c6ec8744d64103d428a3

Linux

e9b83d5cdefd4486b32a927d7505cdeebb43e6977759ba069d9373e46ca7d0f2
e547872761d81c3afc9c2a42cac3931e2a1defc2c56a0a3c57b28ea91e7686cd

MacOS

17b0b1a9271683f30e5bfd92eec9c0a917755f54060ef40d9bd0f12e927f540f
5c884be3635eb55ce02e141d6fb07f760b6dbcace54f2217c69f287292ce59f6

KPOT Stealer

f33c78cddcf99dd999b065644a17dcbac1b222a7f3342b3fe3293ddb6ecf0060
2f83e130e52cb13944899e81f4ecf49decf52e3949f6d41b45e8b1a19a658ed6
587a4463673093554cd75b5c9ccb6c254a9d6e8769b1e45ea0390eb2b9d57bff
adeba13b358ea8be691fd7f4d025a6ea27b9b120d97d312ea875d6067434d77e
dd1792bcdf560ebaa633f72de4037e78fe1ada5c8694b9d4879554aedc323ac9

Amadey

279524f17f8dd8753f57c2e3e91d21ad84db10316dfbf925cc19556cef55b99d
18fd6b193be1d5416a3188f5d9e4047cca719fa067d7d0169cf2df5c7fed54c0
5545f31c832c8bde6cf7563cdc0f4a4b9b15416480e14f15420b1691444c376d

Avigayil Mechtinger

Avigayil is a product manager at Intezer, leading Intezer Analyze product lifecycle. Prior to this role, Avigayil was part of Intezer's research team and specialized in malware analysis and threat hunting. During her time at Intezer, she has uncovered and documented different malware targeting both Linux and Windows platforms.