Conduct a Search of Recent Malware

a. Using your favorite search engine, conduct a search for recent malware. During your search, choose four

examples of malware, each one from a different malware type, and be prepared to discuss details on

what each does, how it each is transmitted and the impact each cause.

Examples of malware types include: Ransomware, Trojan, Hoax, Adware, Malware, PUP, Exploit, Exploit

Kit and Vulnerability. Search for malware by visiting the following websites using the following search

terms:

• McAfee Threat Center Threat Landscape Dashboard

• Malwarebytes Labs Threat Center (Top 10 Malware)

• Securityweek.com > virus-threats > virus-malware

• Technewsworld.com > security > malware

b. Read the information about the malware found from your search in the previous step, choose one and

write a short summary that explains what the malware does, how it is transmitted, and the impact it

causes.

Trojan.BitCoinMiner

### **About trojans**

A trojan is usually deliberately designed by its author to appear authentic and attractive. For example, it may appear to be a screensaver, a service pack, an application update and so on. Once installed or opened, the trojan may perform its promised function, or display a decoy document to distract the user. In the background however, it also silently performs unauthorized actions (its *payload*), without the user's knowledge or consent.

Programs identified as Trojan.BitCoinMiners can either function as a miner, or install a separate component that can do so. Malware that use miners as part of their payload are essentially hijacking a user's resources to create cryptocurrency units for the malware author's benefit.

A trojan is usually deliberately designed by its author to appear authentic and attractive. For example, it may appear to be a screensaver, a service pack, an application update and so on.

### **Installation**

Trojans rely on tricking the user into believing that the program is authentic, so that they unwittingly install the program themselves. To do this, most trojans mimic or entirely copy the style and branding of popular legitimate programs or files. Some trojans (particularly on the Android platform) are actually copies of legitimate apps that have been repackaged or **trojanized** to include harmful components.

Trojans are often distributed using the same (or very similar) names and designs as popular programs, to increase the chances that users will mistake the trojan for the legitimate app and install it instead.

Once installed or opened, the trojan may perform its promised function, or display a decoy document to distract the user. In the background however, it also silently performs unauthorized actions (its **payload**), without the user's knowledge or consent.

### **Impact**

Depending on its creator's intent, a trojan's payload can range from:

* Mildly annoying pranks, like changing desktop icon positions, to
* Serious, user-inhibiting actions, like disabling the keyboard or mouse, to
* Critically destructive actions, like erasing files or stealing data

It is often very difficult for users to realize that a trojan is performing harmful actions, as they are usually well camouflaged to keep the system from triggering any notification messages that might arouse the user's suspicions.

### **Types of trojans**

Trojans are often classified into [sub-types](https://www.f-secure.com/v-descs/guides/classification_guide.shtml) based on the actions they perform. These are just a few of the possible types:

* Trojan-downloader Contacts a remote server and downloads other harmful programs from it
* Trojan-dropper Contains one or more harmful components that it drops and installs
* Trojan spy: Monitors activity on the device, or steals content from it
* Password-steeler: Steals passwords and other confidential details from the device

### **About cryptocurrency mining programs**

A **cryptocurrency** is an anonymous, decentralized form of digital currency, which can be used online as a medium of exchange much like traditional, physical currencies. Multiple cryptocurrencies exist, such as BitCoin, Ethereum and Monero.

Cryptocurrency units can be created by any user with specialized mining programs or miners that run the necessary mathematical calculations. Examples of mining programs include Coinhive, Cryptoloot, Electrum, Hashflare and MinerGate, though there are dozens of other similar programs available online.

The 'crypto' part of the term refers to the use of cryptography both for creating the currency units and for securing transactions made with the units. Because of the anonymity provided by cryptocurrency, its legality and acceptance varies considerably between countries.