Centers of Academic Excellence Forum

Use of Botnets for Mining Cryptocurrencies

December 2020

Renita Murimi

Associate Professor of Cybersecurity

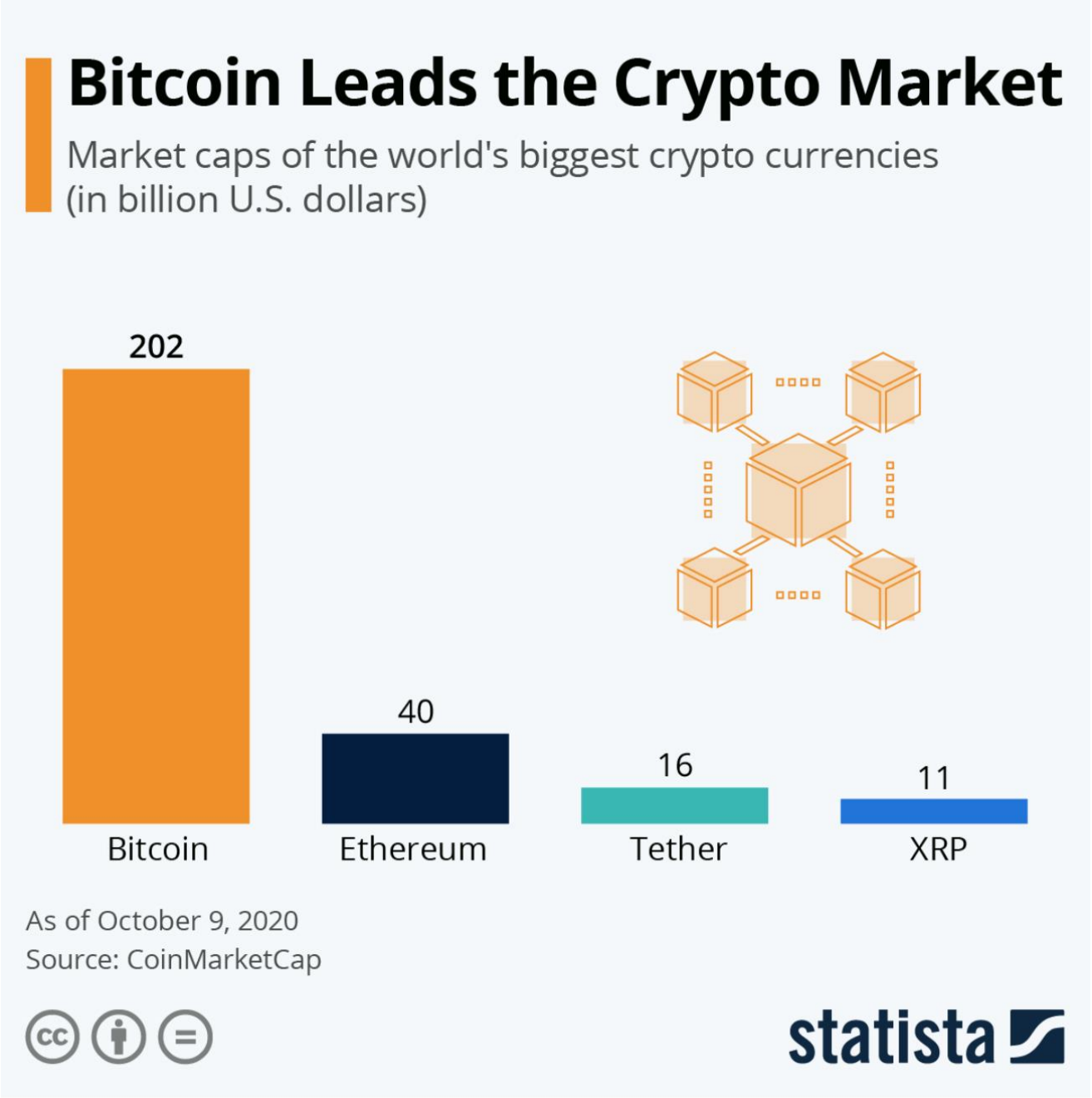
University of Dallas

UNIVERSITY OF DALLAS

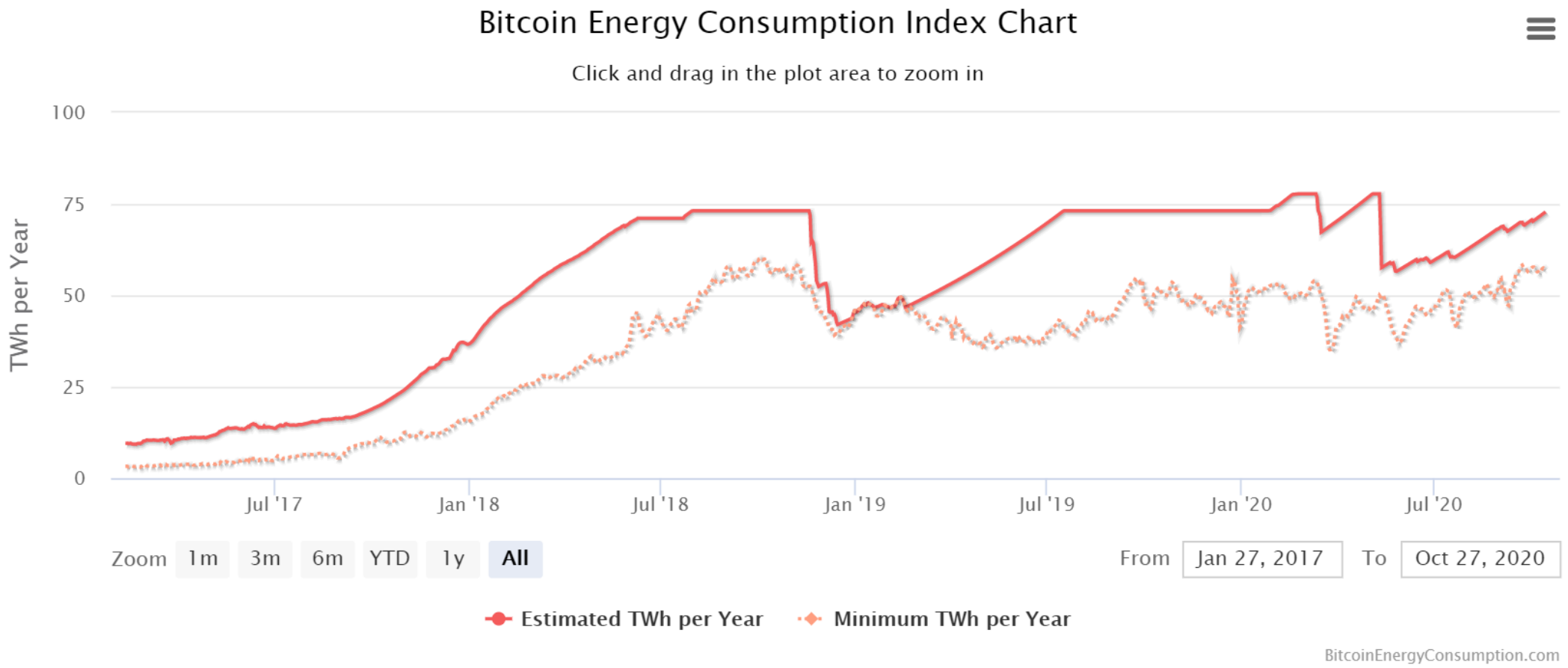
In this talk…

- History of botnet-inspired threats
- Operational mechanisms of botnets
- In-depth look at significant botnets that have attacked cryptocurrencies
- Countermeasures
- Implications for the future

Market capitalization



Energy Consumption Index Comparison



Footprints

Annualized Total Footprints

Carbon Footprint

34.60 Mt CO2

Comparable to the carbon footprint of **Denmark**.

Electrical Energy

72.83 TWh

Comparable to the power consumption of **Austria**.

Electronic Waste

12.15 kt

Comparable to the e-waste generation of **Luxembourg**.

Single Transaction Footprints

Carbon Footprint

300.30 kgCO2

Equivalent to the carbon footprint of **750,762** VISA transactions or **50,051** hours of watching Youtube.

Electrical Energy

632.22 kWh

Equivalent to the power consumption of an average U.S. household over **21.37** days.

Electronic Waste

105.40 grams

Equivalent to the weight of **1.62** 'C'-size batteries or **2.29** golf balls. (Find more info on e-waste here.)

Rising popularity

- Distributed nature of currency generation
- Anonymity
- Low barrier to entry
- Browser-based mining software

Botnet core

- Command and Control (C&C) architectures: backbone of botnet operations
- Aided by the IRC protocol
  - C&C server sends commands to malware-infected machines, which are then capable of launching DDoS attacks, data manipulation, and malware propagation.
- IRC protocol: text-based protocol that allows clients in various topology configurations to connect to a server over communication
- Can also use the HTTP protocol for C&C communication

Push and pull frameworks

- Two frameworks for C&C communications
- Push
  - Bots wait for commands from the C&C server, i.e., the server pushes the commands to bots in real time. IRC-based bots fall into the push category.
- Pull
  - Servers store commands in a file
  - Bots check back at later times to retrieve and execute the commands, i.e., the bots pull the commands from a file stored in the C&C server.
  - Most HTTP-based bots fall into this category of botnets that do not adhere to real-time botmaster control.

The appeal of botnets for cryptomining

- Distributed nature of both botnets and cryptocurrency mining
- Anonymity in cryptocurrency
  - Each node is identified only by its IP address
  - Contrast to fiat currencies
- Botnets – initially used for spam
  - In 2019 ransomware from phishing emails increased 109% over 2017.
  - Ransomware attacks increased 41% in 2019 with 205,000 businesses who lost access to their files.
  - Wannacry, CryptoLocker, SamSam, Petya

Source: Purplesec Cybersecurity Statistics

Types of botnet-based mining activity

- Direct mining:
  - Botmaster distributes the mining executable inside a wrapper script with specified parameters to be mined.
  - Made available as trojans inside external applications, which are deployed with the botmasters credentials.
  - A large number of bots in the botnet are mining and delivering the cryptocurrencies directly to the botmasters account.
- Proxied mining
  - Uses a proxy server deployed by the botmaster.
  - Hides the addresses of all the bots and appears as a single powerful miner.
- Dark pool mining
  - Botmaster maintains a mining pool that participates in the mining of bitcoins on the Bitcoin peer-peer network.

Consensus protocol

- Consensus protocol: Nodes on a network perform proof-of-work required to solve a cryptographic puzzle
- Assumption: every node can observe the proof-of-work done by peer nodes
- A possible attack
  - Eclipse attack: effectively isolates a node, blocking its view of the consensus protocol
  - Found to be more effective than infrastructure-based attacks

Mining environment

- Traditionally, used ASIC or GPU processors
- ArtForz
  - Around 2010
  - Among the first few developers to mine Bitcoin with private code
  - Network of 24 Radeon 5970s
  - Controlled a quarter of the mining power at the time
  - Purported to control 4% of bitcoins available
  - Used FPGAs and ASICs
- A new breed of less-intensive mining
  - In-browser files that execute mining code

Browser Evolution and Adaptability for Cryptomining

Browser evolution – HTML, CSS, JavaScript, HTML5

- HTML – Tim Berners Lee – 1993
  - Simple markup language, containing only 18 elements
- JavaScript – Brendan Eich – mid 1990s
- IETF and W3C standards
  - HTML version 5
  - Allows for cross-platform mobile applications
  - Supports web workers – scripts run in threads in the background without affecting webpage performance

Cross Origin Resource Sharing (CORS)

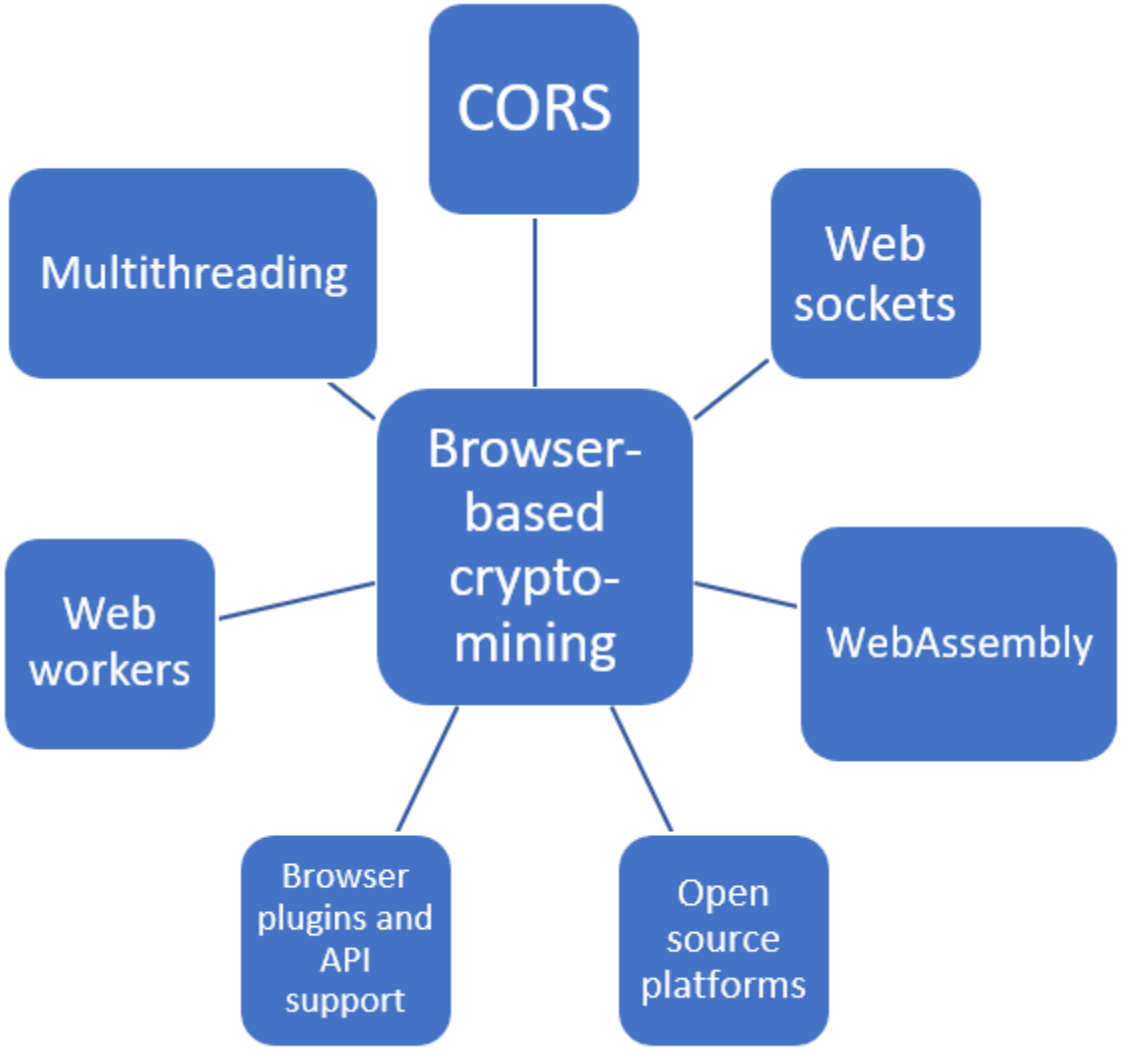
- Allows websites on different domains to share data and enables communication between servers and client browsers for data requests.
- Allows for mechanisms to override the same-origin policy, thus enabling web browser scripts from one page to offer access to data from another page even if they do not have the same origin.
- Same origin policy was also one of the limitations of JavaScript Web workers, however, CORS has offered an ingenious work-around to the problem of same-origin policy.
- CORS and Web Workers together allow for cross-domain workers through the creation of intermediate pseudo-JavaScript formats called blobs.

How does that help cryptomining?

- Ability to work in the background without affecting website performance
- Cross-domain data sharing
- Ability to work with APIs
- Stealthy tactics (pop-under)
  - Not easily detected
  - Potential to stay open indefinitely
  - Persist beyond clicks on the X icon
- Anti-detection techniques
  - Fileless – running native applications, not injected code
  - Ability to kill other cryptomining processes

Other factors that aid cryptomining

- Websockets
  - Support full-duplex connection between browser and server on TCP
- WebAssembly (WASM)
  - Modern web platform: virtual machine (VM) and the API collection
  - Traditionally, VM has only been able to load JavaScript
  - WASM can run application code from any language on the web browser in a compact binary format
  - Advantages
    - Speed of running native apps
    - Improved performance, portability and interoperability
    - Applications: browser-based password cracking, cryptomining


CORS
Multithreading
Web sockets
Browser-based crypto-mining
Web workers
WebAssembly
Browser plugins and API support
Open source platforms

Cryptojacking

Cryptojacking

- Aka drive-by mining, in-browser mining
- Executable files run, usually without the consent of the client machine and the corresponding payoff is delivered to the website.
- Generally JavaScript files or WASM modules that infect web servers and are enabled by third-party libraries, browser misconfigurations, or advertisements
- Computational resources of the user machine running the browser are leveraged when the user visits the website, and has the ability to render such client machines into bots for a botnet.

Coinhive – legitimate framework for browser-based mining

- One of the first platforms to offer browser-based cryptomining
- Provides developers with APIs and is geared toward optimized performance by browser-based mining.
- Enables the creation of unique IDs called “site keys” in Coinhive.
- These site keys map to miners and are therefore used to link rewards for the mining operation.
- Multiple site keys can map to the same wallet
- Mines Monero with CryptoNight and CryptoNote algorithms
  - CryptoNight: compatible with CPU computational resources
  - CrytpoNote: Offers anonymity

Issues with cryptojacking

- Abuse of user consent
- Compromise of user machines by transforming them into bots
- Profit models of complicit websites hosting the JavaScript executables that run mining scripts
- Breach of the existing browser, network, and cloud configurations
- Botnet-powered payload and loot.

Coinhive

- AuthedMine: user consent for in-browser mining
  - Asks for user consent prior to using the computational hashing power of the user's machine.
- Coinhive receives 30% of all Monero currency that is mined, with the other 70% sent to the cryptocurrency wallet that is associated with the mining account.
- Payments made even if the mining is carried out without the user's consent.
- Even though Coinhive is a legitimate distributed mining utility providing a valid source of revenue in lieu of ads on webpages, it often surfaces on hacked websites.
- Restricts CPU usage – avoids triggering alarms

Specific attacks

Cryptocurrency theft

- Pony botnet software
  - 2014
  - Linked to the theft of more than $200,000 in cryptocurrency wallets of about 30 different currencies such as bitcoin, dogecoin, and litecoin.
- Activated by clicks on suspicious links or spam software that was hidden inside executable files.
  - Once activated, it avoided detection by antivirus software and was able to access the wallet.dat files on users' computers.

Clipboard Hijacking

- Exploits the fact the long cryptocurrency wallet addresses made up of alphanumeric characters are difficult to remember.
  - Users copy and paste this information on a clipboard.
- ComboJack malware
  - Installed by clicking on an infected attachment, scans the clipboard every half second and scans it for wallet addresses.
  - Once a wallet address is detected, ComboJack replaces it with a hard-coded wallet address belonging to the attacker.
  - The unsuspecting user, in the meanwhile, returns to the clipboard and pastes the address inserted in the clipboard by ComboJack

Attacking underlying structure

- BGP hijacking
  - BGP routing protocol, which is used to store and broadcast route information between neighbor networks.
  - BGP does not check for the validity of broadcasted route announcements, it was exploited to inject fraudulent route information from an autonomous system (AS) to intercept and send traffic to the wrong destination.
  - Enable node and network-wide attacks by isolating portions of the network (partitioning attack).
  - BGP hijacking was also able to slow traffic and thereby propagation of blocks in the bitcoin protocol toward other nodes (delay attack).
  - Causes hundreds of events every month

Prominent Cryptomining Botnets

ZeroAccess Botnet

- First appeared in 2011
- Largest known botnet that uses P2P mechanisms for communication
- Initial version: bitcoin mining
- Newer version: click fraud
- Distributed architecture: redundancy and robustness
- Test operation results
  - At the Bitcoin USD rate of 131, the potential benefits of bitcoin mining using ZeroAccess were less than 50 cents a day for one computer, versus thousands of dollars a day for a botnet.
  - In contrast, the click fraud operation of ZeroAccess was more profitable, resulting in potentially tens of millions of dollars a year.

Smominru botnet

- 2017
- Shadow Brokers released a GB worth of exploits developed by the NSA.
- Targeted Windows vulnerabilities, specifically Windows SMB protocol
- Worm-like capabilities
- Powered by Eternal Blue exploit
  - Leveraged in WannaMine – click on fraudulent link
- Turned infected machines, mostly servers, into cryptominers
- Peak: 526,000 machines, ~ $2.3 million in revenue

Dofoil

- Cryptomining application
- Spread to half a million computers in less than 24 hours
- Used a combination of spawned processes
- Modified Windows registry and opened connection remote C&C architecture
- Resist detection

Adylkuzz

- Used both EternalBlue and DoublePulsar malware
- Provides a covert channel through which kernel code can be exploited
- WannaCry: linked to 3 hardcoded bitcoin wallets
- AdylKuzz: numerous wallets with small revenue
- Interesting side effect
  - Worked as a backdoor and closed the doors behind it to prevent further exploitation of SMB vulnerability
  - Machines protected from WannaCry

Botnets targeting mobile apps, websites and IoT devices

Botnets Targeting Mobile Apps

- Google Play apps
  - Recitiamo Santo Rosario Free
  - SafetyNet Wireless App
  - Wallpaper apps containing BadLepricon - mine
- Repackaged versions of popular apps
  - Football Manager Handheld
  - Songs
  - TuneIn Radio
  - Prized
- Mode of operation
  - JS Miner: load JS library from Conhive
  - CPU Miner: apps are repackaged versions of legitimate apps that are infected with CPU mining code

Honorable mention: Loapi

- Discovered by Kaspersky Labs
  - Downloads a Monero cryptocurrency miner that overheats the phone components and destroys the phone.
  - Dubbed as a jack-of-all-trades
  - Performs cryptomining, launching DDoS attacks, inject ads, and ability to hide under the logos of antivirus solutions and porn sites
  - Capable of boosting ratings for ads, directing SMS messages, and subscribing users to paid services.

Botnets Targeting Websites

- Cryptomining software has been found on a variety of sites
  - WordPress
  - CBS Showtime
  - Live chat and help widgets
  - BitTorrent distributions sites
  - Starbucks public WiFi
  - Desktop version of FB Messenger
  - Steam

Botnets Targeting IoTs

- Mirai botnet
  - Targeted insecure IoT devices, while avoiding device addresses linking to GE, HP, or the US DoD.
  - Scanned the Internet for big blocks of open Telnet ports
  - Used default user ID/password combinations to gain control of closed-circuit TVs, DVRs, and routers in one of the biggest IoT-powered attacks.
  - Although initially Mirai was used to launch DDoS attacks, recent variants of Mirai include bitcoin mining modules.

Countermeasures for cryptomining botnets

Profiling

- Signature-based detection
- Software profiling
- Hardware profiling

Countermeasusres for cryptomining botnets	Profiling	Software profiling
		Hardware profiling
	Secure web development frameworks	Blacklists and whitelists
		Adstripping/blocking browser tools
		Content Security Policy
	Software Engineering	Patching
		Reverse Engineering
		Network hardening
	Social frameworks	Legislation and poicies
		Open Source Intelligence (OSINT)

Profiling

- Software:
  - Unusually high CPU usage
  - Presence of traditional mining software (WebAssembly, WebWorkers)
  - Analyze code
  - MFA, CAPTCHAs, creation rate of new accounts and domain names
- Hardware:
  - Evaluate execution patterns
  - Look for network activity

Secure Web Development Frameworks

- Adstripping browsers
  - Would you like to watch our ads or would you rather spare CPU cycles for cryptomining?
- Blacklists
  - US DoT and Office of Foreign Assets Control (OFAC) publishes lists of Specially Designated Nationals and Blocked Persons List (SDN)
  - Use browser extensions (No Coin)
- Whitelists
  - CoinBlockerLists
  - Blocks software and kills loaded scripts

Novel approach

- Challenge of advertising revenue, user preferences, and privacy
- Basic Attention Token (BAT)
- Developed by the team that developed JavaScript and Firefox
- Ethereum-based digital token that eliminates the middlemen in the digital advertising spaces
- Users are rewarded for their attention in the form of BAT and publishers receive a majority of the ad revenue that was previously lost to bots and middlemen, and advertisers are able to obtain superior data analytics.
- Works with the Brave browser
- The Brave browser monitors user's activities, and the data is stored on a distributed ledger.
- Advertisers send ads in the form of smart contracts to the browser, which are unlocked when a user views the ads who then gets rewarded in BATs.
- BAT can be spent in the browser for premium articles, donations, and other in-browser transactions.

Other approaches

- Patching
- Reverse Engineering
- Network Hardening

Future Directions

- Cryptocurrencies are beginning to gain wider acceptance across various domains in government, banking, electronic commerce, and other sectors
- Raises several questions that are intertwined in the legal, fintech, and social spheres
- Still illegal in China, Bolivia, Columbia, Ecuador, Russia, Vietnam, and Russia, among others
- Even in countries where it is legal, differing laws on mining and use
- Regulations
- Need for more energy-efficient mining operations
- Perceptions matter
  - CryptoAsset Sentiment Survey

Thank you!

Questions