WHITE PAPER

Mighty Morphing Crypto Danger

Cryptomining Malware Gets More Destructive

neustar®

TABLE OF CONTENTS

CRYPTOMINING MALWARE: THE DARK SIDE OF THE CRYPTOCURRENCY REVOLUTION

Cryptocurrency has become mainstream.

Worldwide market capitalization for more than 4,500 cryptocurrencies[1] surged to over $1.8 trillion in March 2021[2] – in part a reflection of growing acceptance by institutional investors and corporate leaders.

Tesla started accepting bitcoin in February 2021, and purchased US$1.5 billion in the cryptocurrency for its own holdings.[3] A few days later Mastercard announced it would begin supporting selected cryptocurrencies on its network.[4]

But as cryptocurrency moves mainstream and gains value, cryptomining – the process of verifying transactions to earn cryptocurrency by solving extremely complex math problems –also becomes more profitable.

Cryptomining is especially profitable as a criminal enterprise, when illicit miners steal the enormous data processing capacity and energy resources that it requires.

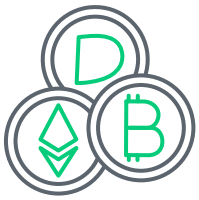
The key is cryptomining malware – covert mining code that can be embedded in your network servers, web applications and cloud containers to subjugate your IT assets by hijacking your processing and electrical power.

That's just for starters. The newest generation of cryptomining malware has introduced a whole new array of threats.

Cryptomining malware subjugates your IT assets and hijacks your processing and electrical power. That's just for starters.

1 Number of Cryptocurrencies Worldwide from 2013 to 2021, Statista.com, February 15, 2021
2 Global Cryptocurrency Charts, CoinMarketCap.com
3 Steve Kovach, "Tesla Buys $1.5 Billion in Bitcoin, Plans to Accept it as Payment," CNBC.com, February 8, 2021
4 Chris Isidore, "Bitcoin's Big Moment: Mastercard jumps on the Bandwagon," CNN.com, February 11, 2021

CRYPTO BASICS

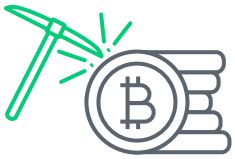


Cryptocurrency

A digital currency with ownership records stored in a database secured by strong cryptography, and transactions recorded in a digital ledger using blockchain technology.

Cryptomining

The process of verifying cryptocurrency transactions and adding them to the blockchain ledger and earn cryptocurrency as a reward. Multiple miners compete to verify each block of transactions using a proof-of-work algorithm that involves extremely complex mathematical problems requiring significant processing resources.



Cryptomining Malware or Cryptojacking

Malware inserted into a network or web application to perform cryptomining work by covertly stealing processing power, typically as part of a distributed network, to earn free cryptocurrency for the illicit miner.

Cloud Cryptojacking

Cryptomining malware that compromises cloud environments and cloud containers from Amazon Web Services (AWS) and other cloud service providers, typically via exposed or misconfigured APIs (Application Programming Interfaces) and ports, or malicious Docker images.

AN EVOLVING, DEEPENING THREAT

No online threat is static, and that's especially true of cryptomining malware.

It started as a bit of JavaScript, intended as a legitimate revenue alternative to website ads. Sites would be able to earn cryptocurrency by enlisting the devices of their visitors for cryptomining[5]—supposedly with the consent of the visitors.

The consent part didn't last.

By mid 2018, browser-based JavaScript had morphed to executable malware that could be inserted into computers and networks – and it accounted for 35% of online threats.[6] One miner infected more than 500,000 machines, pocketing an estimated US$2.6 million.[7]

Cryptomining malware syphons significant processing power from its host to solve the complex problems that serve as proof-of-work for verification of a block of cryptocurrency transactions.

Its spread was documented and reported. But the threat didn't gain the same notoriety – or the same focused efforts at prevention – as other prominent cybercrimes, for a couple of reasons:

1. **It's not readily visible, and hard to find.** Unlike ransomware or RDDoS (Ransom Distributed Denial of Service) threats – which have to announce themselves to earn money for the cybercrook – cryptomining malware succeeds by remaining invisible and undetected.
2. **"All" it does is steal resources.** It doesn't lock out users, or encrypt files, or flood your servers. The effects of first-generation cryptomining malware were generally limited:
   - Reduced processing power resulting in slower operations and, occasionally, damaged hardware
   - Increased power consumption, boosting your electric bill and sometimes resulting in overheating.

That was the first generation. Now it's more serious.

More electricity than what?

Cryptomining for bitcoin alone consumes more electricity than Argentina[8].

5 Ben Dixon, "A Guide to Cryptojacking," TheDailySwig.com, April 3, 2020
6 "2018 Webroot Threat Report Mid-year Update," September 2018
7 Danny Palmer, "A Giant Botnet Is Forcing Windows Servers to Mine Cryptocurrency," ZDNet, February 1, 2018
8 Cristina Criddle, "Bitcoin Consumer 'More Electricity than Argentina'." BBC.com, February 10, 2021

Today, cryptomining malware has evolved into a far greater threat.

Infections are way up, and it's even harder to detect. The soaring value of bitcoin and other cryptocurrencies has made cryptomining a far more profitable business, and cybercriminals always follow the money.

- In Q4 2020, cryptomining malware surged by 53% compared to Q3.[9]

That's just detections – and many current versions of the malware employ evasion techniques to install itself only if it is likely to go undetected.[10]

The malware threatens and attacks more assets. Just as the first versions of browser-based malware evolved to infect Windows machines, today's versions have adapted to threaten an ever-growing range of digital assets, including:

- Linux machines
- Web apps and cloud containers from AWS, Google and other providers
- IoT devices[11]

Infections have more – and more dangerous – consequences. The risks are no longer just diminished processing power and stolen electricity. Bad actors have added new, more malevolent capabilities into the malware. For example:

- More of your servers can be infected by variants with worm capabilities[12]
- Your assets can be commandeered into a botnet for both cryptomining and DDoS (Distributed Denial of Service) attacks[13]
- AWS credentials, Docker API logins and other sensitive credentials can be stolen[14]

Cryptomining malware is an intensifying threat that demands serious prevention efforts.

9 Phil Muncaster, "Coin-Mining Malware Volumes Soar 53% in Q4 2020," Infosecurity Magazine, January 20, 2021
10 Matthew Beedham, "New Cryptocurrency Mining Malware Is Spreading across Thailand and the US," TheNextWeb.com, June 4, 2019
11 Prajeet Nair, "Cryptomining Worm now Targets Web Apps, IoT Devices," BankInfoSecurity.com, December 17, 2020
12 Sergiu Gatlan, "Malware Spreads as a Worm, Uses Cryptojacking Module to Mine for Monero," BleepingComputer, March 12, 2019
13 Lindsey O'Donnell, "Linux Devices Under Attack by New FreakOut Malware," ThreatPost.com, January 19, 2021
14 Catalin Cimpanu, "A Crypto-mining Botnet Is now Stealing Docker and AWS Credentials," ZDNet, January 8, 2021

ATTACK VECTORS

Are you infected?

Since cryptomining malware is designed to go undetected, look for indirect evidence:

- Increases in processor utilization
- Non-seasonal increases in electricity consumption
- Suspicious patterns in network traffic from C&C communication

One of the challenges of countering cryptomining malware is the sheer variety of attack vectors and delivery methods targeting both devices and cloud applications:

Attacks targeting open or misconfigured APIs including web applications with an open port, Docker containers with an exposed API, and hosts with an open port

Attacks exploiting malicious docker images infect containers, and in some versions steal AWS credentials

Phishing and spear phishing emails with a malicious link that runs code to place a cryptomining script on the device

Malvertising and compromised websites with malicious code that installs malware when clicked by an unsuspecting user

Infected applications, files or browser extensions that install cryptomining malware when downloaded by users

Attacks covered by a diversionary DDoS attack that dominates the attention of the IT security team and allows the bad guys to insert the malware into a server

DNS hijack that steers users to a malicious site, either by poisoning your DNS cache or by taking over a legitimate website your users frequent

ANATOMY OF CRYPTOMINING INFECTIONS

Attacker targets open port in web app or open API in container

User clicks on phishing email, visits malicious site, or downloads infected file

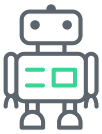
Attacker inserts malware via DNS hijack or during DDoS attack

Cryptomining malware installs on device(s) or cloud-based resources

Worm component (if present) searches to infect more devices

Malware communicates with external command-and-control server or botnet for assignments

Malware commandeers processor to run cryptomining processes, reducing performance



May join botnet for additional malicious activities such as DDoS attacks

HEADING OFF THE THREAT

With so many attack vectors it should be no surprise that there is no magic bullet to prevent cryptomining malware from infecting your assets.

The most effective approach is a comprehensive strategy that utilizes a variety of protective tools and practices across multiple layers of defense, including these best practices:

- Employ a web application firewall to protect web apps
- Use a recursive DNS service that includes a DNS firewall
- Make sure you have comprehensive DDoS protection
- Be ready to identify and counter a DNS hijack attempt
- Implement a rigorous phishing defense program including user education
- Plan and control software patches, updates and fixes for immediate, secure implementation
- Conduct vulnerability and penetration testing using an outside agent

Cryptominers collected US$4.06 million in a single hour on February 11, 2021.[15]

15 Omkar Godbole, "Bitcoin Miners Earn Record Hourly Revenue of $4M," Coindesk.com, February 12, 2021

HOW NEUSTAR CAN HELP

You can protect your assets from being commandeered by cryptomining malware more effectively with an effective defensive posture. The security experts at Neustar can help, with four essential services to strengthen your defenses.

1 **UltraWAF Web Application Firewall** UltraWAF is a cloud-based security tool that protects your web applications wherever they are hosted. Its flexible deployment options include both a negative security capability, which only blocks traffic that includes an identified threat or attack, and a positive security capability that only allows traffic that is explicitly permitted. It also offers a powerful learning mode that monitors and profiles traffic to your applications to help distinguish between truly anomalous and potentially malicious traffic on one hand, and patterns that are unusual but still legitimate on the other.

2 **UltraDNS Firewall** Neustar UltraDNS Firewall is an integral filtering component of our enterprise-grade, cloud-based recursive DNS service. It blocks communication between DNS-reliant cryptomining malware and external command and control (C&C) servers or botnets, leaving the malware idle. It also helps prevent malware from entering your network in the first place by blocking access to malicious and suspect websites and sources from any device, using threat intelligence from Neustar and other sources. Finally, UltraDNS Firewall makes it easier to identify and remove malware without impacting business operations.

3 **DDoS Protection** Neustar offers a flexible, highly capable suite of DDoS mitigation solutions, including our always-on, cloud-based UltraDDoS Protect as well as hybrid and on-premise options. With a massive global mitigation infrastructure that delivers industry leading scrubbing capacity and near instantaneous detection and deflection capabilities, our solutions can handle even the largest volumetric attacks, protecting you from DDoS attacks that can be used as a diversion to cover cryptomining malware as well as other malicious attacks, including DDoS ransom attacks.

4 **Professional Services** The rapid evolution of cryptomining malware to attack and compromise new assets, including cloud resources like web apps and containers, along with the sheer number of attack vectors make it a particularly challenging threat. Neustar professional services can help your IT security team get up to speed quickly with network vulnerability assessments and recommendations, resolution of patch/fix issues, disaster recovery planning and employee training. Neustar can also conduct penetration testing to simulate actual attacks and assess your network readiness.

ABOUT NEUSTAR

Neustar is an information services and technology company and a leader in identity resolution providing the data and technology that enables trusted connections between companies and people at the moments that matter most. Neustar offers industry-leading solutions in Marketing, Risk, Communications, and Security that responsibly connect data on people, devices and locations, continuously corroborated through billions of transactions. Neustar serves more than 8,000 clients worldwide, including 60 of the Fortune 100. Learn how your company can benefit from the power of trusted connections at www.home.neustar.

WP-SEC-295760-05.17.2021