Fighting Back Against

CRYPTOJACKING

Matthew Hickey
Director, Sales Engineering
The Threat Landscape Has Shifted

Ransomware
- 26% of threats

Advanced Malware
- 20% of threats

Email Malware
- 20% of threats

Web Malware
- 12% of threats

Generic Malware
- 12% of threats

Cryptocurrency/Financial Malware
- 8% of threats

Privilege Escalation
- 1% of threats

Bots
- 1% of threats

Exploits
- Most organizations have no exploit prevention

Source: SophosLabs

54% of organizations hit twice on average in 2017

83% agree it has become more difficult to stop threats

^Source: The State of Endpoint Security Today Survey
The Evolution of a Ransomware Attack

Samsam’s Evolutionary Timeline

- **DECEMBER 2015**
  SamSam beta testing, Base64 encoded.

- **FEBRUARY 2016**
  Payment sites moved to the dark web.

- **JUNE 2016**
  June version 2, AES encrypted.

- **JUNE 2017**
  SamSam version 2, garbage code added to avoid detection.

- **OCTOBER 2017**
  SamSam version 3, encrypted payload ‘stubbin’. Password required to launch the ransomware.

- **JUNE 2018**
  SamSam version 3, encrypted payload changed to ‘.satoshi’.

- **DECEMBER 2017**
  Highest ransom paid, $64,000 USD.

- **APRIL 2018**
  SamSam version 3, encrypted payload changed to ‘.berkshire’.

- **JULY 2018**
  SamSam version 3, encrypted payload changed to ‘.sophos’.

SOPHOS
Attack Stretched Across Globe

Percentage of SamSam victims by country, as identified by Sophos

Source: SOPHOS
Percentage of SamSam victims by industry sector

- Government: 13%
- Healthcare: 26%
- Education: 11%

Percentage of SamSam victims by sector that went public

- Education: 38%
- Healthcare: 78%
- Government: 100%
- Private Sector: 0%
Monetization of Compromization
Generic Malware

Phase 1: Deliver malware

Phase 2: ???

Phase 3: Profit...?
Ransomware

Phase 1
Deliver ransomware

Phase 2
Encrypt files

Phase 3
Maybe Profit?
Cryptojacking Malware

Phase 1
Deliver cryptojacking malware

Phase 2
Mine coins

Phase 3
Profit!
NOW CRYPTOJACKING THREATENS CRITICAL INFRASTRUCTURE, TOO

Iceland: Crypto Mining Companies Will Consume More Energy Than Households In 2018

Ready-Made Crypto Mining Kits Lure More Than Geeks in Singapore

U.S., UK government websites infected with crypto-mining malware: report

Cryptojacking attack hits Australian government websites

Iceland is set to consume more energy for crypto mining than for household use this year, the Associated Press reports Monday, Feb. 12. The naturally cold climate and access to renewable resources make it a prime location for mining operations.

Thousands of websites, including ones run by U.S. and UK government agencies, became infected with malware that causes web browsers to secretly mine cryptocurrency.

Ready-made crypto mining kits are luring more than just geeks. Sophos researchers have discovered that ready-made kits are being distributed via malicious websites, making it easier for cybercriminals to infect unsuspecting users.
Setting the Stage

Cryptomining
- The act of performing the complex calculations required to generate cryptocurrency
- Legitimate and malicious usage
- You may (or may not) keep the cryptocurrency proceeds

Cryptojacking
- Stealing resources to mine for cryptocurrency without obtaining permission
- All cryptojacking is cryptomining and is 100% malicious
- The bad guys keep the cryptocurrency proceeds

Miners
- Computers/people that are paid a certain number of units of the cryptocurrency for their work
- Two primary jobs:
  - Generating cryptocurrency
  - Validating transactions on the blockchain

Blockchain
- A shared ledger duplicated several times across a network of computers
- Run by miners to tally transactions, ensure authenticity, etc.
Table Stakes

**Hardware**
*Casual or business, you need to invest in hardware. A reasonable ROI is expected.*

**Keeping up with the competition**
*To win requires more and more power over time, as more people invest in more powerful hardware.*

**The power of one (or not, in this case)**
*As a single casual miner, you’re unlikely to mine successfully. The bad guys understand this too!*
How to be a miner in four easy steps
Legitimate Mining

Step 1: Find a job!

- Known as joining a pool
- It’s really like getting a job
  - What do I need to do?
  - What do I get paid for my effort?

Step 2: Deposit my salary here...

- Where is your wallet?
- Hardware, or Software, or an Exchange...
Legitimate Mining

Step 3: **Start working...**

- Download your mining program of choice
- Most will use a GPU in preference to CPU
- Config file from the Pool

Step 4: **Get paid...**
Seriously. I can take it.
Get technical on me.
Geeking out on the Blockchain

Private Key Cryptography

Distributed Network

Client

Database

Block

Hashed History
Description
Time
Public Key

User A
A's Public Key
A's Private Key
Mining Etherium

Mining Etherium in 3 bullet points
• Miners will run the block’s unique header metadata through a hash function
• If the miner finds a hash that matches the current target, the miner will be awarded Ether
• Broadcast the block across the network. Validated and added to every copy of the blockchain

That sounds too hard, let’s cheat!
• Called “Proof of Work” for a reason
• Considering moving to “Proof of Stake”
• Difficult to manipulate the blockchain
The Many Faces of Cryptojacking
The Rise Of Malicious JavaScript Miners

- Cryptocurrencies surged in value during 2017
- Crooks turned to malicious JavaScript miners to generate cryptocurrency
- When a user surfs to a site or page hosting a malicious JS miner it just runs
- CPU increases. The device slows to a crawl and gets hotter and hotter
Javascript Miner Example: CoinHive
Demo: CPU Surge When Visiting Infected Site
The Grey-Zone of JavaScript Miners

“Watch our ads or we’ll use your CPU for cryptomining”

• Legitimate websites want to make money
• What’s the lesser of two evils?
• Legitimate or malicious?
WannaMine – A Native Code Attack

**We Want You...To Mine for Us!**

- WannaMine similar to WannaCry but installs a miner instead ransomware
- Native mobile apps, or modified popular apps can include mining code
- Steals your resources, productivity and makes money for the bad guys
What does cryptojacking mean for my organization?
The Downsides of Cryptojacking

1. **The unbudgeted operating expenses** from powering computers to work for someone else.

2. **The opportunity costs** because legitimate works gets slowed down.

3. **The security risks** from who-knows-what untrusted programs and network connections.

4. **The reputational and regulatory costs** of reporting, investigating and explaining the cryptomining activity.

5. **The ethical concerns** of allowing employees to legitimately mine. Are they now the bad guy?
The Sophos Position

“In the absence of a reliable way to differentiate between consensual and non-consensual mining, the bad apples ruin the good ones”
- Joe Levy, CTO, Sophos

- Cryptomining
- Cryptojacking
How To Stop Cryptominers
Protecting against JavaScript Cryptojacking

Sophos XG Firewall
First line of defense.
Block it and don’t let it onto your network!

Central Server Protection
Don’t let it execute on your server.

Sophos Central Endpoint
Last line of defense. Don’t let it execute.

Sophos Mobile
Block known mining websites both on and off your network
Protecting against Native Code Cryptojacking

Sophos XG Firewall
First line of defense. Block malware from getting onto your network!

Sophos Intercept X for Server (EAP est. May 2018)
Block the exploit techniques used to spread cryptojacking

Sophos Intercept X
Blocks the exploit techniques used to spread cryptojacking. Deep Learning detects and blocks malicious executables

Sophos Central Endpoint
Endpoint Protection file scanning detects and blocks malicious executables.

Synchronized Security
Unparalleled visibility into all cryptomining apps running on your network. Deny or Allow?

Sophos Mobile
Stop malicious apps being installed on your mobile devices
Best Practices

• Keep your devices patched – minimize risks of exploits
• Use mobile management technology – stop cryptojacking apps
• Educate your team:
  o Cryptomining is NOT an acceptable use of your company’s resources.
  o The importance of stopping traditional malware vectors e.g. phishing
• Maintain a strong password policy
• Keep an eye out for the tell-tale signs that you’re being cryptojacked
  o Slow network
  o Spike in CPU consumption
  o Soaring electricity bill
Next Steps
Read the Cryptojacking whitepaper
sophos.com/cryptojacking

Standing Up to CRYPTOJACKING
Best Practices for Fighting Back

Cryptojacking has recently erupted onto the cybercrime scene, thanks to the surge in value during 2017 of cryptocurrencies such as Bitcoin, Monero, and Ethereum.

Criminals are aggressively targeting laptops, desktops, servers, and even mobile devices. From a single device to entire networks, they infect as many devices as they can to mine for cryptocurrency on, or while using, other people’s computers. Simply put, you do the work, pay for the electricity and hardware, and they pocket the rewards.

Read this paper to learn how to fight back! We’ll explore the differences between legitimate mining and cryptojacking, how cryptojacking works, the costs of cryptojacking to today’s organizations, and practical steps you can take to avoid being a victim of cryptojacking.
Further Reading:

SamSam Whitepaper

How to Stay Protected Against Ransomware
Further Reading:

Naked Security

- https://nakedsecurity.sophos.com/2018/02/14/watch-our-ads-or-well-use-your-cpu-for-cryptomining/
- https://nakedsecurity.sophos.com/2018/01/31/what-are-wannamine-attacks-and-how-do-i-avoid-them/

Sophos Knowledge Base

- Block JavaScript Cryptominers: https://community.sophos.com/kb/en-us/127988