How to detect & respond on crpytojacking and cryptomining malware

eFocus, 24th Apr 2018

Roman Cupka, Principal Consultant CEE

Flowmon
Driving Network Visibility

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware		→
2. Web based attacks	↑	2. Web based attacks		→
3. Web application attacks	↑	3. Web application attacks		→
4. Denial of service	↑	4. Phishing		↑
5. Botnets	↑	5. Spam		↑
6. Phishing	⊃	6. Denial of service		↓
7. Spam	↓	7. Ransomware		↑
8. Ransomware	⊃	8. Botnets		↓
9. Insider threat	⊃	9. Insider threat		→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss		→
11. Exploit kits	↑	11. Data breaches		↑
12. Data breaches	↑	12. Identity theft		↑
13. Identity theft	↓	13. Information leakage		↑
14. Information leakage	↑	14. Exploit kits		↓
15. Cyber espionage	↓	15. Cyber espionage		→

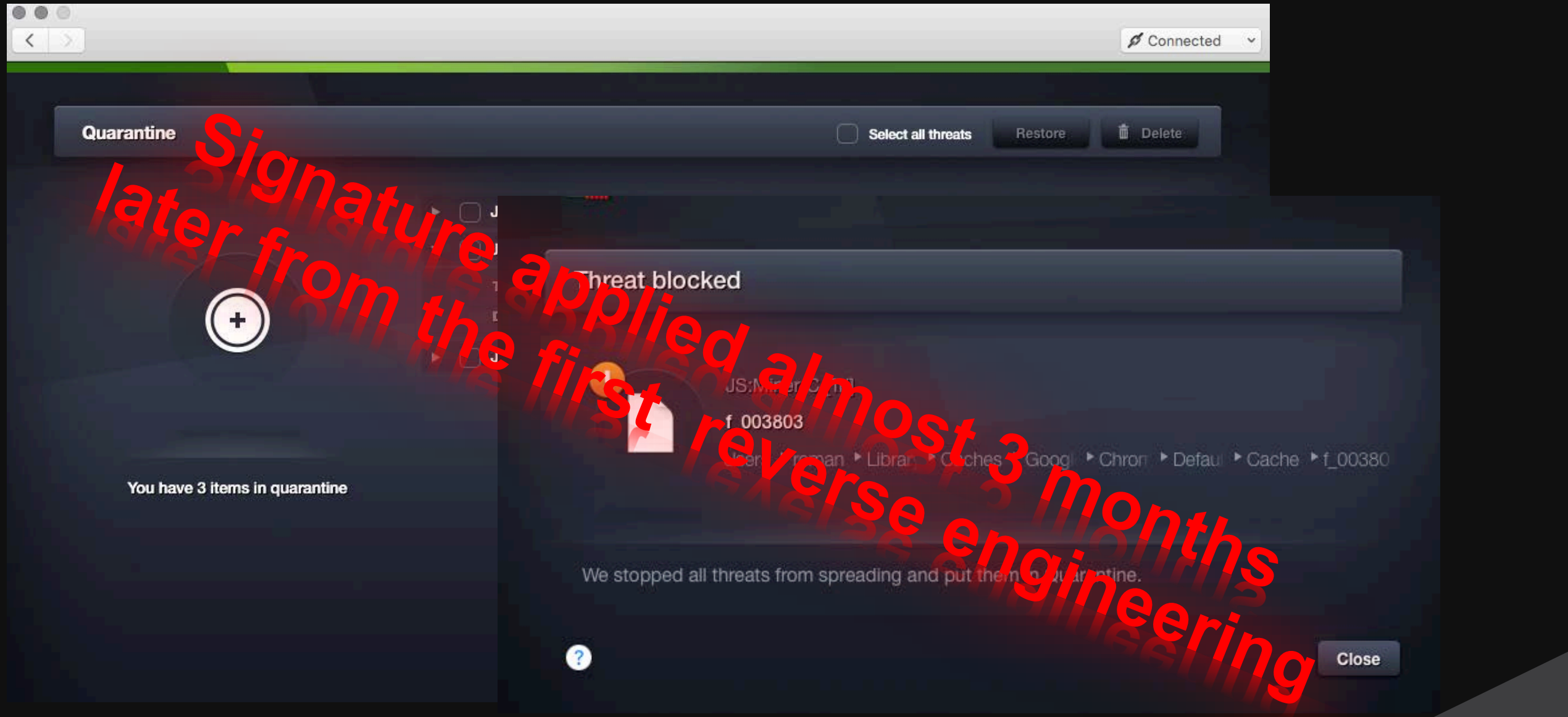
Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Figure 1: Overview and comparison of the current threat landscape 2017 with the one of 2016.

3 Malware Trends to Watch Out for in 2018 (Minerva Labs)

- Evasive Techniques
- Defenders' Hope for Vaccination
- The Rise of Cryptomining Malware

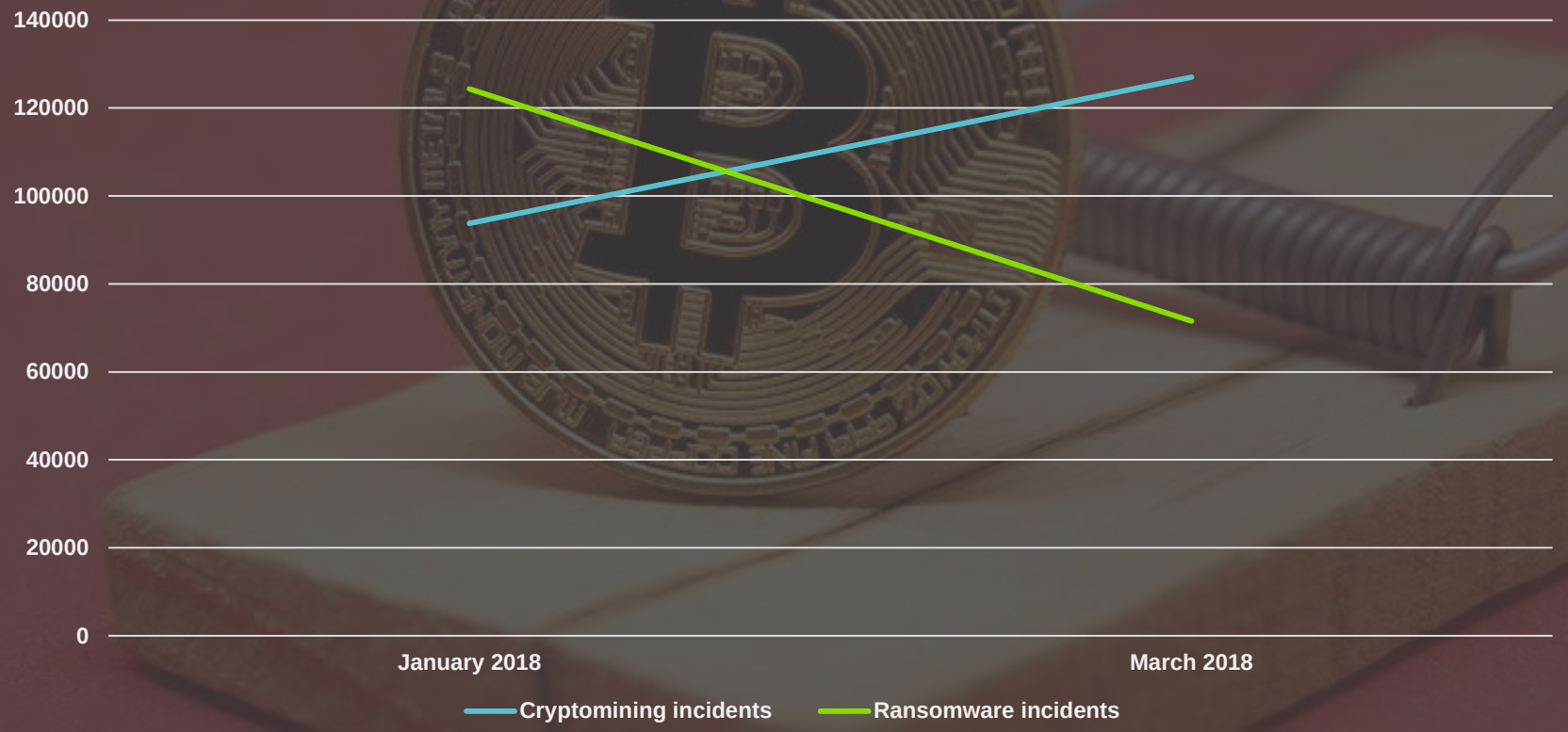
Flowmon
Driving Network Visibility



Signature applied almost 3 months later from the first reverse engineering

Flowmon
Driving Network Visibility

***Cryptominer-based attacks*, not ransomware-based attacks, have been the *top threat* so far *this year*, according to Comodo Cybersecurity Threat Research Labs' *Q1 Global Malware Report.* "Hackers see cryptojacking as a cheaper, more profitable alternative to ransomware,"**



Flowmon
Driving Network Visibility


Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency — infecting enterprise infrastructure with crypto mining software — to have a steady, reliable, ongoing revenue stream.

Hackers do this by either getting the victim to click on a malicious link in an email that loads crypto mining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser.

Flowmon
Driving Network Visibility

Cryptojacking malware is relatively simple (but can go undetected for a long time)

Phishing campaigns
Malvertising
Compromised websites
Software downloads

Servers, computers, smartphones.
(steal CPU power to mine cryptocurrencies)

CSO – security issue
CIO – operational issue
CFO/CEO– financial & reputation impact

Flowmon
Driving Network Visibility

Russian Scientists Arrested for Using Nuclear Weapon F to Mine Bitcoins

Saturday, February 10, 2018 Wang Wei

Share 21.6k Share Tweet Share

Lessons from the Cryptojacking At

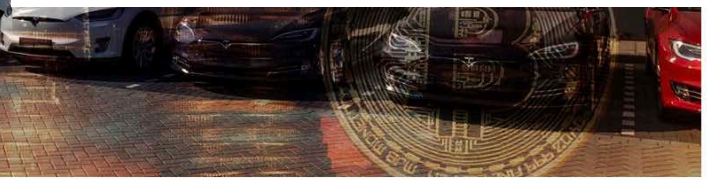
RedLock CSI Team
02.20.18 6:00 AM

4000 Government Websites Hacked in less than 4 Hours to Mine Cryptocurrency

Water Utility in Europe Hit by Cryptocurrency Malware Mining Attack

By: Sean Michael Kerner | February 07, 2018

Unauthorized cryptocurrency mining attacks come to industrial control systems for the first time, as cryptojacking attacks continue to grow.



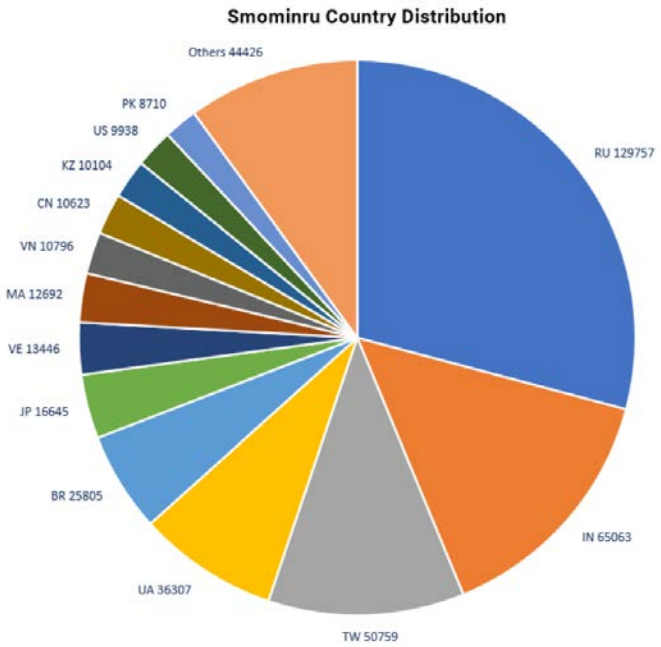
Unauthorized crytocurrency mining attacks, sometimes referred to as "cryptojacking" have found a new target - operational technology used in critical industrial infrastructure.

Security firm Radiflow, discovered that cryptocurrency mining malware was found in the network of a water utility provider in Europe. The attack is the first public discovery of an unauthorized cryptocurrency miner impacting industrial controls systems (ICS) or SCADA (supervisory control and data acquisition) servers.

"This is the first instance of such a cryptocurrency miner that we have seen in an industrial site," Ilan Barda, CEO

Cryptocurrency Mining Malware Using NSA Exploit

- Using the **EternalBlue SMB Exploit** (CVE-2017-0144) responsible for Wannacry
- **Smominru infection** has been observed in Russia, India, and Taiwan
  - Use of **Windows** Management Infrastructure (servers, computers)
  - Botnet mined **8900XMR** (31.1.2018 **since May2017**)
  - Using leaked NSA's **RDP** protocol exploit to find vulnerable systems
  - Botnet **C&C** hosted in DDoS protection service SharkTech



Flowmon
Driving Network Visibility

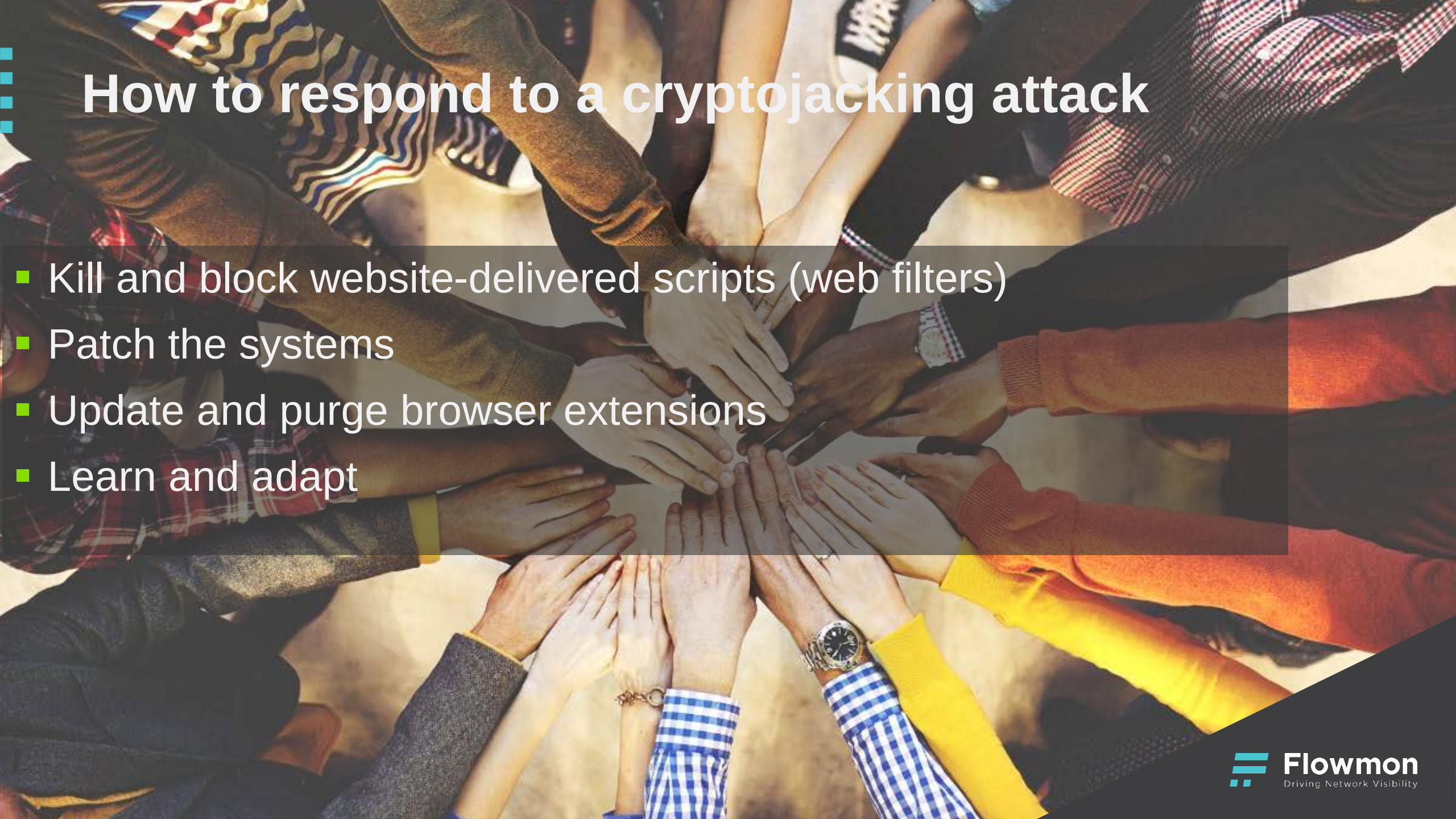
How to prevent cryptojacking

- Incorporate the cryptojacking threat into your security awareness training, focusing on phishing-type attempts
- Install an ad-blocking or anti-cryptomining extension on web browsers
- Keep your web filtering tools up to date
- Maintain browser extensions
- Use a mobile device management (MDM) solution to better control what's on users' devices

How to detect cryptojacking

- Train your help desk to look for signs of crypto mining
- **Deploy a network monitoring solution**
  - Receiving and returning hashes communication
  - Focusing on changes of suspicious ports and protocols
  - Suspicious patterns detecting by machine learning
  - AI with behavior based anomaly detection system
  - Threat Intelligent System

How to respond to a cryptojacking attack



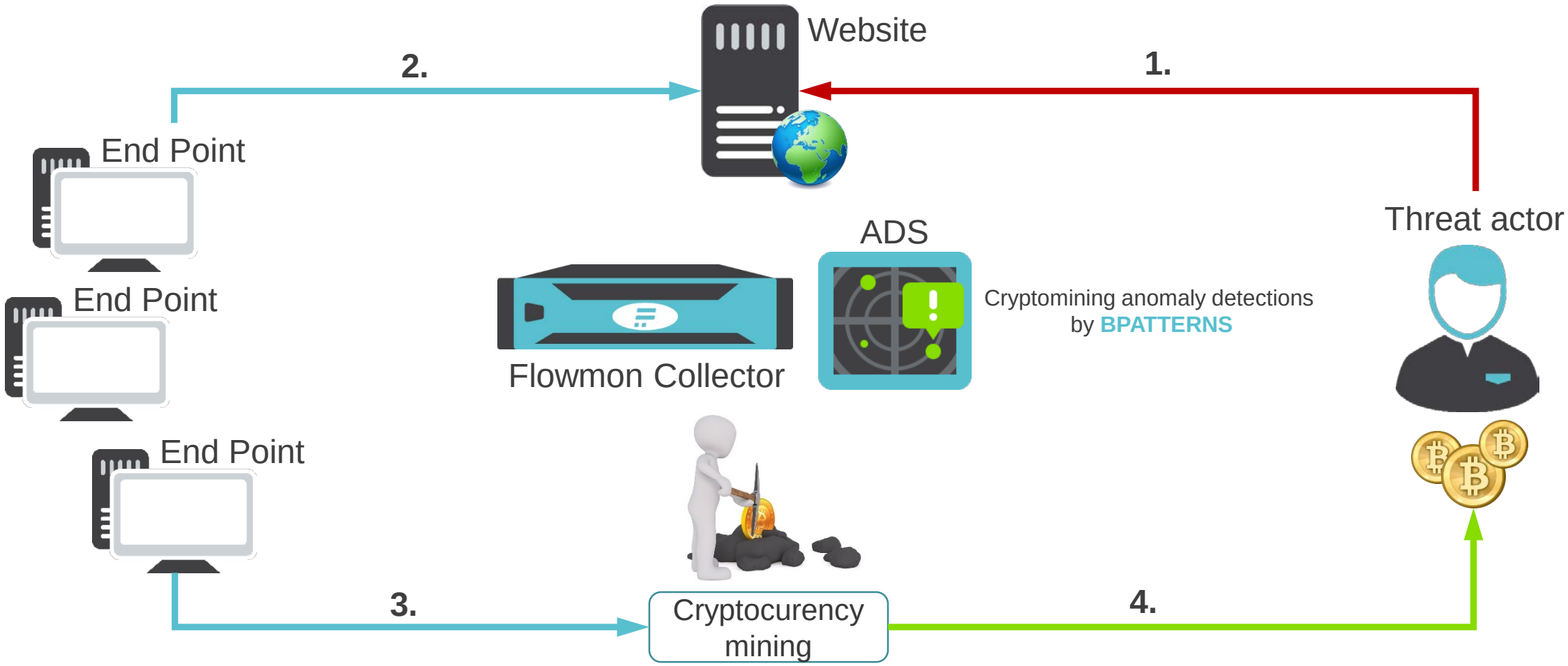
- Kill and block website-delivered scripts (web filters)
- Patch the systems
- Update and purge browser extensions
- Learn and adapt

Flowmon
Driving Network Visibility


THE DECISIVE FACTOR IN THE FIGHT AGAINST CYBER-THREATS.
Cryptojacking
Botnets
Malware
ARTIFICIAL INTELLIGENCE
Data exfiltration
Phishing
DDoS
Flowmon
Driving Network Visibility

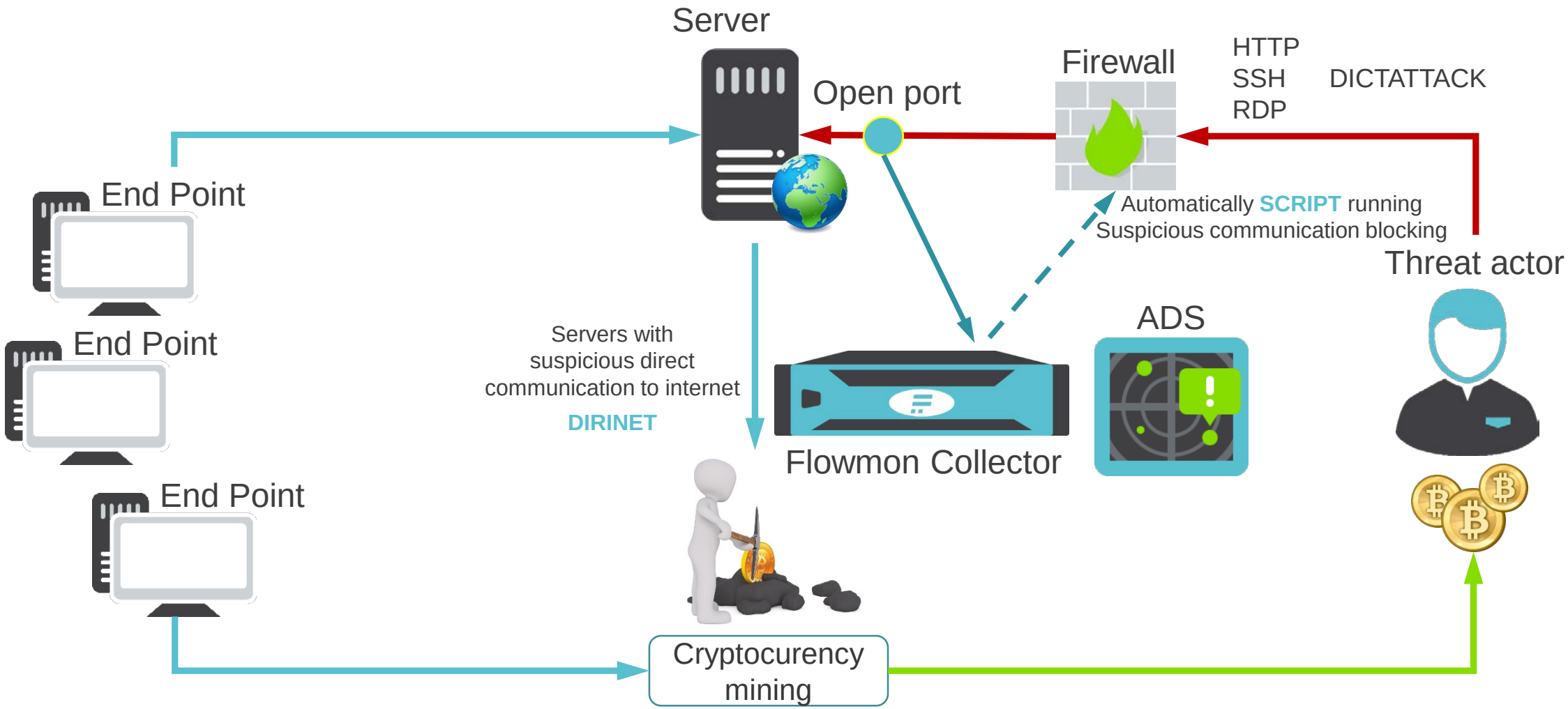
“Malware, like cyberspace itself, is merely a reflection of traditional, ‘real-world’ human affairs, and malware is always written for a purpose, whether it’s crime, espionage, terrorism or war,” *Dr. Kenneth Geers, chief research scientist at Comodo Cybersecurity*

Flowmon
Driving Network Visibility



https://www.flowmon.com/en/blog/crypto-jacking-crypto-mining

Flowmon
Driving Network Visibility



https://www.flowmon.com/en/blog/crypto-jacking-crypto-mining

Flowmon
Driving Network Visibility

BUILDING WALLS AND CHECK POINTS

90% of the security budget – mainly perimeter security - where only 25% of attacks target this point in the network.

ENSURING YOUR INVESTMENTS TO PREVENTION DO NOT GO WASTED

Flowmon stores the full statistical history of communication and provides on-demand and auto-triggered recording of detected incidents. It is a reliable source-of-truth and enables you to understand the characteristics of an attack and to discover bottle-necks, predict upcoming attacks and to insure better prevention.

LAYING CLEVER TRAPS

Early detection with Flowmon Anomaly Detection System covers gaps left by standard prevention technologies and represents the people, time, skillset which are lacking to identify a problem before it causes major impacts on company productivity.

REDUCING MEAN-TIME-TO-RESOLVE

Fundamental network and security tools that many of us already use in day-to-day operations have the capabilities necessary to block or restrict suspicious traffic. Use the whole potential of such technologies you have already implemented with Flowmon to provide a flexible incident response at no additional costs.

RESTORING BUSINESS AS USUAL

Eliminate unnecessary costs on IT operations and insure time-efficient disaster recovery with Flowmon, which helps you to conduct an assessment of the scope of the attack. This includes understanding what parts of the network have been compromised, what needs to be re-installed, recovered, and adjusted. Flowmon enables effective collaboration between all IT teams.

Flowmon
Driving Network Visibility

„Blockchain does not know that Bitcoin is dead“

A blockchain, originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography.

Bitcoin with “B” is a protocol that runs on this technology and gives it other possible features and capabilities.

Flowmon
Driving Network Visibility

REPLACE
the capacity, experience, skills and toolset your engineers lack

MEASURE
availability and reliability of your business critical services

PROVIDE
your admins the gear used during the whole lifecycle of network incident

COMPLY
with directives such as GDPR or NIS

Thank you for your attention

FIND
reliable source of truth across IT departments to collaborate on fast resolution

is what it takes to protect your productivity and data security, to protect your clients and your reputation

Flowmon
Driving Network Visibility