

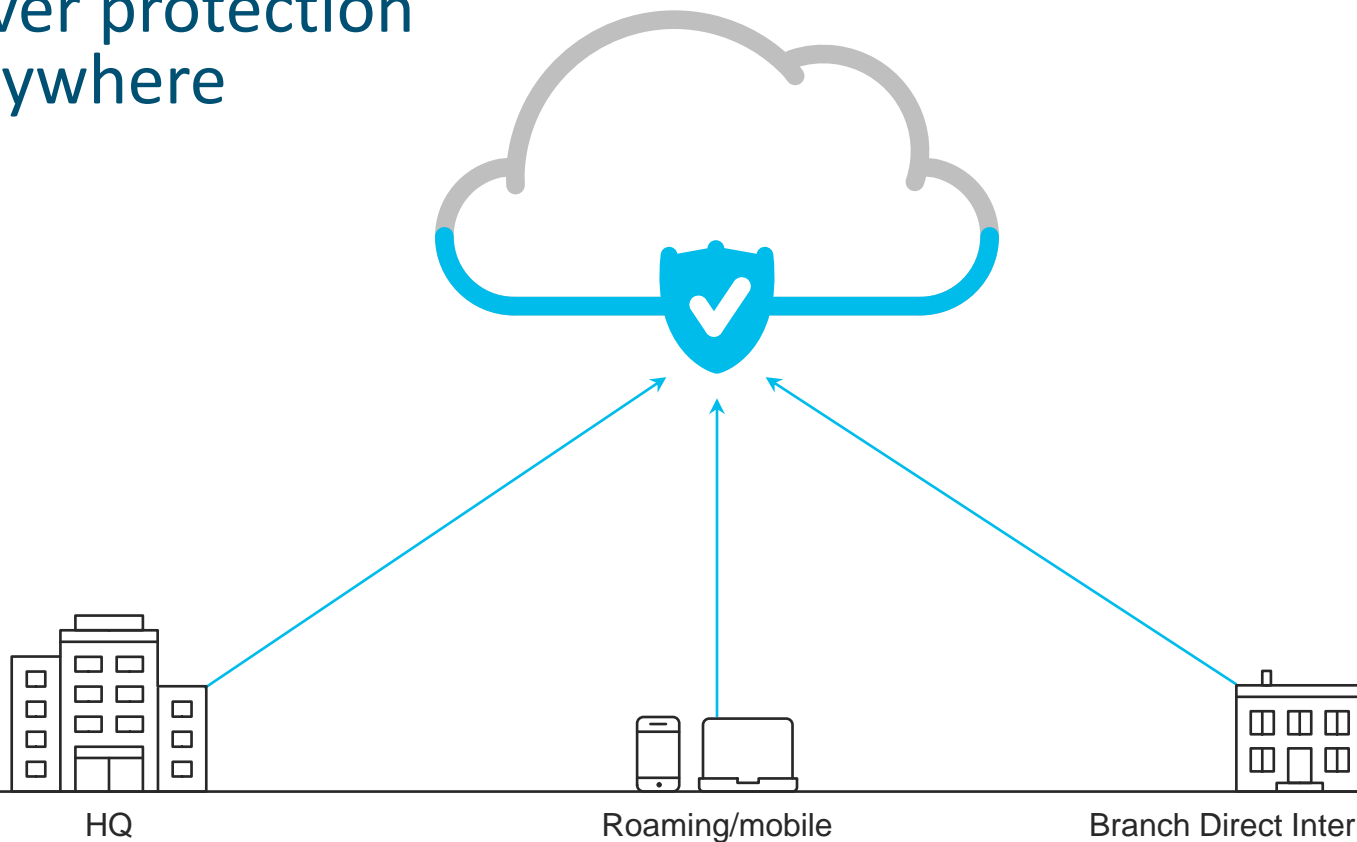


Securing your Journey to the Cloud

Alessandro Monforte, Regional Sales Manager, cloud security

Amonfort@cisco.com

Deliver protection everywhere



Boost existing security

Enable off-network

Transform edge security

Addressing key security challenges



Malware and
ransomware



Gaps in visibility,
coverage and
control



Cloud apps
and shadow IT



Difficult to
manage security

Our view of the internet

200B

requests
per day

90M

daily active
users

15K

enterprise
customers

160+

countries
worldwide



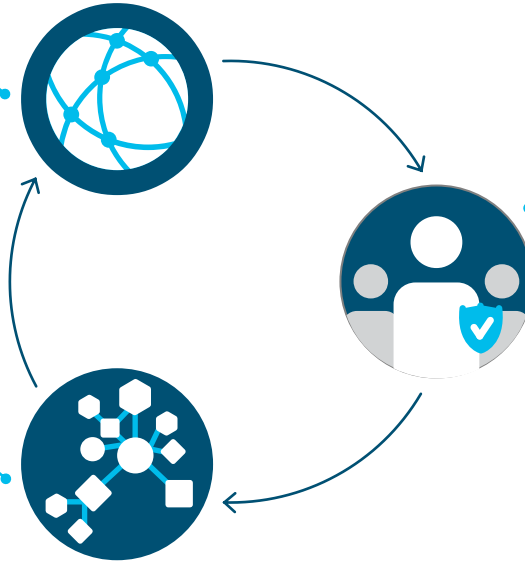
Cisco Talos: Intelligence to see attacks before launched

Data

- Cisco Talos feed of malicious domains, IPs, and URLs
- Umbrella DNS data — 200B requests per day

Models

- Dozens of models continuously analyze millions of live events per second
- Automatically uncover malware, ransomware, and other threats



Security researchers

- Industry renown researchers
- Build models that can automatically classify and score domains and IPs

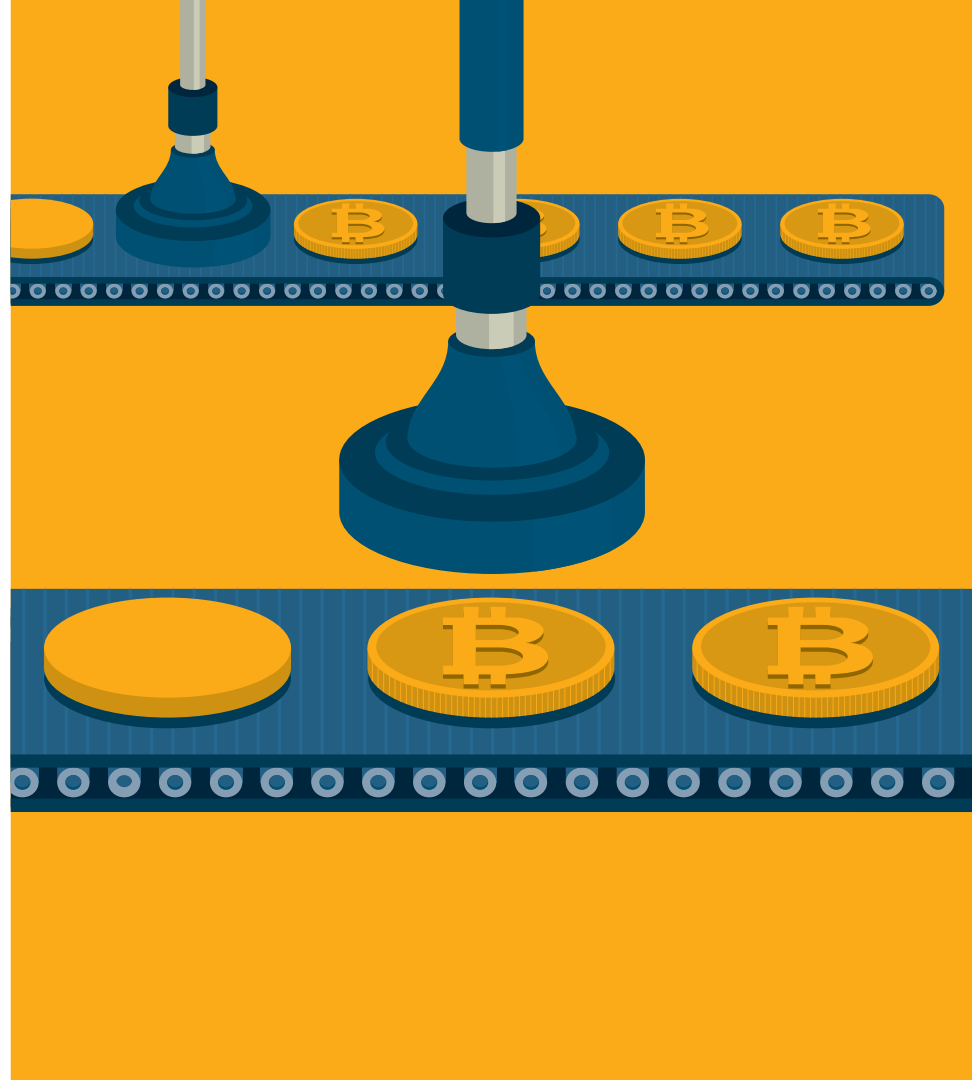
Cryptomining

The process of generating new units of the cryptocurrency

Not inherently bad, but could be

Bitcoin example:

- Miners use their computing power to verify a 3rd party's Bitcoin transactions
- Rewarded with new Bitcoins proportional to the amount of computing power they donated to the Bitcoin network



Cryptojacking

- Cryptojacking is “unethical” cryptomining
- Secret use of business’ computing power to mine cryptocurrencies through individual machines
- Done in browser JavaScript exploits, cloud AWS instances, etc.



COVID-19 Themed Malspam and Phishing

COVID-19 Concern

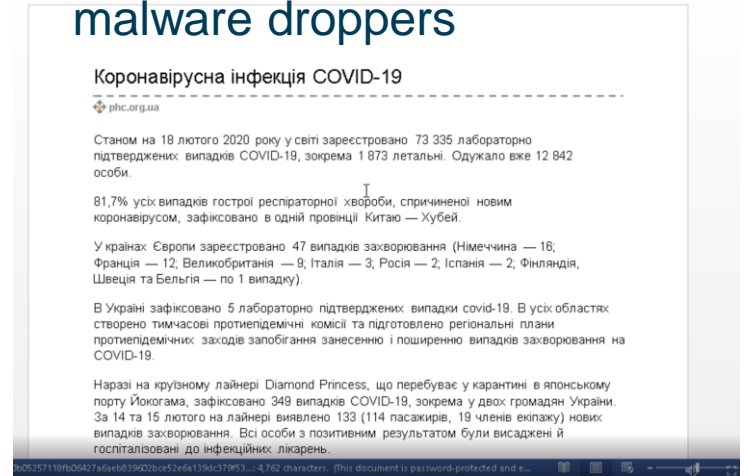
People want to be **informed, prepared**

People know **money is coming** from their government

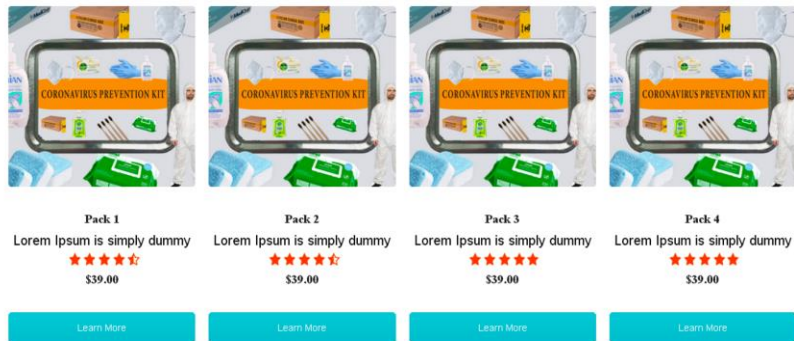
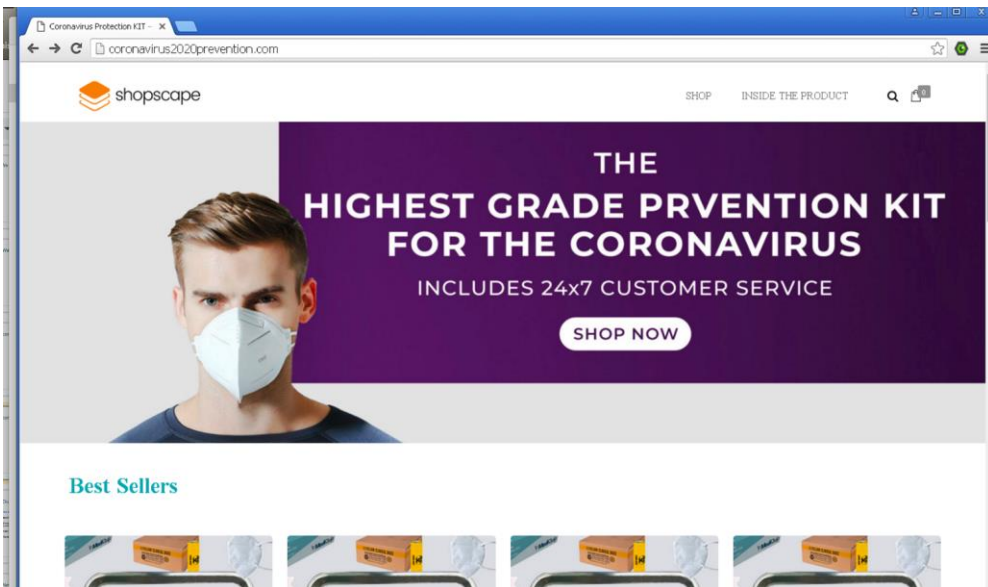
Tactics

- 'Information for COVID-19 in your area'
- 'Log in to read this important information'
- 'You have had contact with someone who has tested positive, download this form to seek medical care'
- 'We want to deposit money into your account'

- Covid-19 filename attachments
- Links in email body leading to 'important safety information' - malware droppers



Example: coronavirus2020prevention.com



coronavirus2020prevention.com

coronavirus2020prevention.com

INVESTIGATE

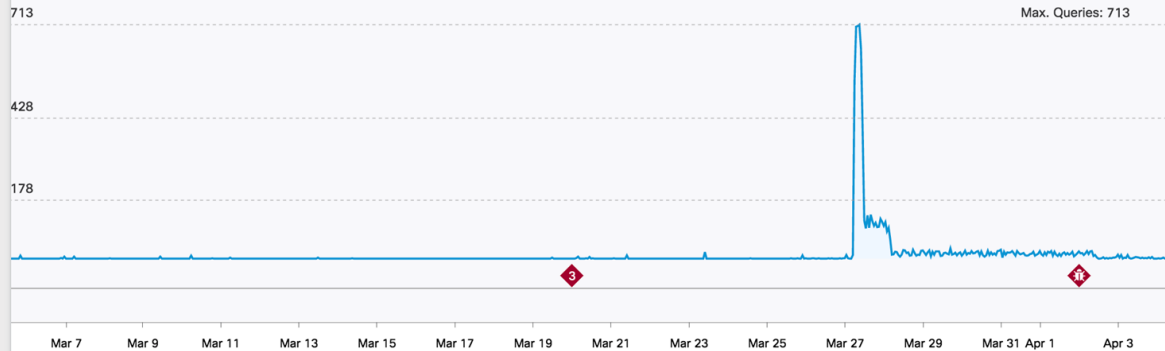
BACK TO TOP

Timeline

Current Content Category: None

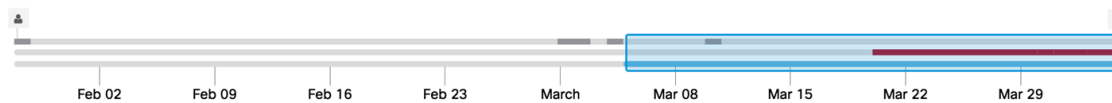
DNS Queries Domain Events DNS Changes

Mar 5th, 2020 - Apr 4th, 2020



Event History

Security Categories DNS Changes Query History



Our View of the Internet

200 Billion Internet requests per day

April 3rd, 2020

114,645 domains have been registered with the word 'corona' or covid' in the domain name

1,390 of the domains were **phishing** domains

74,568 of the domains were **malware** domains **65%**

