CYBER SECURITY LANDSCAPE IN THE ENERGY SECTOR

Sami Ruohonen | Tactical Defense Unit

F-Secure


TARGETED
RANSOMWARE
F-Secure

INFECTION FLOW

F-Secure

DELIVERY

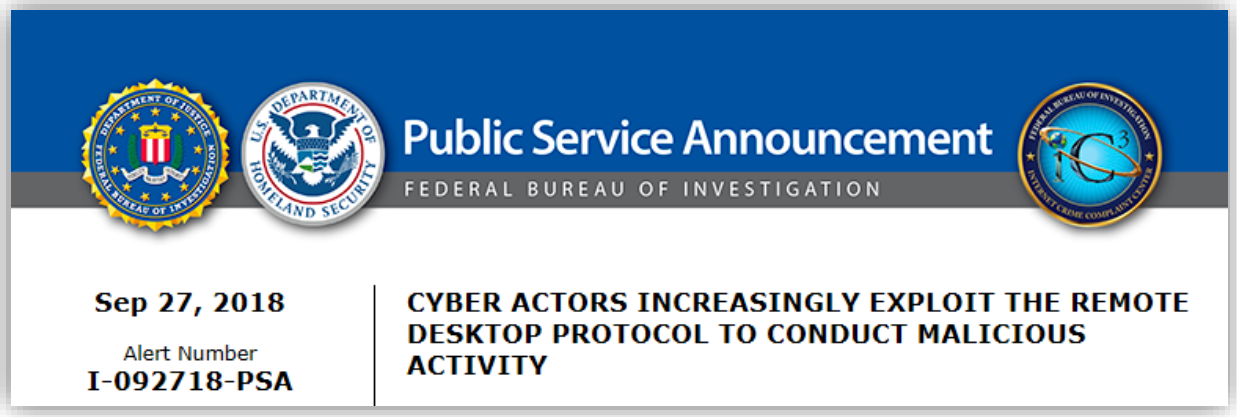
PHISHING

DRIVE-BY COMPROMISE

PUBLIC-FACING SERVICES

F-Secure

DELIVERY VIA RDP



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Sep 27, 2018

Alert Number
I-092718-PSA

CYBER ACTORS INCREASINGLY EXPLOIT THE REMOTE DESKTOP PROTOCOL TO CONDUCT MALICIOUS ACTIVITY

The US Department of Homeland Security released a public service announcement alerting of increasing RDP attacks.

Threats include mostly ransomware but RDP access can also be sold in the dark web.

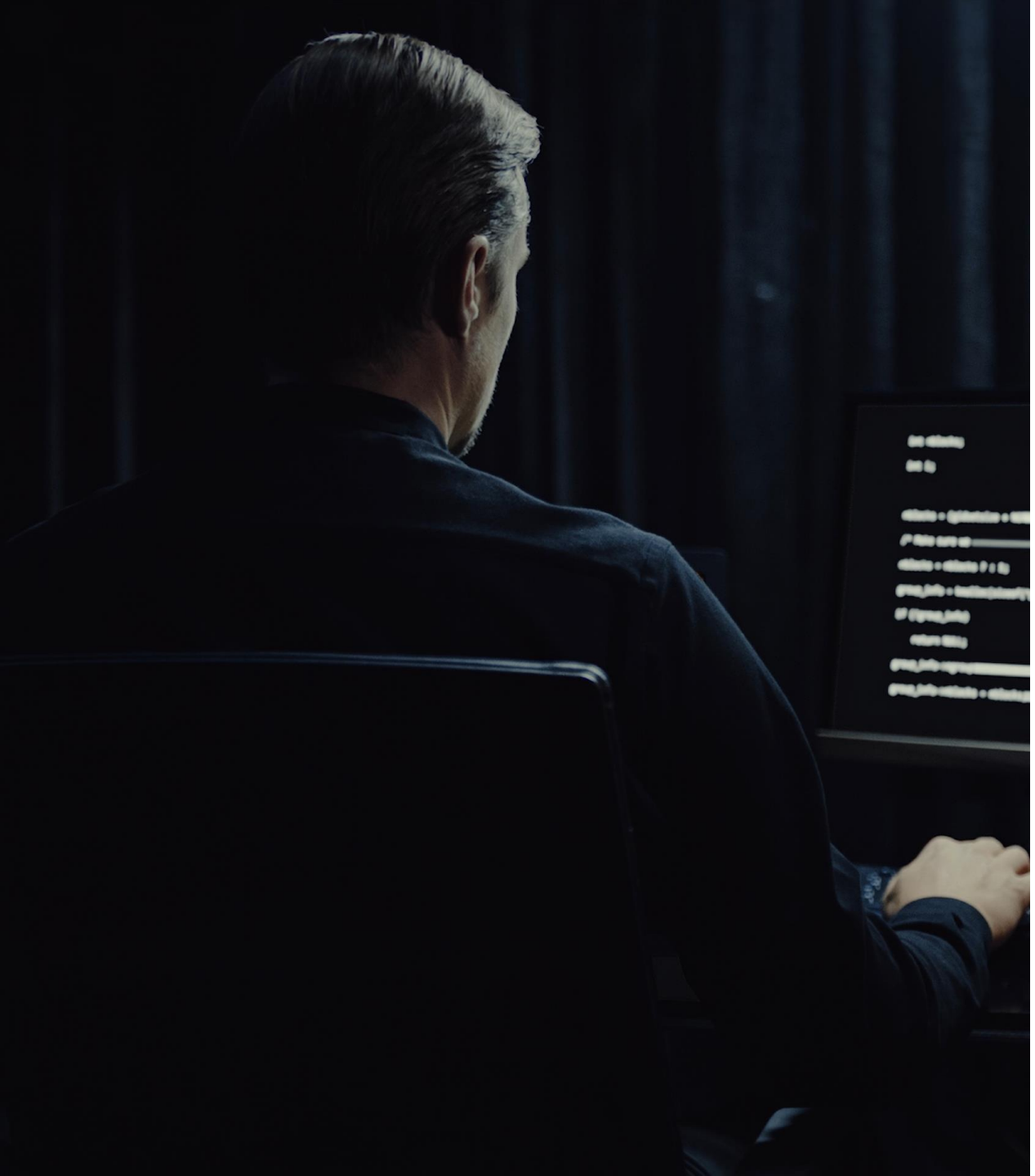
F-Secure

RANSOMWARE ATTACKS

"This [incident] will also affected our response time to logged calls as some of internal systems to dispatch and order material have been slowed by the impact," **the city said**.

F-Secure


CYBER
ESPIONAGE
F-Secure



ADVANCED PERSISTENT THREATS

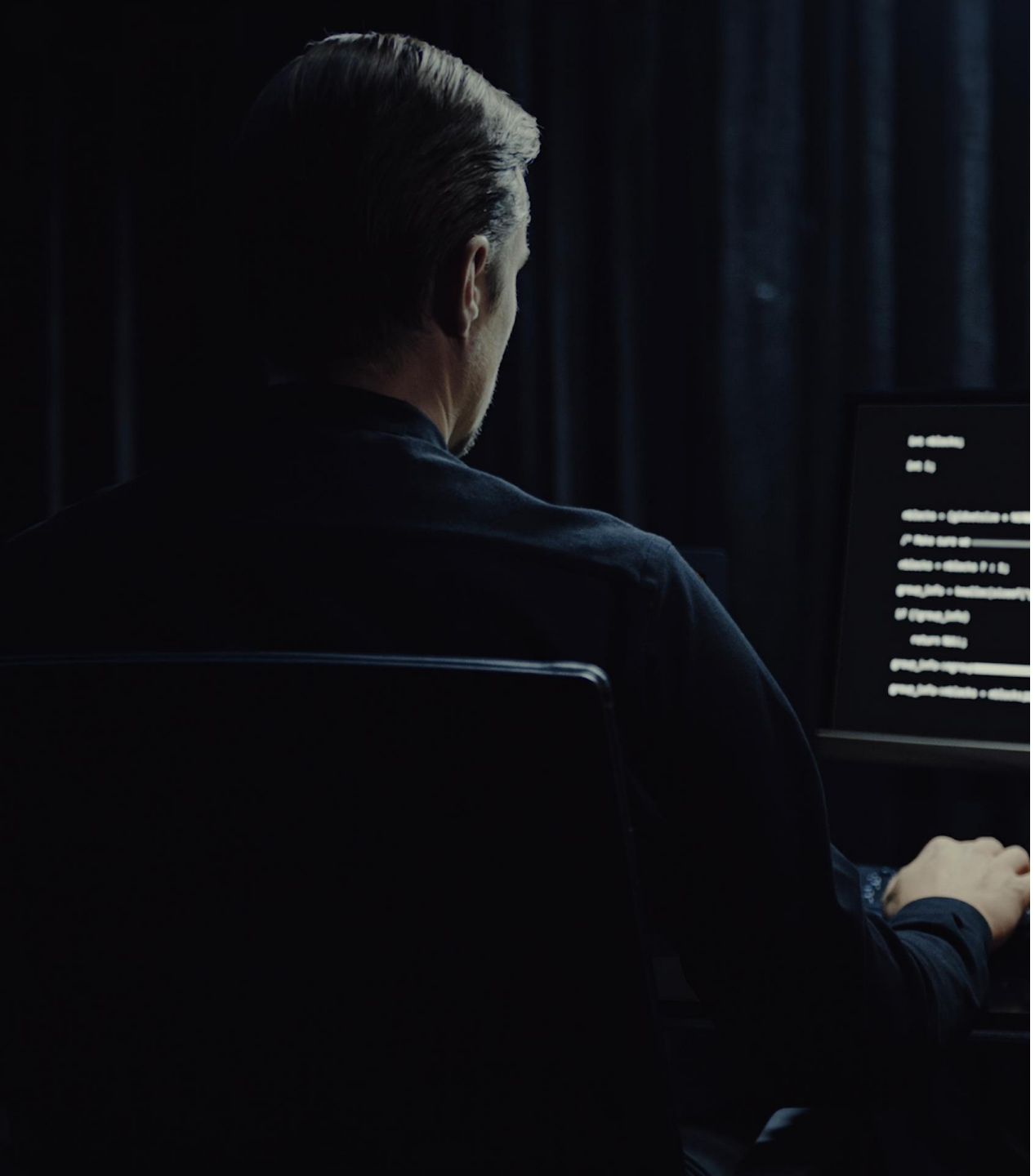
Subtle & Silent

Strong foothold

Defense evasive techniques

Non-invasive exfiltration

F-Secure



MOTIVES

APT10

- IP theft
- Espionage

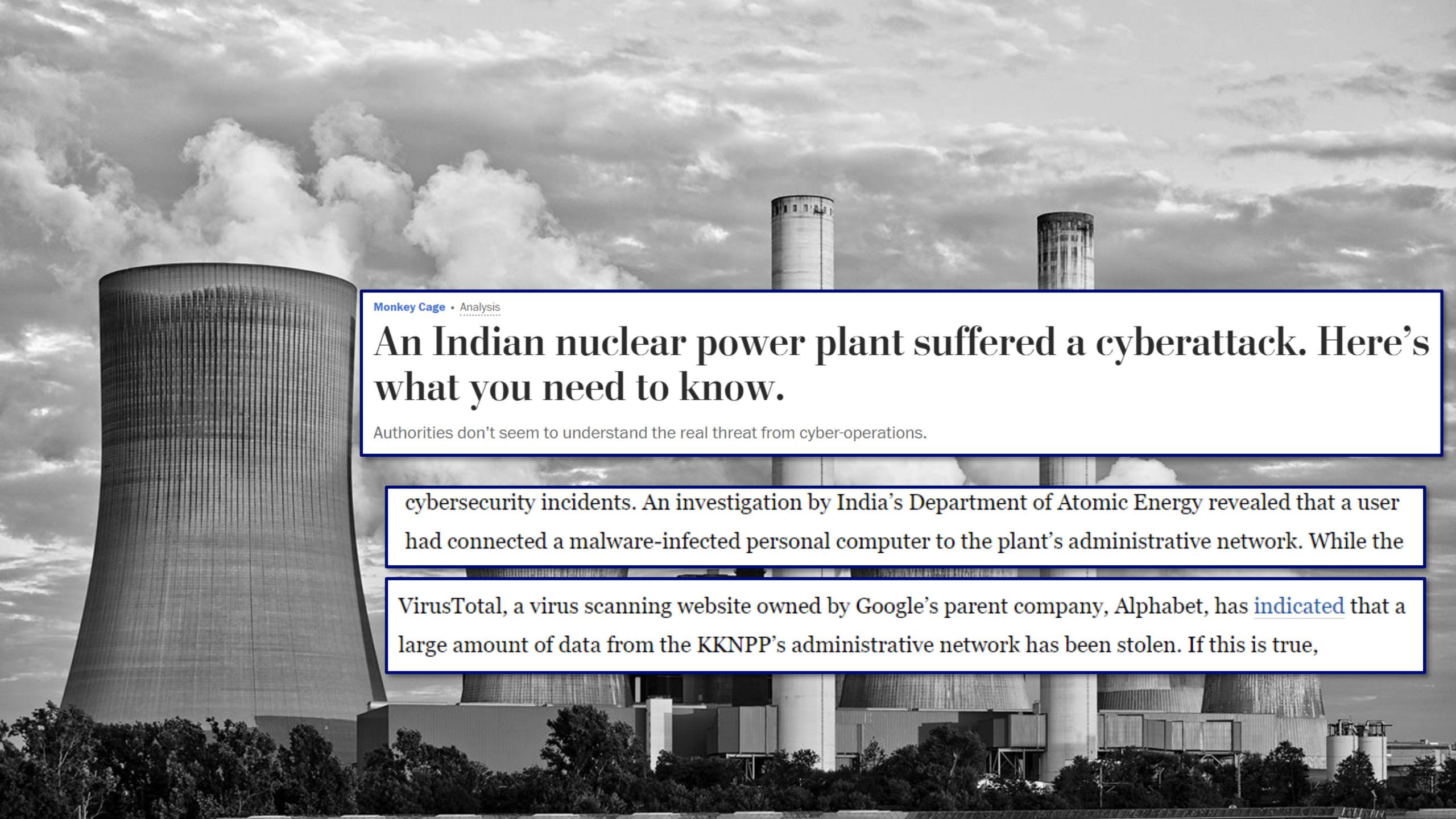
Lazarus (APT38)

- Financial gain
- Espionage

APT33

- Sabotage
- Espionage

F-Secure



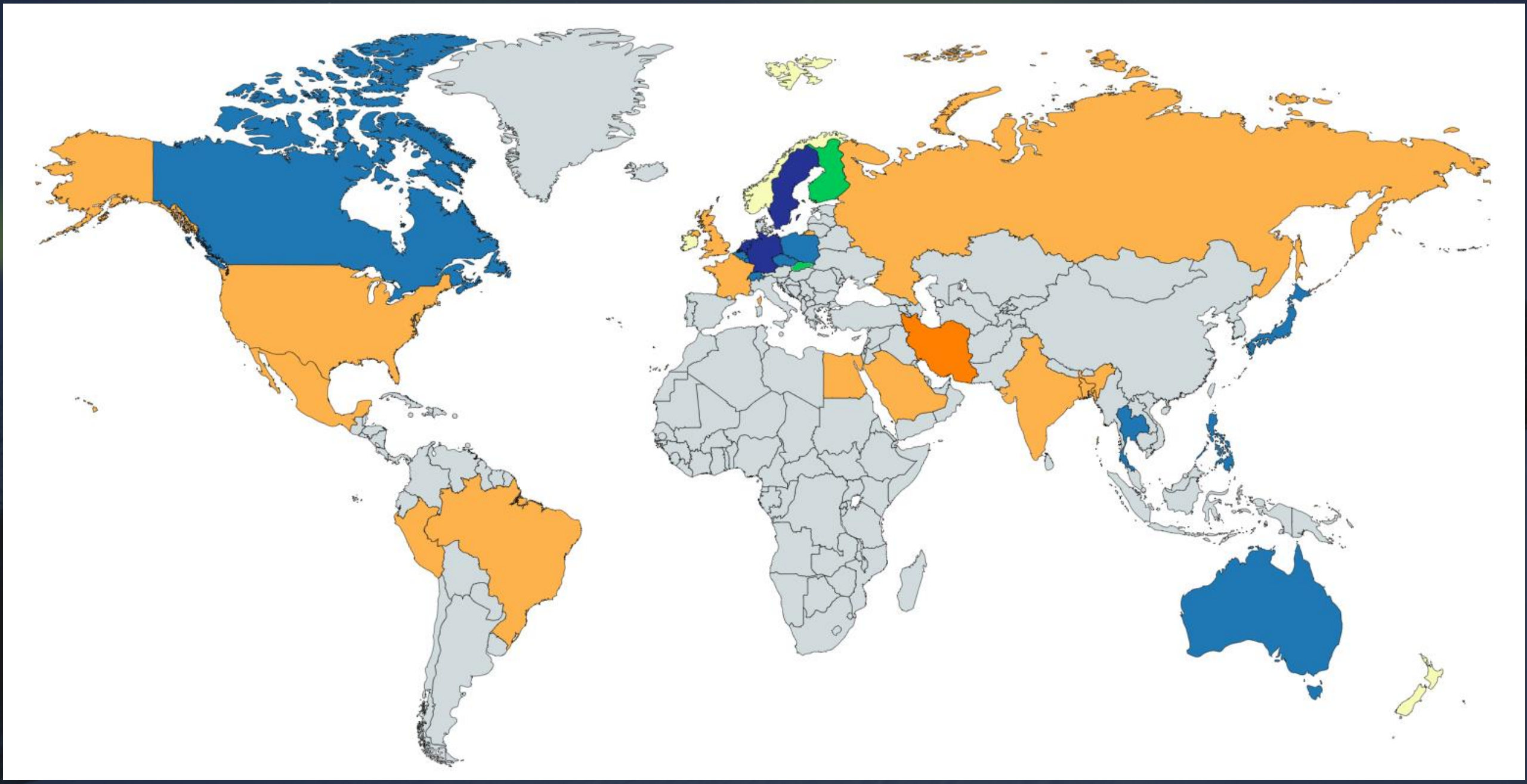
Monkey Cage • Analysis

An Indian nuclear power plant suffered a cyberattack. Here's what you need to know.

Authorities don't seem to understand the real threat from cyber-operations.

cybersecurity incidents. An investigation by India's Department of Atomic Energy revealed that a user had connected a malware-infected personal computer to the plant's administrative network. While the

VirusTotal, a virus scanning website owned by Google's parent company, Alphabet, has indicated that a large amount of data from the KKNPP's administrative network has been stolen. If this is true,




F-Secure®