



Are You Afraid
of the
Dark(web)?

THE TALE
OF THE
DIGITAL
DUPLICATE

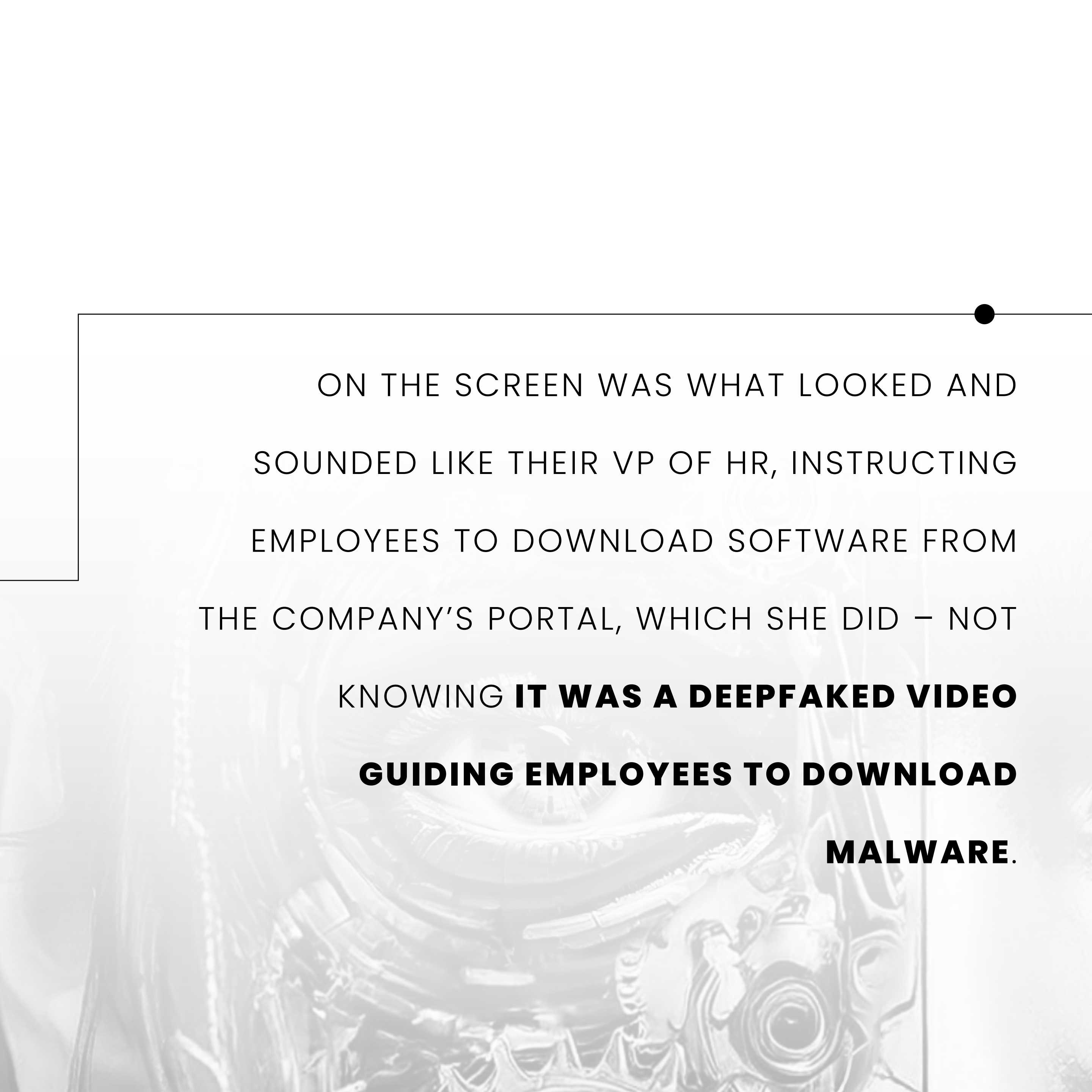


SpyCloud



A LONG-TERM EMPLOYEE RECEIVED
**WHAT SEEMED LIKE A LEGITIMATE
COMPANY EMAIL** INVITING HER TO A
ZOOM CALL FOR NEW PAYROLL
POLICIES. SHE JOINED THE MEETING
WITHOUT HESITATION.

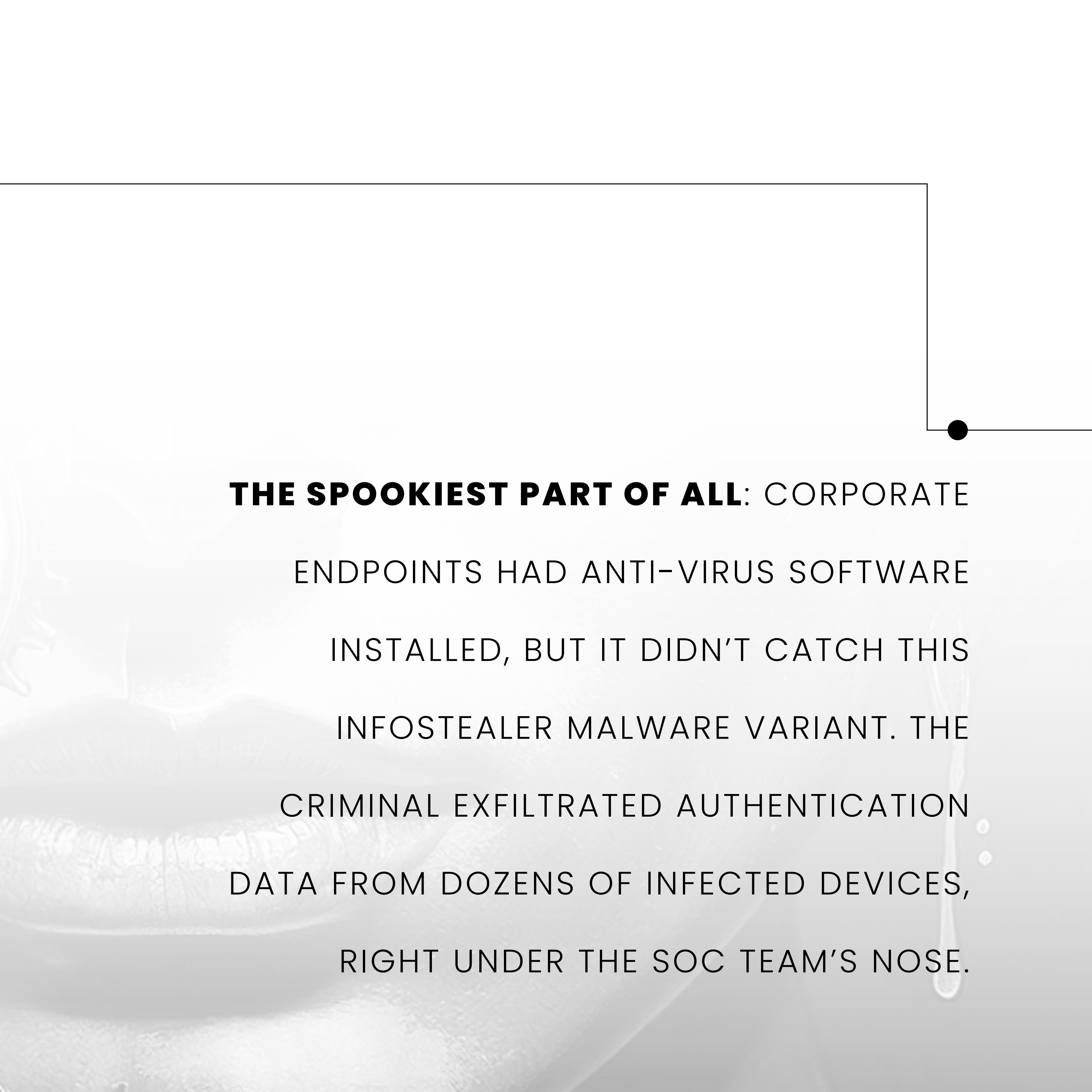




ON THE SCREEN WAS WHAT LOOKED AND
SOUNDED LIKE THEIR VP OF HR, INSTRUCTING
EMPLOYEES TO DOWNLOAD SOFTWARE FROM
THE COMPANY'S PORTAL, WHICH SHE DID – NOT
KNOWING **IT WAS A DEEPAKED VIDEO**
GUIDING EMPLOYEES TO DOWNLOAD
MALWARE.

●

LITTLE DID THE SOC TEAM KNOW – THE VP OF HR USED AN **INFECTED HOME DEVICE** TO LOG INTO WORK APPLICATIONS, AND THAT ACCESS WAS NOW BEING EXPLOITED BY A CLEVER CYBERCRIMINAL. THEY HIJACKED THE VP'S IDENTITY AND NAVIGATED ACROSS THEIR INTERNAL PORTAL – GRABBING PREVIOUS TOWNHALL VIDEO CONTENT TO FEED THEIR DEEPPFAKE CREATOR AND POSTING A NEW WIKI PAGE WITH A LINK TO DOWNLOAD THE MALICIOUS SOFTWARE.



THE SPOOKIEST PART OF ALL: CORPORATE
ENDPOINTS HAD ANTI-VIRUS SOFTWARE
INSTALLED, BUT IT DIDN'T CATCH THIS
INFOSTEALER MALWARE VARIANT. THE
CRIMINAL EXFILTRATED AUTHENTICATION
DATA FROM DOZENS OF INFECTED DEVICES,
RIGHT UNDER THE SOC TEAM'S NOSE.



●
THANKFULLY, WITHIN A DAY, **SPYCLOUD**

ALERTED THE TEAM TO THE DATA

STOLEN FROM THE INFECTED DEVICE –

INCLUDING BUSINESS-CRITICAL

APPLICATIONS HOUSING SENSITIVE

FINANCIAL DATA AND CUSTOMER

INFORMATION.

SPYCLOUD'S **SWIFT EXPOSURE DETECTION**

ALLOWED THE EXPOSED EMPLOYEES' CREDENTIALS TO BE RESET AND ACTIVE SESSIONS TO BE TERMINATED. AND

SPYCLOUD'S **IDLINK ANALYTICS POWERED**


A ROBUST ROOT-CAUSE INVESTIGATIVE

ANALYSIS, ENABLING THE SOC TEAM TO

VISUALIZE THE FULL EXTENT OF THE

DEEPPFAKED VP'S EXPOSURE, AND WORK

WITH THEM TO SECURE THEIR HOME DEVICE.



WITH CONTINUOUS MONITORING, REAL-TIME ALERTS FOR COMPROMISED IDENTITIES, AND INVESTIGATIONS CAPABILITIES FAR BEYOND THE NORM, **SPYCLOUD HELPS ORGANIZATIONS NAVIGATE THE NEWEST THREATS** INCLUDING BEC, DEEPFAKE DELIVERIES, AND INFOSTEALER MALWARE.





CHECK YOUR OWN DARKNET

EXPOSURE, INCLUDING MALWARE
EXFILTRATED PASSWORDS AND MORE.

LEARN MORE ▶

Are You Afraid
of the
Dark(web)?

SpyCloud