# ANATOMY OF AN (EMAIL) ACCOUNT TAKEOVER ATTACK

PHASE 1



## STAGE 1

## TARGET ACQUISITION

- O DIRECT
- O ONLINE RESEARCH
- O SUPPLY CHAIN ANALYSIS
- **O WHOIS**

the organisations they want to infiltrate. Researching which organisations would make a good target, looking to many online sources, even social media, to ascertain who's who, understand relationships between organisations and the individuals within. Whois data can be used to understand domain-related information like email format.

The starting point for any attack is identifying

STAGE 2

- **O INTERNET**
- O SOCIAL MEDIA
- O DARK WEB O DIRECTORY HARVESTING ATTACKS
- The attacker begins to build a target list of

ACCOUNT HARVESTING

valued targets like senior executives, finance teams or privileged users.

specific individuals or groups, often high



## STAGE 3 GAINING ACCESS

### O OBTAIN CREDENTIALS THROUGH PHISHING, CRACKING, BRUTE FORCE,

- BREACH DATA, SOCIAL ENGINEERING O ENTRY - TYPICALLY VIA **OUTLOOK WEB ACCESS (OWA)**
- Once the target organisations and target accounts have been identified the next

step is to obtain the credentials or passwords required to gain access to the accounts. There are many approaches to this, including phishing, which can be multi-channel and highly complex, using copycat emails and fake login pages to steal credentials.

**RESEARCH SHOWS** BUSINESS EMAIL COMPROMISE ATTACKS TARGETED AT FINANCE TEAMS ARE UP A STAGGERING

WITH **HIGHER VOLUME** CAMPAIGNS ALSO TAKING ROOT AS EFFORTS TO **COMPROMISE OVER** RECIPIENTS AT ONCE INCREASED BY MORE THAN A QUARTER (SOURCE ABNORMAL SECURITY BEC REPORT Q12020)

**BUSINESS EMAIL COMPROMISE** ATTACKS ACCOUNTED FOR 50 CRIME LOSSES 2019 (!) **33** LOSSES FROM CORPORATE **DATA BREACHES AVERAGE LOSS** 575 (

(SOURCE FBI INTERNET CRIME REPORT 2019)



## ORGANISATIONAL RECON

SIAGE 4

#### O IDENTIFY KEY DEPARTMENTS AND INDIVIDUALS Once inside the account, the attacker will use

- O MAP RELATIONSHIPS (INTERNAL / EXTERNAL)
- EVALUATE TRUST O UNDERSTAND PROCESSES
- PHASE 2

AND SIGN-OFF LEVELS

sign off payments. This informs the attacker about communication style, processes and policy so the attack will be more likely to fly under the radar.

email history, inbox and sent items to map the

departments and people of interest, learning the

chain of command and who has the authority to

organisation internally, identifying key

STAGE 5 MAILBOX RE-CONFIGURATION



### O CAREFULLY NAMED FOLDER **CREATION**

## O INBOX RULES TO RE-ROUTE MESSAGES (TO NEW FOLDERS)

within email services, designed to help users organise

and streamline their activity, to subtly syphon messages

away from the intended recipient. Keywords in content

or subject line or sender ID can be used to identify

conversations of interest to the hacker.

The attacker takes advantages of the standard tools

O KEYWORD RULES

CONVERSATION HIJACKING

O MONITOR MESSAGES AND FOLDERS

O HIJACK CONVERSATIONS

O INSERT FALSE INVOICES

**COMPANIES WORLDWIDE** 

ESTIMATED WILL COST

**ACCOUNT TAKEOVER** 

SECURITY TEAMS WHICH

**JUNIPER RESEARCH** HAS

IS A THORN IN THE

SIDE OF ENTERPRISE

**\$25BN** 

Now the attacker is poised to pose as

the account owner, mimicking their

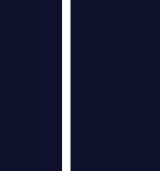
conversations with colleagues and

suppliers to fool them into making

false payments or exposing IP - while

the account owner is none the wiser.

style and slipping into email



# **O DIVERT PAYMENTS**

STAGE 7

**OF INTEREST** 

STAGE 6

ONWARDLY TARGET EXTERNALLY FACING APPS (ONEDRIVE, SHARE POINT ETC.)

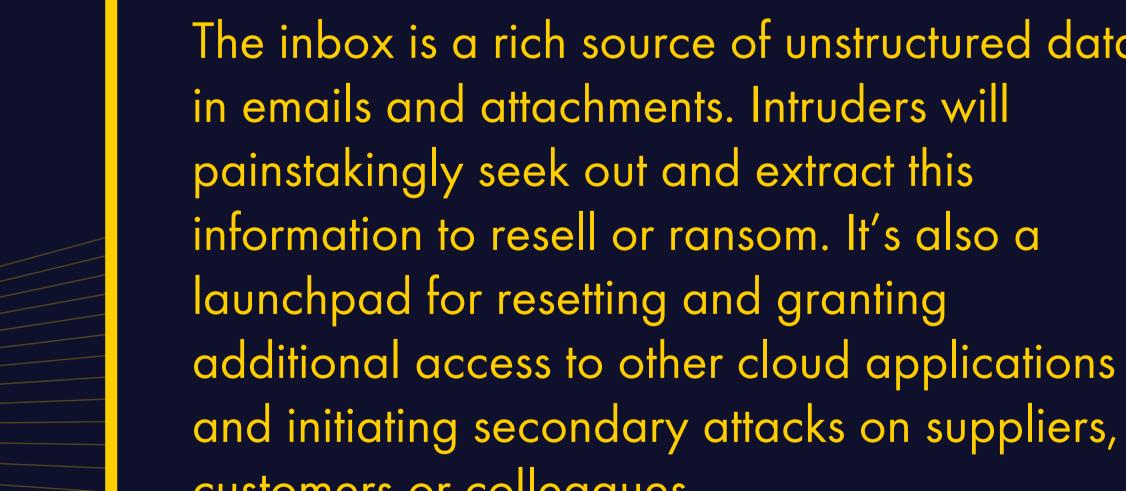
DATA EXFILTRATION

AND ATTACHMENTS

O IDENTIFY UPSTREAM /

The inbox is a rich source of unstructured data

customers or colleagues.





## STAGE 8 CLEAN UP O DELETE MESSAGES O REMOVE RULES AND FOLDERS

- CREATE BACKDOORS - E.G. ROGUE USER ACCOUNTS\*
- Attackers clean up their tracks and pack up their toolkit before making an understated departure, often with their next attack in mind.

**UNSTRUCTURED DATA** • EXTRACT DATA IN EMAIL HISTORY INCLUDES DATA IN FILES SUCH AS WORD DOCUMENTS **EXCEL SPREAD SHEETS PRESENTATIONS DOWNSTREAM TARGETS** WEBPAGES



AND AS MUCH AS **OF BUSINESS DATA** IS STORED

80-90%

OF THE DATA IN ANY

ORGANIZATION IS

**UNSTRUCTURED** 

**EMAIL MESSAGES** 

NO EVIDENCE

OBSERVED IN THE WILD TO DATE

SECURINGS

If you would like to stop Account Takeover impacting your business, start a conversation with us about how we can help with adaptive multi-factor authentication (MFA), part of our consolidated cloud security platform, and Securing 365.