censornet.

ANATOMY OF AN (EMAIL) ACCOUNT TAKEOVER ATTACK

PHASE 1

STAGE 1
TARGET ACQUISITION

- DIRECT
- ONLINE RESEARCH
- SUPPLY CHAIN ANALYSIS
- WHOIS

The starting point for any attack is identifying 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.

STAGE 2
ACCOUNT HARVESTING

- INTERNET
- SOCIAL MEDIA
- DARK WEB
- DIRECTORY HARVESTING ATTACKS

The attacker begins to build a target list of specific individuals or groups, often high valued targets like senior executives, finance teams or privileged users.

RESEARCH SHOWS BUSINESS EMAIL COMPROMISE ATTACKS TARGETED **AT FINANCE TEAMS** ARE UP A STAGGERING **87%**

WITH **HIGHER VOLUME** CAMPAIGNS ALSO TAKING ROOT AS EFFORTS TO **COMPROMISE OVER 10 RECIPIENTS** AT ONCE INCREASED BY MORE THAN A QUARTER

(SOURCE ABNORMAL SECURITY BEC REPORT Q12020)

STAGE 3
GAINING ACCESS

- OBTAIN CREDENTIALS THROUGH **PHISHING, CRACKING, BRUTE FORCE, BREACH DATA, SOCIAL ENGINEERING**
- 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.

BUSINESS EMAIL COMPROMISE ATTACKS ACCOUNTED FOR **50%** OF CYBER CRIME LOSSES IN 2019

33X LOSSES FROM CORPORATE DATA BREACHES

AVERAGE LOSS

$75K

(SOURCE FBI INTERNET CRIME REPORT 2019)

STAGE 4
ORGANISATIONAL RECON

- IDENTIFY KEY DEPARTMENTS AND INDIVIDUALS
- MAP RELATIONSHIPS (INTERNAL / EXTERNAL)
- EVALUATE TRUST
- UNDERSTAND PROCESSES AND SIGN-OFF LEVELS

Once inside the account, the attacker will use email history, inbox and sent items to map the organisation internally, identifying key departments and people of interest, learning the chain of command and who has the authority to 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.

PHASE 2

STAGE 5
MAILBOX RE-CONFIGURATION

- CAREFULLY NAMED FOLDER CREATION
- INBOX RULES TO RE-ROUTE MESSAGES (TO NEW FOLDERS)
- KEYWORD RULES

The attacker takes advantages of the standard tools 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.

ACCOUNT TAKEOVER IS A THORN IN THE SIDE OF ENTERPRISE SECURITY TEAMS WHICH **JUNIPER RESEARCH** HAS ESTIMATED WILL COST **COMPANIES WORLDWIDE**

$25BN IN **2020**

STAGE 6
CONVERSATION HIJACKING

- MONITOR MESSAGES AND FOLDERS
- HIJACK CONVERSATIONS OF INTEREST
- INSERT FALSE INVOICES
- DIVERT PAYMENTS

Now the attacker is poised to pose as the account owner, mimicking their style and slipping into email conversations with colleagues and suppliers to fool them into making false payments or exposing IP – while the account owner is none the wiser.

STAGE 7
DATA EXFILTRATION

- EXTRACT DATA IN EMAIL HISTORY AND ATTACHMENTS
- ONWARDLY TARGET EXTERNALLY FACING APPS (ONEDRIVE, SHARE POINT ETC.)
- IDENTIFY UPSTREAM / DOWNSTREAM TARGETS

The inbox is a rich source of unstructured data in emails and attachments. Intruders will painstakingly seek out and extract this information to resell or ransom. It's also a launchpad for resetting and granting additional access to other cloud applications and initiating secondary attacks on suppliers, customers or colleagues.

UNSTRUCTURED DATA INCLUDES DATA IN FILES SUCH AS

WORD DOCUMENTS

EXCEL SPREAD SHEETS

PRESENTATIONS

PDF

WEBPAGES

EMAIL MESSAGES

80 - 90% OF THE DATA IN ANY ORGANIZATION IS **UNSTRUCTURED**

AND AS MUCH AS 60% OF **BUSINESS DATA** IS STORED IN **EMAIL** – AND MUCH OF IT **EXCLUSIVELY**

(SOURCE IDC)

STAGE 8
CLEAN UP

- DELETE MESSAGES
- 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.

*NO EVIDENCE OBSERVED IN THE WILD TO DATE

SECURING 365

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**.

DISCOVER MORE AT **CENSORNET.COM**