30% USING 365

ANATOMY

ACTORS GANING ACCESS TO LEGITIMATE A/C

BRUTE FORCE ATTACKS. → VOLUME BASED APPROACH. KNOWN PASSWORD LISTS.

PAYING INVOICE TO 3RD PARTIES. → PHISHING EMAILS

SPOOFED LOGIN PAGES. USING RANDOM STRINGS TO INCLUDE COMPANIES.

MOTIVATION → PROBABLY MONEY/FINANCIAL BUT ALSO PERSONAL INFO.

- INITIAL COMPROMISE
- MANNER. → ACCESS TO EMAIL/AC THEN ONWARD TO OTHERS.

PHISHING EMAIL - REPORTED

CHECK HEADERS IS THE EMAIL SPOOFED?

COLLECT EVIDENCE - AUDIT LOGS IN 365

ADMIN. TOOLS

COMPLIANCE PORTAL

AUDIT LOGS. (90 DAYS) → TIME BOUND. METADATA FOR TENANCY

DOWNLOAD FOR INTERROGATION. CSV. FORMAT. (ANALYSED BY TOOLS).

FILTER BY USER A/C.

FINE TUNING ANALYSIS

MONITORING AND ACTING ON LOGS. → API SET UP ALERTS? SIEM?

LOGS CONTAIN IP ADDRESS → SEARCH FOR THE POINT WHERE IP ADDRESS CHANGES
TO IDENTIFY ANOMYLOUS EVENT.

IMPACT & EXTENT OF COMPROMISE → ANALYSIS FROM LOG.
→ TRIGGER ACTIVITIES E.G. FORWARD RULES.

PINPOINT DATE & TIME OF COMPROMISE AND THE MECHANISM

ESTABLISHING TIMELINE.

→ REMOVE SIMILAR PHISHING EMAIL.

ESTABLISH WHAT THE MALICIOUS ACTOR HAS DONE WITH THE COMPROMISED ACCESS.

FOLDERS & DOCUMENTS CREATED

ESTABLISH RELATED MALICIOUS ACTIVITIES.

- ACTORS OFTEN REPEAT ACTIONS.

FIRST ACTION: DISABLE ACCOUNT!

→ INVALIDATE TOKENS/SESSIONS.

ASSESSMENT OF ACTIVITY/LOSS - BUILD. EVIDENCE BASE.