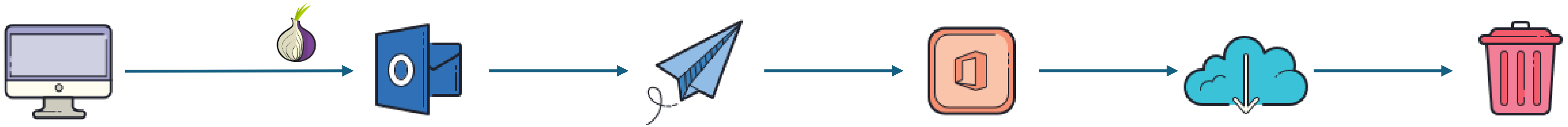
KJ Ninja, 2024/3

Cloud base ID to Exfiltration attack

T1110 Brute Force, T1621 Multi-Factor Authentication Request Generation,
T1114 Email Collection, TA0010 Exfiltration



Repeated MFA prompt (MFA fatigues) → Login Outlook with Tor → Creation of Inbox rule → Access SharePoint → Mass Download Files → Mass Delete Files

Simulation

1. Access Outlook by Tor browser
   - 15 times failed attempts (within 5 min)
   - Successfully login to Outlook

2. Create forwarding rules

e.g.
- DEV05A (New-InboxRule)
- DEV05B (New-InboxRule)
- DEV05C (New-InboxRule)

3. Access SharePoint

e.g. 40 files access

4. Donwload files

e.g. 40 files

5. Delete files

e.g. 40 files

Alerts in XDR

1. Multiple failed login attempts

(1. Multiple Failed Sign-Ins)

2. Suspicious behavior: Multiple failed login attempts

3. Activity from a Tor IP address
4. Logon from a risky IP address
5. Anonymous IP address
6. ***Suspicious behavior: Impossible travel activity***

7. Suspicious inbox forwarding rule
8. Activity from a Tor IP address

MDA: Learning period (7 days)

9. Suspicious file access activity (by user)

10. Unusual file download (by user)

11. Activity from a Tor IP address

12. Suspicious massive data read

13. Unusual file deletion activity (by user)