БИТВА ЗА ДОМЕН

Microsoft

SecOps and Incident Response with Azure Advanced Threat Protection

Дмитрий Узлов
Компания «ТЕХНОПОЛИС»

THE DAILY NEWS

Attack shuts down [redacted] organization for 2 days

Investigation determined that threat actor was present on network for over 5 months.

Data sources indicate dozens of other institutions may be similarly impacted.

Wrecking ball malware was used to distract victim and response teams from main attack.

Attack timeline

1

Day 1:
Attackers successfully target Patient Zero with backdoor malware

LATERAL MOVEMENT

2

Day 84 – 129:
Moves laterally through network; **obtains privileged credentials** and accesses sensitive systems.

EXFILTRATE DATA

3

Day 134:
Threat actor executes fraudulent transfers of funds.

DOMAIN DOMINANCE

5

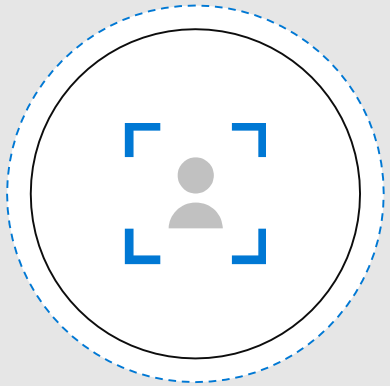
Day 135:
Uses **remote code execution** from a local machine to **domain controller**, gaining domain admin accounts

DENIAL OF ACCESS

4

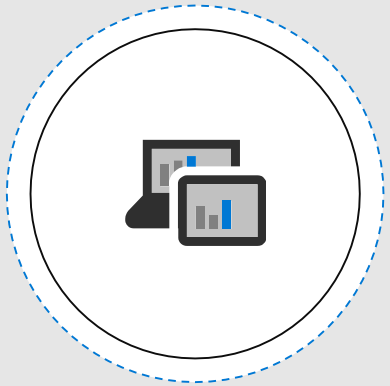
Day 135:
After customer detects fraudulent transactions, wrecking ball malware is delivered.
Operations are brought to a halt!

Microsoft Threat Protection



Identities

Users and Admins

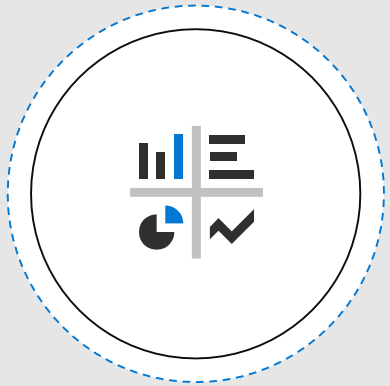


Endpoints

Devices and Sensors

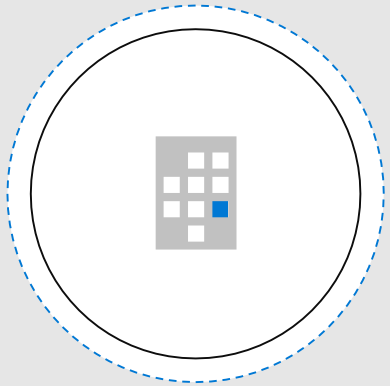
User Data

Email messages and documents



Cloud Apps

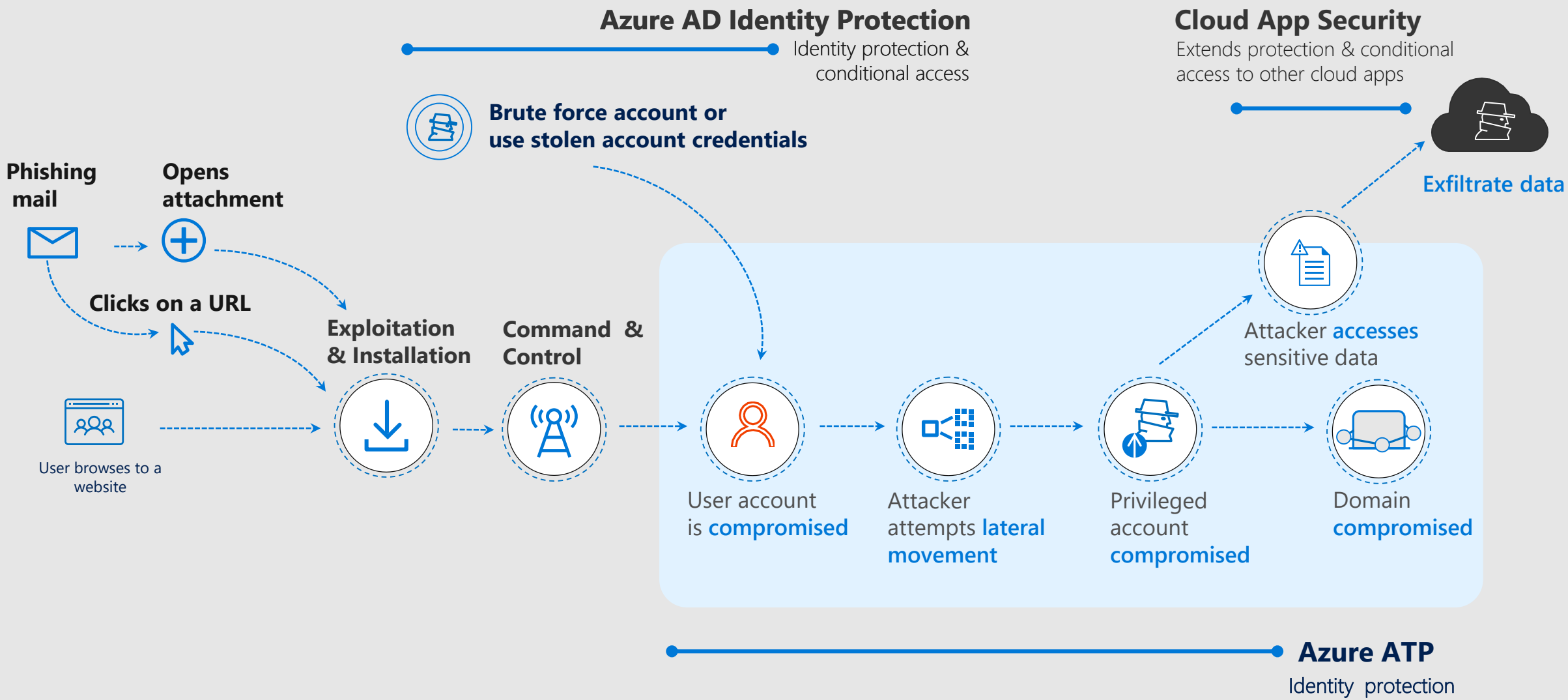
SaaS Applications and Data Stores

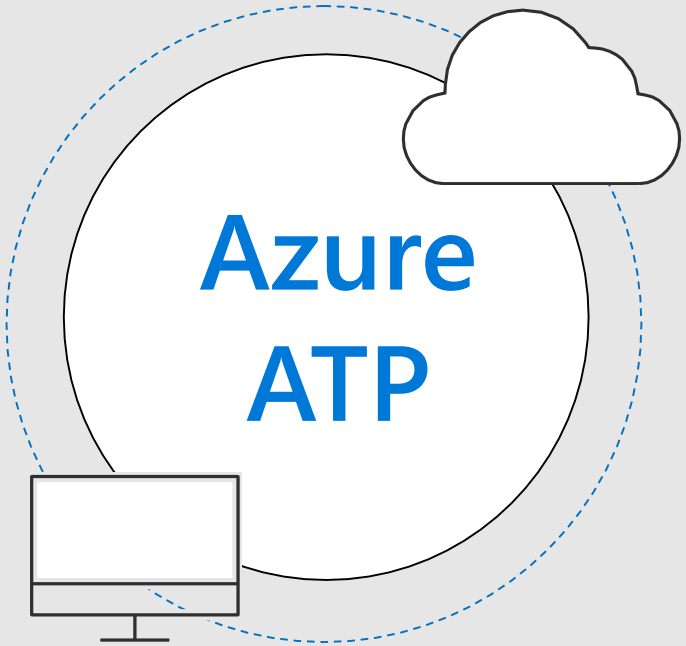


Infrastructure

Servers, Virtual Machines, Databases, Networks

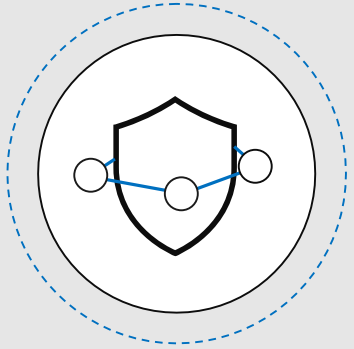
Maximize Detection During Attack Stages





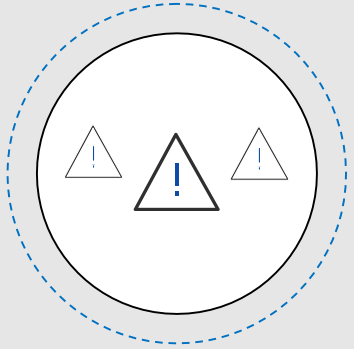
Detect and investigate advanced attacks, compromised identities, and insider threats

Azure Advanced Threat Protection

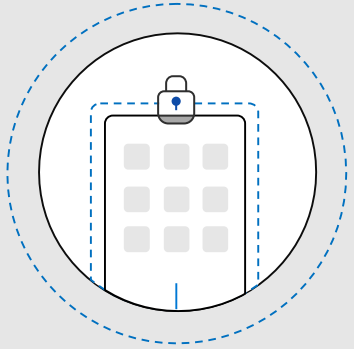


Detect threats fast with Behavioral Analytics

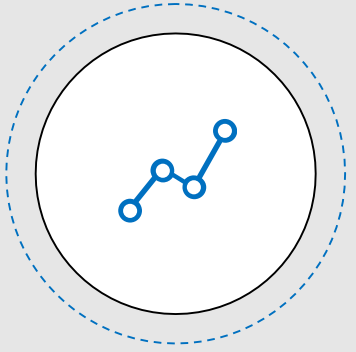
Focus on what is important using attack timeline



Reduce the fatigue of false positives

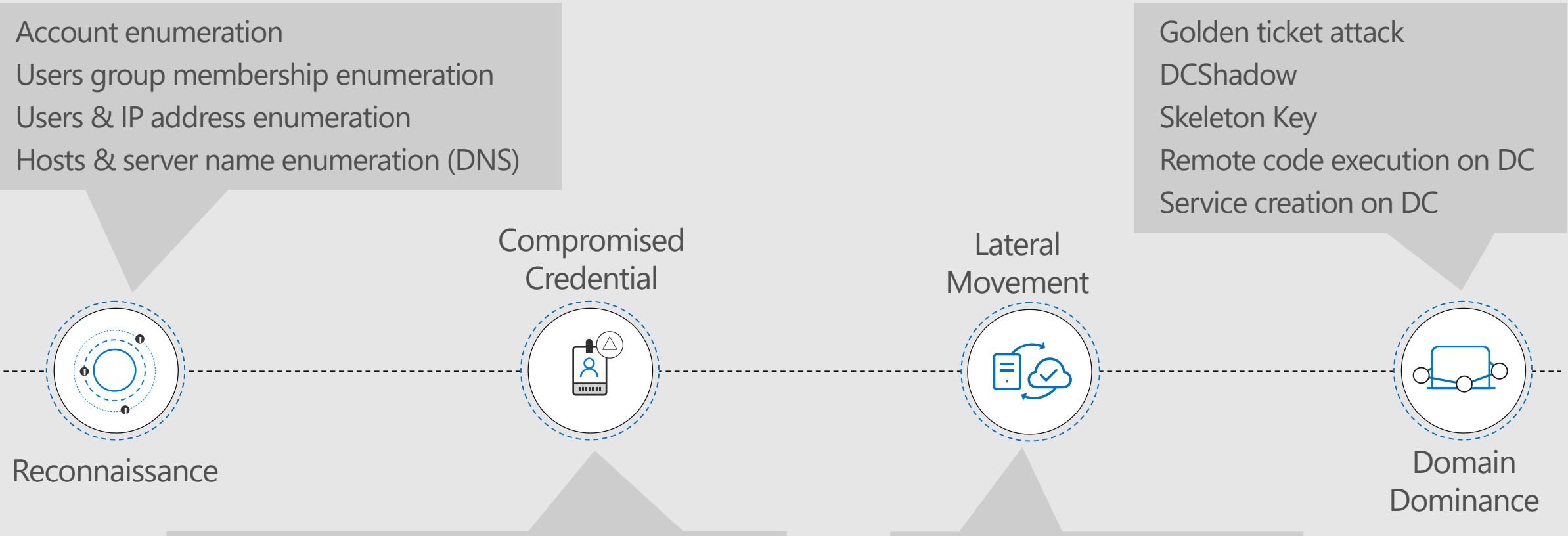


Protect at scale with the power of the cloud



Best-in-class security powered by the Intelligent Security Graph

Detect advanced attacks throughout the kill chain



How Azure ATP works