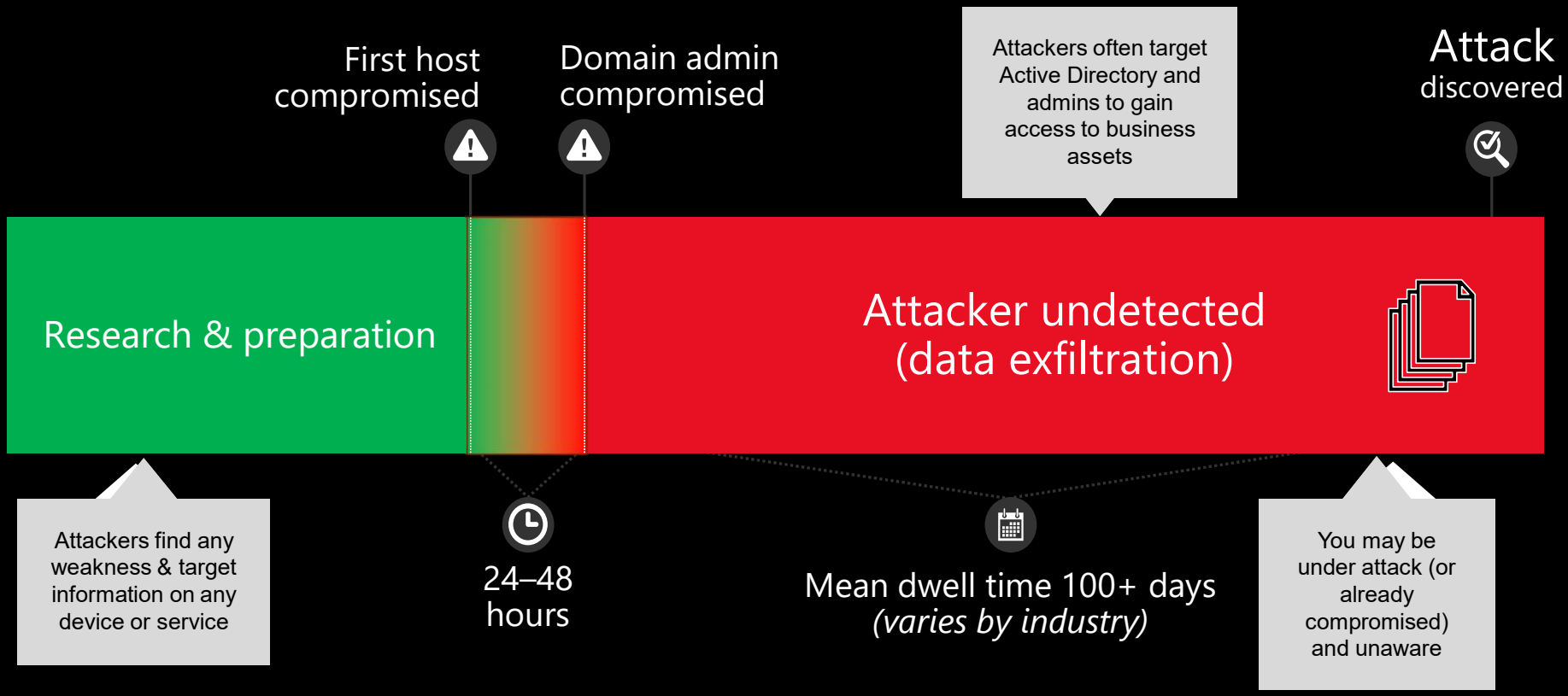
TRUESEC
EVENT

INFRASTRUCTURE SUMMIT 2019

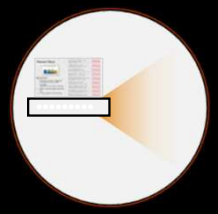
Protect your users with the help of Microsoft 365

Fabio Viggiani Hasain Alshakarti Markus Lassfolk

Attack timeline

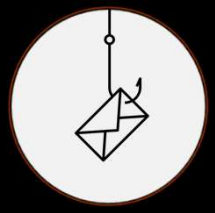


Top 3 Attacks Targeting Users



Password Spray

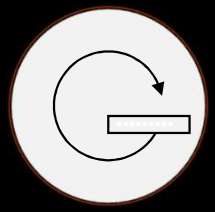
200,000 accounts compromised in Aug 2018
(Primarily via legacy AuthN protocols)



Phishing

5B emails blocked in 2018

44M risk events in Aug 2018



Breach Replay

650,000 accounts with leaked credentials in 2018

Identity - Critical Best Practices

Protecting Privileged Accounts

Password Policies / Password-less / Implement MFA

Block Legacy Authentication / Conditional Access Policies

Synchronize Password Hashes -> Azure Identity Protection

On-prem/Cloud - Critical Best Practices

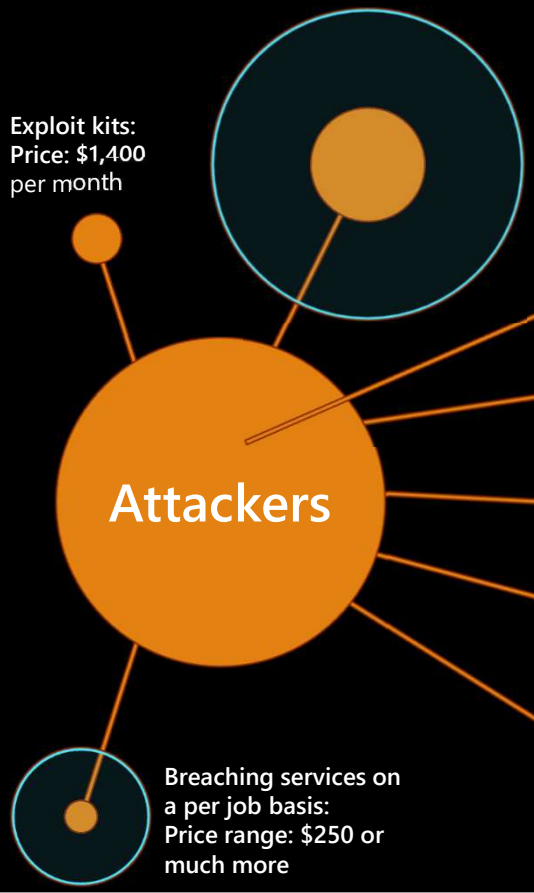
System Hardening / Patching
- Especially Internet Facing
- Attack Surface Reduction
- Policy Compliance & Enforcement

Extended Auditing
- Systems, Firewalls, Office 365, Proxy, Azure, Clients

Centralized logging
- Retention policy

Visibility & Detection Capabilities
- EDR: Defender ATP, Carbon Black, etc
- 24x7 Monitoring (SOC)

Attack services are cheap



Exploit kits:
Price: $1,400
per month

Zero-days:
Price: $5,000 to $350,000

Ransomware:
Price: $66 upfront or
30% of the profit
(affiliate model)

Loads (compromised device):
Price: PC - $0.13 to $0.89
Mobile - $0.82 to $2.78

Spearphishing services:
Price: $100 to $1,000 per
successful account take over

Compromised accounts:
Price: $150 for 400M
Averages $0.97 per 1,000

Denial of Service:
Price: $766.67 per month

Breaching services on
a per job basis:
Price range: $250 or
much more

FOCUS ON HYGIENE, DETECTION & VISIBILITY

Exploit mitigation

Business continuity / disaster recovery (bc/dr)

Lateral traversal / securing privileged access

Attack surface reduction

FOCUS ON MFA/PASSWORDLESS & ZERO TRUST

Mitigation of Identity attacks like phishing and cred theft

Increase cost of these attacks starting with administrative privileges and other business critical assets

ENABLE DDoS PROTECTION FOR CRITICAL SERVICES

Ensure that your business-critical services have DDoS protection from Azure platform or a capable 3rd parties

AZURE SENTINEL

Collect

Microsoft Services

Apps, users, infrastructure

Public Clouds

Security solutions

Analyze & detect threats

Machine learning, UEBA

Investigate & hunt suspicious activities

Interactive Attack Visualization, Azure Notebooks

Automate & orchestrate response

Playbooks

Enrichment with Intelligence (Geo location, IP Reputation)

Data Ingestion

Data Repository

Data Search

Azure Monitor (log analytics)

specialists

Integrate

ServiceNow

Other tools

Community