RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **TECH-W09**

M365 Threat Hunting—How to Understand Attacker's TTPs in Your Tenant

Aaron Turner

VP – SSPM
Vectra AI
https://Vectra.ai

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

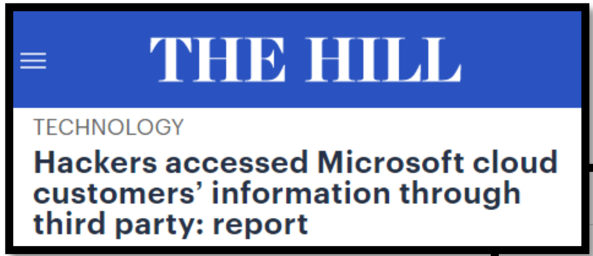
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Agenda

- Understanding M365 Attack Trends
- Common M365 Attack Paths
- Key M365 Threat Hunting Capabilities
- Sample Threat Hunting Scenarios
- M365 Threat Hunting Action Plan

Attackers Targeting Microsoft SaaS Platforms

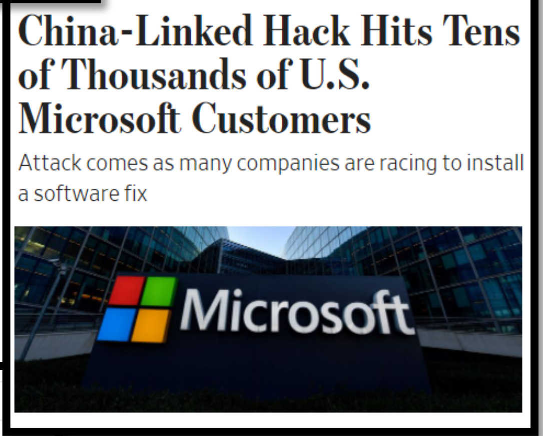
- Azure Active Directory and associated applications facilitated access to the most sensitive information and facilitate critical business operations
- Over the last 2 years, Azure Active Directory and Exchange Online have been the means by which over 100,000 organizations have been compromised around the world
- The efficiency of these attacks has depended upon weak default configurations and the oversights/errors of organizations' M365 administrators



THE HILL

TECHNOLOGY

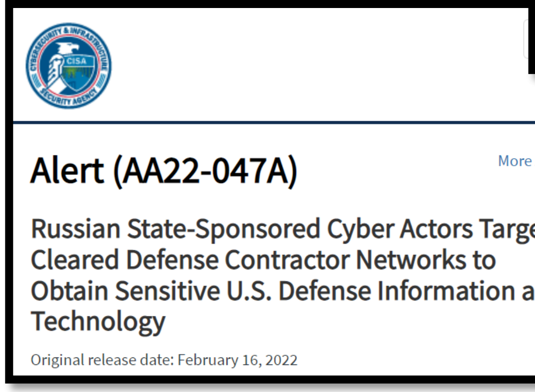
Hackers accessed Microsoft cloud customers' information through third party: report



WSJ

China-Linked Hack Hits Tens of Thousands of U.S. Microsoft Customers

Attack comes as many companies are racing to install a software fix



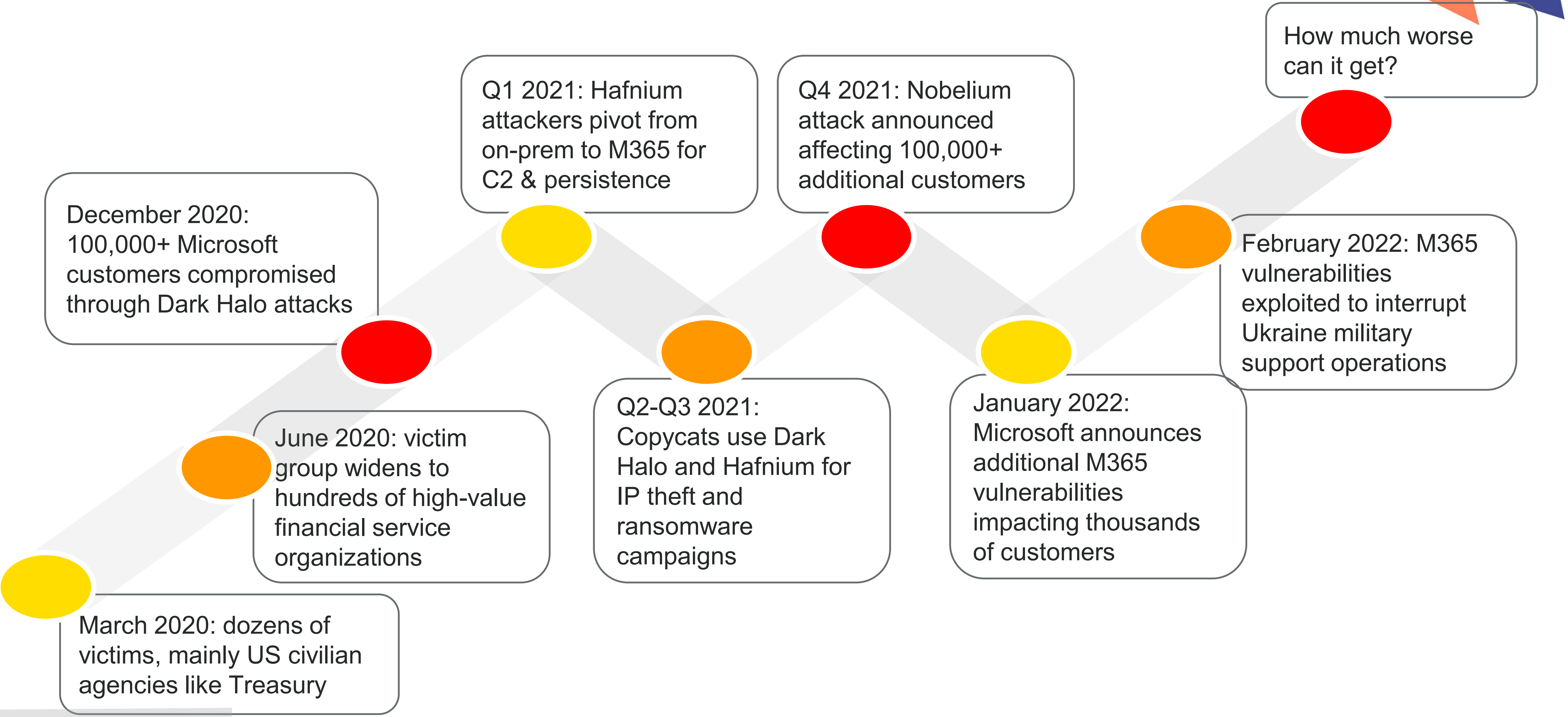
Alert (AA22-047A)

More Alerts

Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology

Original release date: February 16, 2022

Increasing Velocity and Efficiency of M365 Attacks



March 2020: dozens of victims, mainly US civilian agencies like Treasury

June 2020: victim group widens to hundreds of high-value financial service organizations

December 2020: 100,000+ Microsoft customers compromised through Dark Halo attacks

Q1 2021: Hafnium attackers pivot from on-prem to M365 for C2 & persistence

Q2-Q3 2021: Copycats use Dark Halo and Hafnium for IP theft and ransomware campaigns

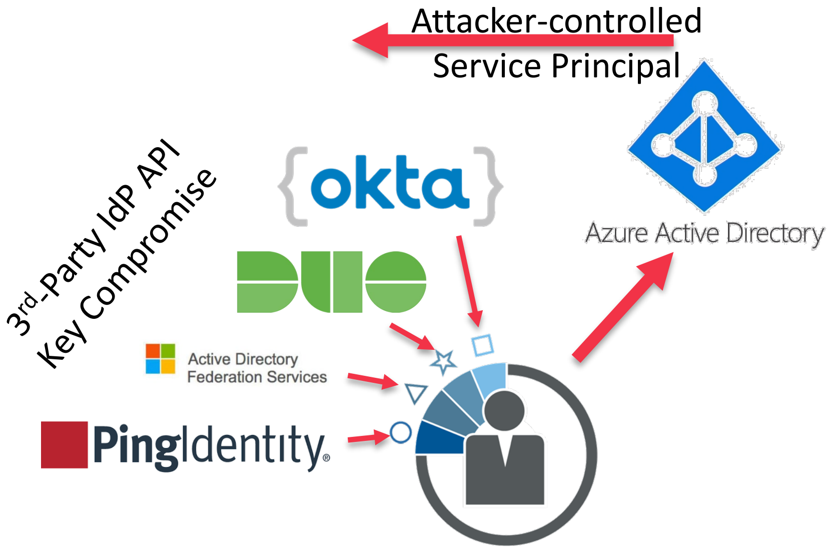
Q4 2021: Nobelium attack announced affecting 100,000+ additional customers

January 2022: Microsoft announces additional M365 vulnerabilities impacting thousands of customers

February 2022: M365 vulnerabilities exploited to interrupt Ukraine military support operations

How much worse can it get?

Common M365 Attack Paths



Attacker-controlled Service Principal

3rd-Party IdP API Key Compromise

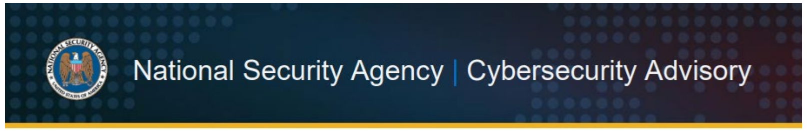
okta

DUO

Active Directory Federation Services

PingIdentity

Azure Active Directory



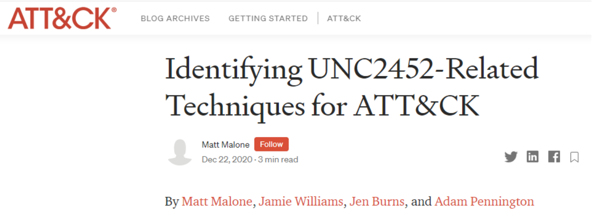
National Security Agency | Cybersecurity Advisory

Detecting Abuse of Authentication Mechanisms

NSA Alert 198854

Exchange Online

Legacy Protocols
IMAP/POP3/AS
MFA Bypass



ATT&CK® BLOG ARCHIVES GETTING STARTED | ATT&CK

Identifying UNC2452-Related Techniques for ATT&CK

Matt Malone Follow
Dec 22, 2020 · 3 min read

By Matt Malone, Jamie Williams, Jen Burns, and Adam Pennington

https://medium.com/mitre-attack/identifying-unc2452-related-techniques-9f7b6c7f3714

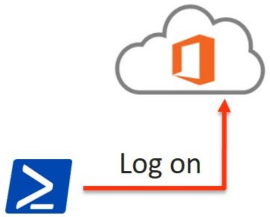
OneDrive

Microsoft Teams

Ransomware Delivery

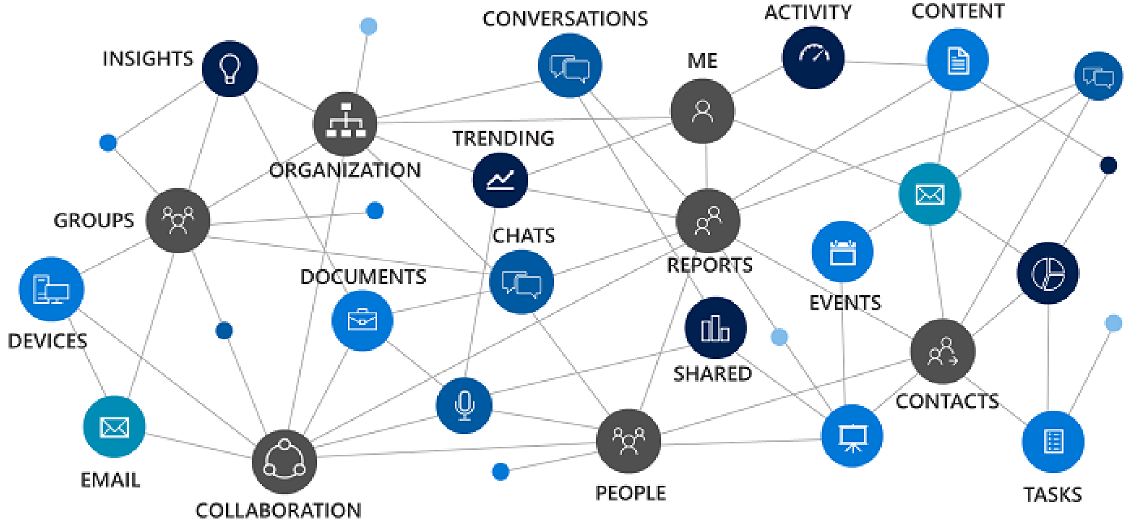
Key Capabilities

- PowerShell
- PowerShell
- PowerShell
- …and GraphAPI knowledge



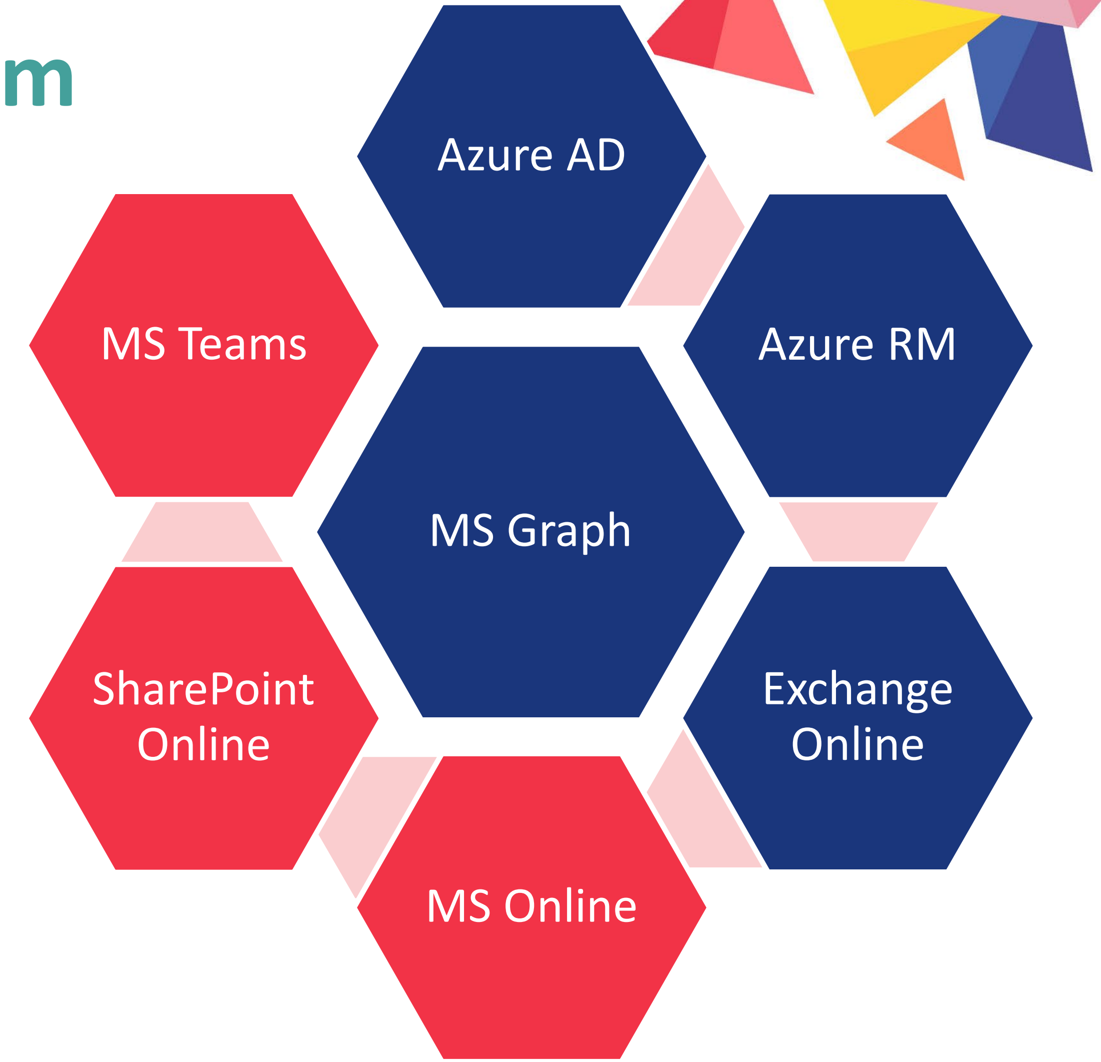
Connect-MsolService

graph.microsoft.com



PowerShell / GraphAPI Conundrum

- Seven different datasources to manage to get basic threat hunting visibility in M365
- Different Logon Methods
  - Supports Service Principals
  - Requires User Credentials
- Mobile Vulnerability Assessment Example
  - How many mobile devices could have their credentials stolen?
- APIs to query:
  - Azure AD (enumerate all active users)
  - Exchange Online (correlate all active mailboxes and mobile connections)
  - MS Graph (Intune data correlation)



Azure AD

MS Teams

Azure RM

MS Graph

SharePoint Online

Exchange Online

MS Online

Threat Hunting Scenario

- Exchange Online Administrator Privilege Abuse
  - Organization has restricted admin tasks to only those with Microsoft Authenticator strictly enforced
  - Long-term unauthorized access discovered
  - How?
- Always fundamentally question EVERY step of the identity supply chain!
  - What is the level of effort to clone a Microsoft Authenticator application?
  - What is the level of effort to compromise a browser used by Exchange Admin?

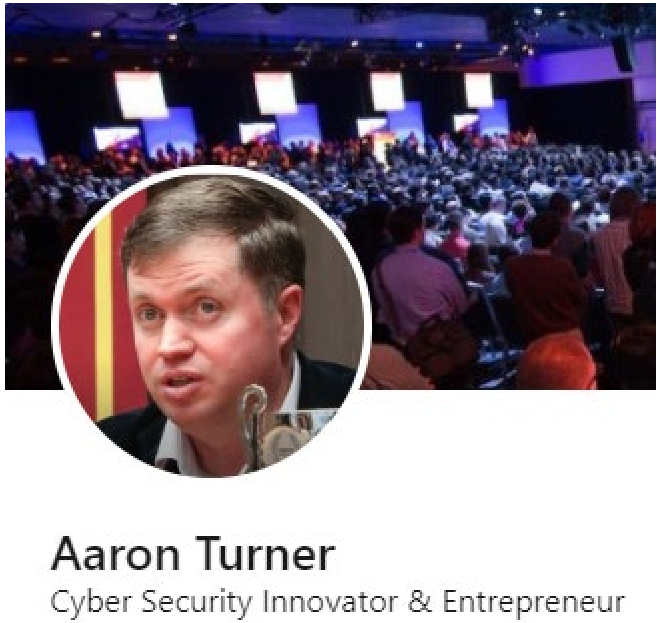
M365 Threat Hunting Action Plan

- Get good at PowerShell!
  - Online Training: Analyzing M365 Security Settings with PowerShell (iansresearch.com)
- Establish appropriate change detection controls
  - First you'll need a baseline, do it NOW
- Implement strong change management for authorized M365 changes
  - Service management tools like ServiceNow can help, but they all require discipline

Questions & Staying In Touch

- Questions & Comments?

- Connect with me on LinkedIn https://www.linkedin.com/in/aaronrturner/



Aaron Turner

Cyber Security Innovator & Entrepreneur