SECRUTINY

Dark Halo

How a new class of cloud cyber attack is reshaping security

Aaron Turner

Founder & CEO - Siriux

Aaron Turner – My Background

- Awarded “Top 5 InfoSec Executive Leaders of Last 30 Years” by SC Magazine
- Worked on teams to establish Microsoft’s first cybersecurity capabilities in late 1990’s and early 2000’s, recognized several times by Bill Gates as cybersecurity leader
- Developed technologies to keep critical infrastructure safe from cyberattacks like Stuxnet
- Inventor, Entrepreneur, Author
- Father of 3 grown daughters and passionate VW T1 Kombi restorationist
- Always looking to gain an advantage over cyber attackers

Agenda

- 2020 - So many exploits… so little time
- Complexity breeds… apathy?
- Dark Halo Attacker M365 Activities
- Big Picture

2020 – So many exploits… so little time

FireEye Tool Proliferation

SolarWinds Supply Chain Attack

VMWare W1 Exploit

Duo MFA Bypass

M365 Privilege Abuse

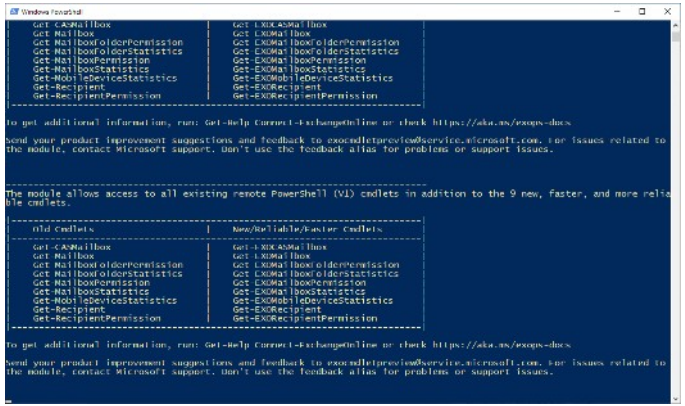
Any APT Campaign

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

M365 Complexity – Tough to Get Straight Answers

- Office 365 security research started in 2017
- First consulting engagement in 2018 with a customer with over 50,000 users
  - Difficult to fully comprehend attack surface
  - 8 weeks of R&D = maybe 25% coverage of security settings
  - VERY difficult to find appropriate documentation
- M365 security configuration research in March 2020 discovered over 7,500 potential settings for each USER within M365

```
    </server-profile>
    <authentication-profile>
      <entry name="HA-AuthProfile-GroupA">
        <multi-factor-auth>
          <mfa-enable>no</mfa-enable>
        </multi-factor-auth>
        <method>
          <ldap>
            <server-profile>HS-LDAPServer</server-profile>
            <login-attribute>hsTeam</login-attribute>
          </ldap>
        </method>
        <allow-list>
          <member>all</member>
        </allow-list>
        <username-modifier>%USERINPUT%@%USERDOMAIN%</username-modifier>
        <user-domain>481</user-domain>
      </entry>
    </authentication-profile>
    <certificate>
      <entry name="4faredirect">
        <subject-hash>680d3661</subject-hash>
        <issuer-hash>680d3661</issuer-hash>
        <not-valid-before>Apr 20 15:14:29 2020 GMT</not-valid-before>
        <issuer>/CN=150.172.202.136</issuer>
        <not-valid-after>Apr 20 15:14:29 2021 GMT</not-valid-after>
        <common-name>150.172.202.136</common-name>
        <expiry-epoch>1618931669</expiry-epoch>
        <ca>yes</ca>
        <subject>/CN=150.172.202.136</subject>
```



Dark Halo – First Global M365 Incident

Nation/state attackers have already used M365's complexity to essentially hide in plain sight. In the US Treasury and other US customers' M365 tenants, reconnaissance and data exfiltration activities were accomplished using poorly-documented M365 administrative interfaces.

In Siriux's research, less than 1 in 10 organizations has invested in any sort of M365 monitoring to detect Dark-Halo-style attacks.

Dark Halo: Discovery/Recon

- M365:
  - Get-AcceptedDomain
  - Get-CASMailbox
  - Get-Mailbox
  - Get-ManagementRoleAssignment
  - Get-OrganizationConfig
- On-Prem Exchange:
  - Get-OwaVirtualDirectory
  - Get-WebServicesVirtualDirectory

Dark Halo: Exfiltration

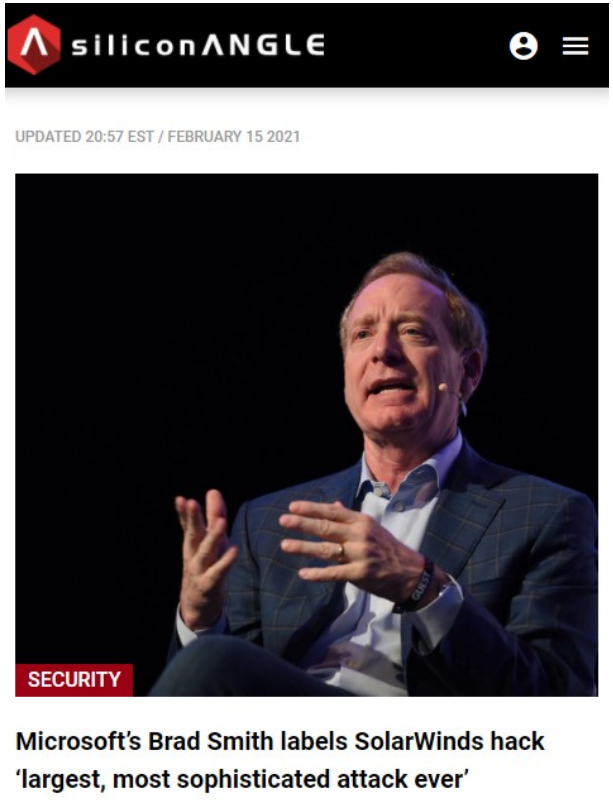
- Set-CASMailbox
- CASMailbox: EwsEnabled
- CASMailbox: ImapEnabled
- CASMailbox: PopEnabled
- CASMailbox: ECPEnabled
- CASMailbox: MAPIEnabled
- CASMailbox: ActiveSyncEnabled
- Get-Mailbox: DelivertoMailboxAndForward
- Get-Mailbox: ForwardingAddress
- Get-Mailbox: AntispamBypassEnabled

Dark Halo: Activity Obfuscation

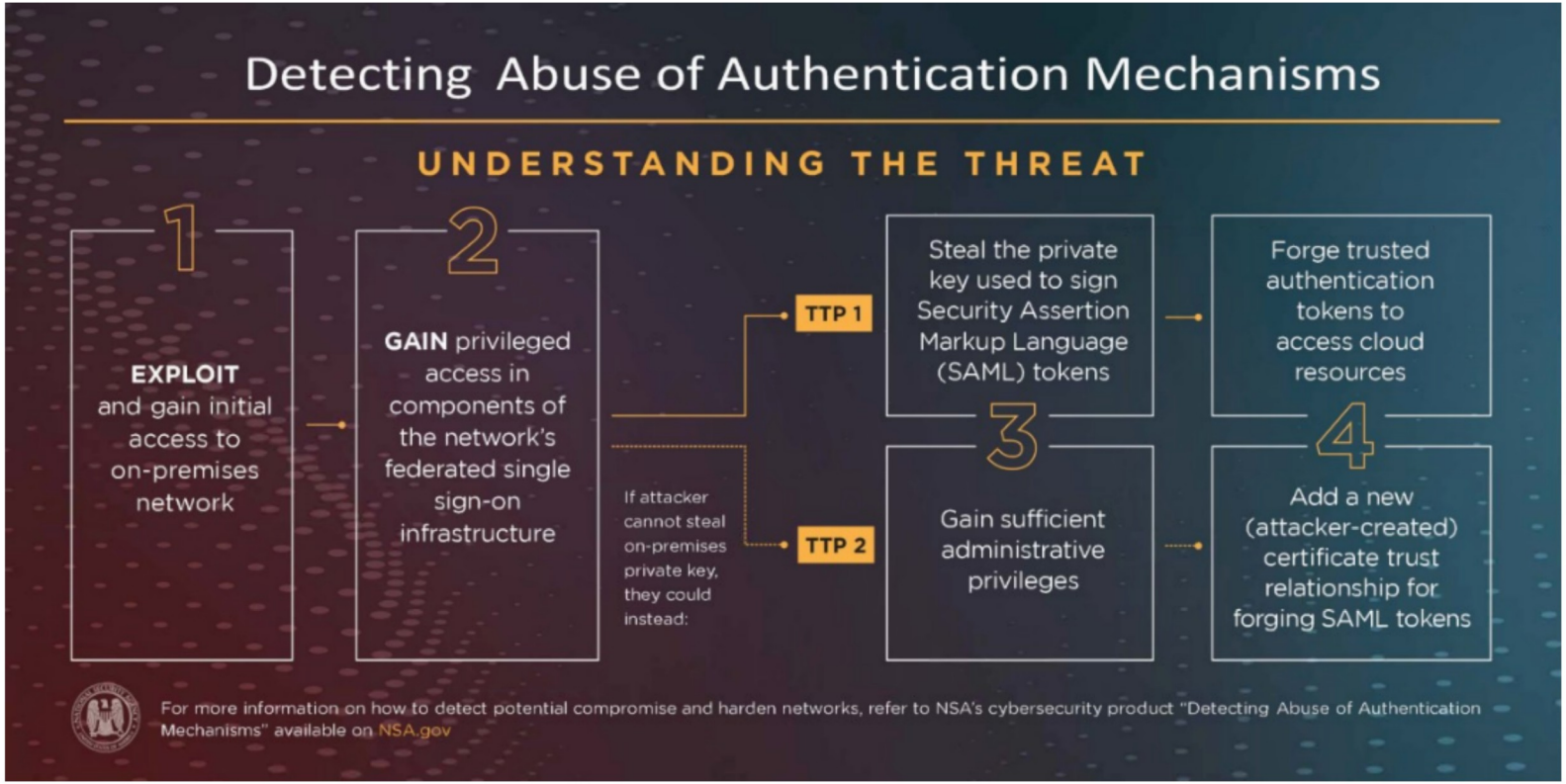
- Get-Mailbox: AuditEnabled
- Get-Mailbox: AuditLogAgeLimit
- Get-AdminAuditLogConfig: AdminAuditLogEnabled
- Get-AdminAuditLogConfig: LogLevel
- Get-AdminAudiLogConfig: UnifiedAuditLogIngestionEnabled

What we've learned

- Siriux has helped dozens of organizations respond to nation/state attacks against their M365 tenants
- The adversaries range from persistent and sophisticated to copycats
- The Dark Halo style attacks of penetrating M365 tenants and persisting have proliferated
- The default settings that Microsoft let most of their M365 clients inherit are not appropriate for proper identity and data protection

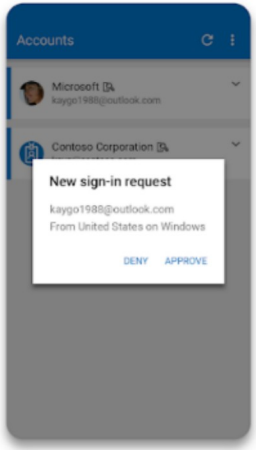


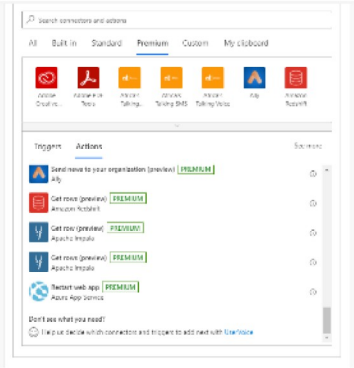
Big Picture: Not just a Microsoft Problem



GATO: M365 Attacks Out of the Bag

- Global Admin Account Takeover (GATO)
  - Browser exploit started the game (probably opportunistic?)
  - Targeted attack against vulnerable iPhone to capture Microsoft Authenticator keys
  - Cloned Authenticator + credentials = full control of tenant
  - Attackers used Exchange Online powershell commands to harvest information from targets' email accounts
  - Information most likely used for financial market arbitrage
- Wild West of Connectors & Apps
  - Without appropriate plugin hygiene and change management, massive exploit risk
  - M365 Power Automate used to clone Sharepoint/OneDrive repositories based upon content rules
  - Microsoft Teams configurations used to snoop on HR communications about layoffs





Detection Tools

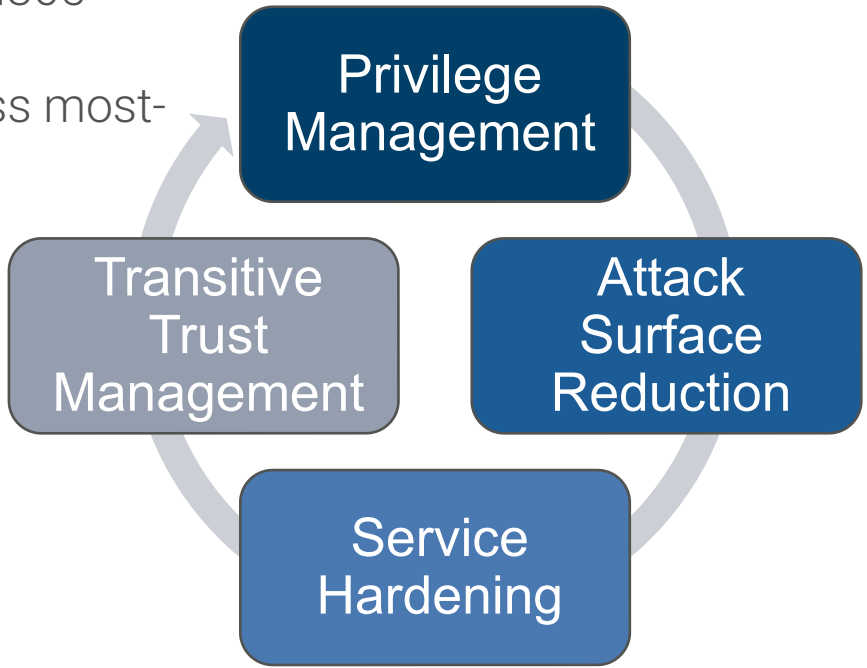
- Azure AD Artefact detection tools:
  - CrowdStrike
  - Mandiant
- Looking at Azure AD artefacts is only part of the problem
  - Azure AD logging, federation credential and service principle forensics
  - Most of the data exfiltration and attacker obfuscation activity observed within Siriux customers and those organizations Microsoft has assisted have significant Exchange Online artefacts
- Secrutiny has worked with Siriux to develop a scan that goes beyond the Mandiant and CrowdStrike tools
  - Exchange Online, SharePoint, Teams and Intune artefacts

Dark Halo Artefacts in Other SaaS Platforms?

- Salesforce Consulting Engagement:
  - Logging disabled in August 2020
  - Unauthorized API data feed installed around same time
- Workday Security Assessment:
  - Anomalous vendor registration activities in September 2020
  - “Authorized” (but unauthorized) vendor payments

M365 Security Tactics

- Begin to assess the integrity of M365 settings:
  - Azure AD privileges relative to M365 controls
  - M365 Application settings across most-targeted apps:
    - Exchange Online
    - SharePoint Online
    - OneDrive
    - Teams



M365 Security Strategies

- Change detection on material M365 settings
- Auditing & Logging:
  - Assess how to economically & efficiently capture M365 audit logs in a SIEM
  - Trick: how to do this without exponentially increasing your SIEM bill
  - Event filtering is key
- Identity Provider Hygiene
  - Improve auditing and logging for MFA component integrity
  - Evaluate Identity Provider key rotation
  - Improve telemetry from SAML-driven apps for identity use & correlate to other indicators

DARK HALO & M365

MAKE USE of a FREE SIRIUX DARK HALO SECURITY SCAN

CONTACT SECRUTINY TODAY TO PROTECT YOUR M365 INVESTMENT.

HOW MICROSOFT'S SaaS CONFIGURATION HELPED ATTACKERS HIDE IN PLAIN SIGHT.

MS 365 COMPLEXITY LEAVES IT OPEN TO THREATS.

WE MUST UNDERSTAND THE THREAT, WHICH ISN'T JUST A MICROSOFT PROBLEM!

GET the ADVANTAGE over ATTACKERS!

M365 CLOUD: "INFRASTRUCTURE AS CODE"

PRIVILEGE MANAGEMENT

ATTACK SURFACE REDUCTION

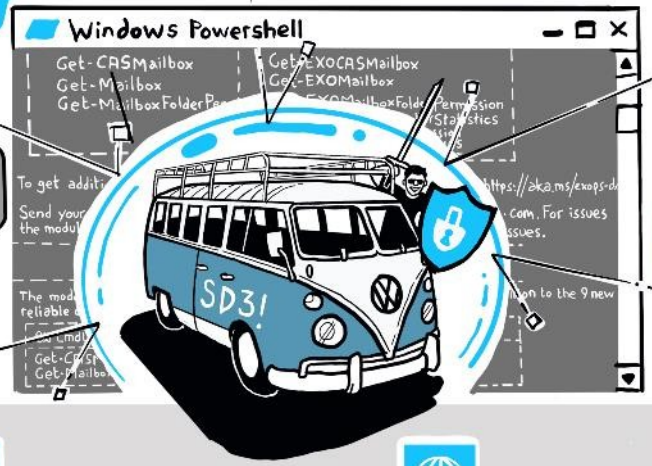
LOOK AT LACK OF AUDIT-LOGGING!

TRANSITIVE TRUST MANAGEMENT

ELIMINATE/IMPROVE THIRD PARTY IDENTITY PROVIDER USAGE!

SERVICE HARDENING

NATION-STATE ATTACK LEADS to 'DARK HALO' PROLIFERATION!



THE ATTACKS / 'THE THREAT':

1	EXPLOIT & GAIN ACCESS TO ON-PREMISES NETWORK.	
2	GAIN PRIVILEGED ACCESS IN COMPONENTS OF THE NETWORK'S FEDERATED SINGLE SIGN-ON INFRASTRUCTURE	
3	STEAL THE PRIVATE KEY TO SIGN SAML TOKENS	GAIN SUFFICIENT ADMINISTRATIVE PRIVILEGES
4	FORGE TRUSTED AUTHENTICATION TOKENS	ADD A NEW CERTIFICATE TRUST RELATIONSHIP FOR FORGING SAML TOKENS

0203 8232 999

INFO@SECRUTINY.COM

WWW.SECRUTINY.COM

SECRUTINY

Questions?

Follow me on LinkedIn

HTTPS://LINKEDIN.COM/IN/AARONRTURNER