HAS ANYONE SEEN THE PRINCIPAL?

Emilian Cebuc & Christian Philipov

Fwd:CloudSec – 13th September 2021

WHO ARE WE?

- Security consultants @F-Secure Consulting
- Professional ~~Meme Masters~~ Cloud enthusiasts – particularly Microsoft's Azure platform
- Helping people secure their cloud estate and breaking stuff along the way

- Shoutout for the original talk idea to Javan Joshua Mnjama - @JavanMnjama

Emilian Cebuc - @RockBoyEmy

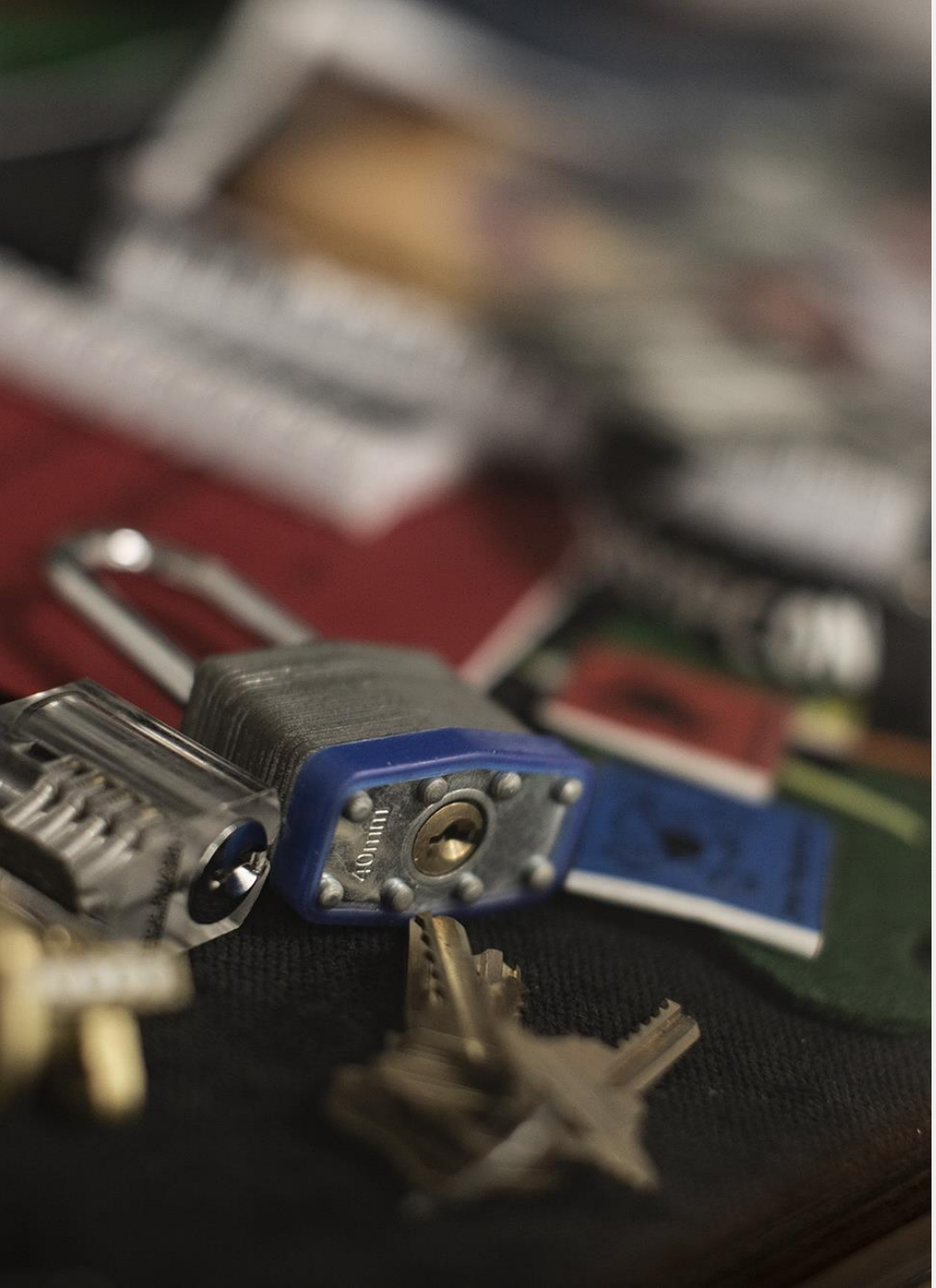
Cristian Philipov - @chrispy_sec

F-Secure

CLOUD COMPROMISES IN THE WILD

- Holmium (APT33) attack – full network control in under a week [1]
- "Living off the Land" (LoL) attacks – leveraging legitimate functionality [2]
- Compromised Azure resources & extensions
- Un-monitored O365 accounts and ADFS
- Password sprays & Phishing
- Lack of MFA

F-Secure



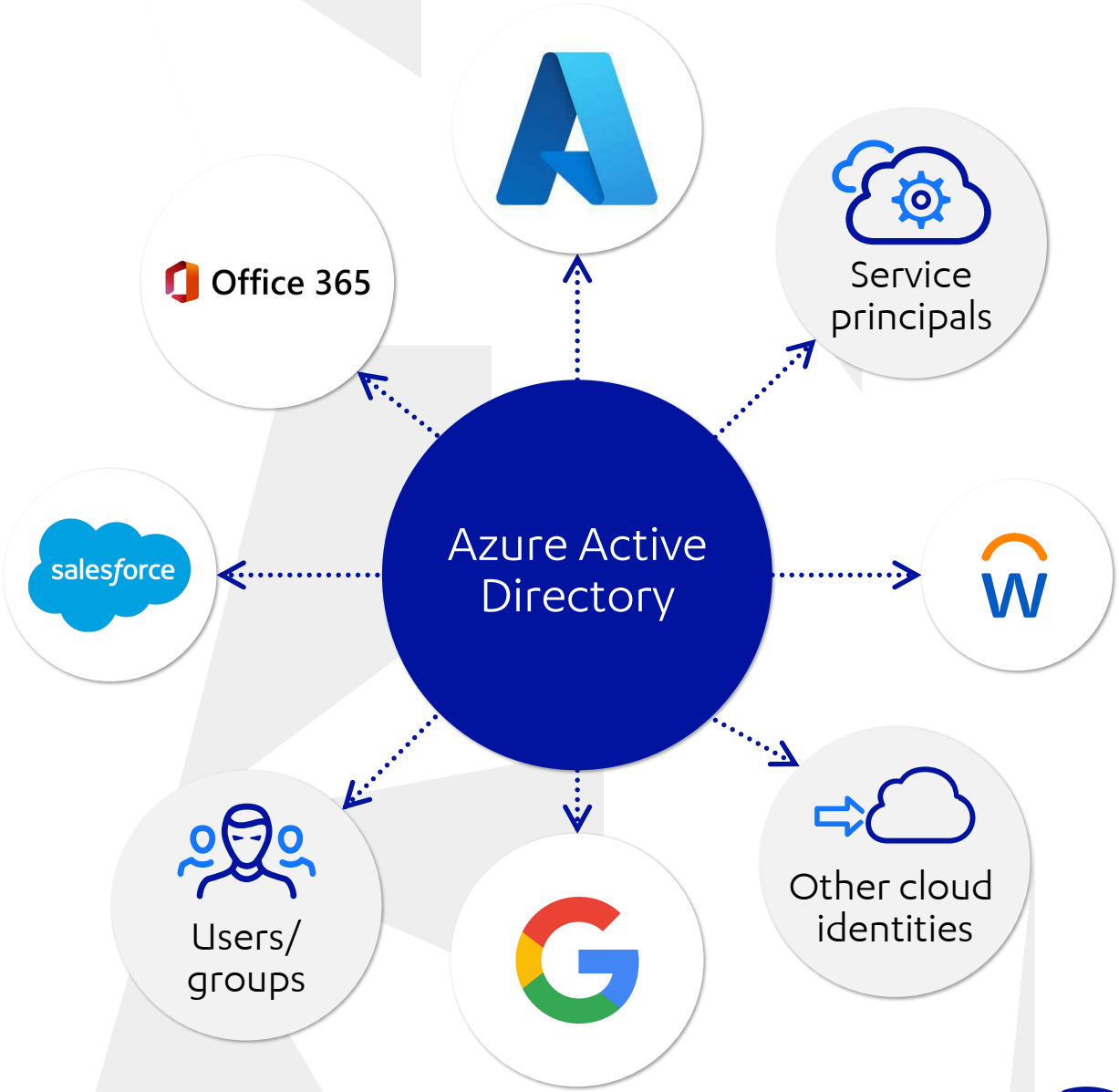
AGENDA

- Azure AD Service Principals
- Azure StormSpotter & cypher queries
- Attack scenarios & exploitation
- Detection & prevention

F-Secure

AZURE AD & SERVICE PRINCIPALS

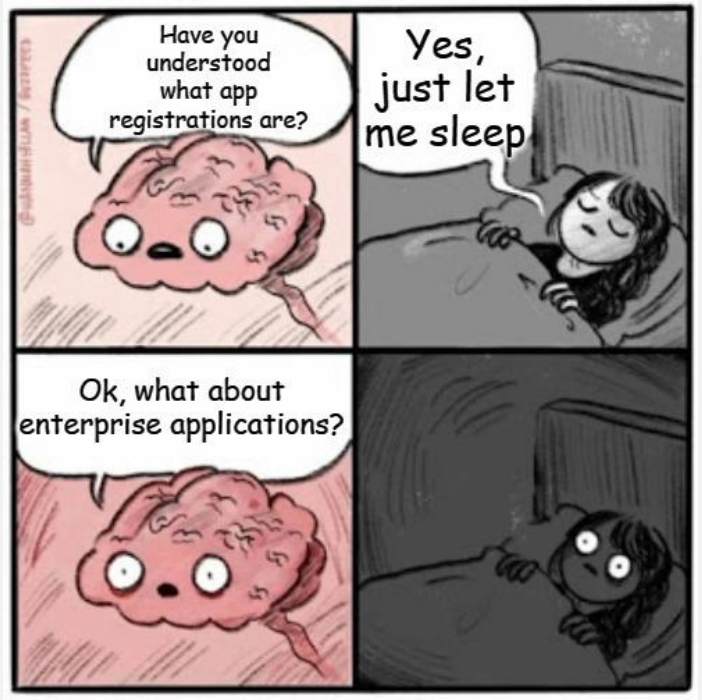
- An Identity Provider (IdP) & Identity and Access Management (IAM) service, in the cloud
- In Azure, you can have identities
- These can have *roles* assigned to them
- Service Principals are accounts for representing non-user entities



F-Secure

SERVICE PRINCIPALS AND CLOUD APPS

- Numerous possibilities for applications in the cloud
  - For employees, customers and partners
- AAD Apps can be "registered" – unique definition
  - A *class* if you think of OOP
- "Instantiate" a copy of the app
- A Service Principal account gets created

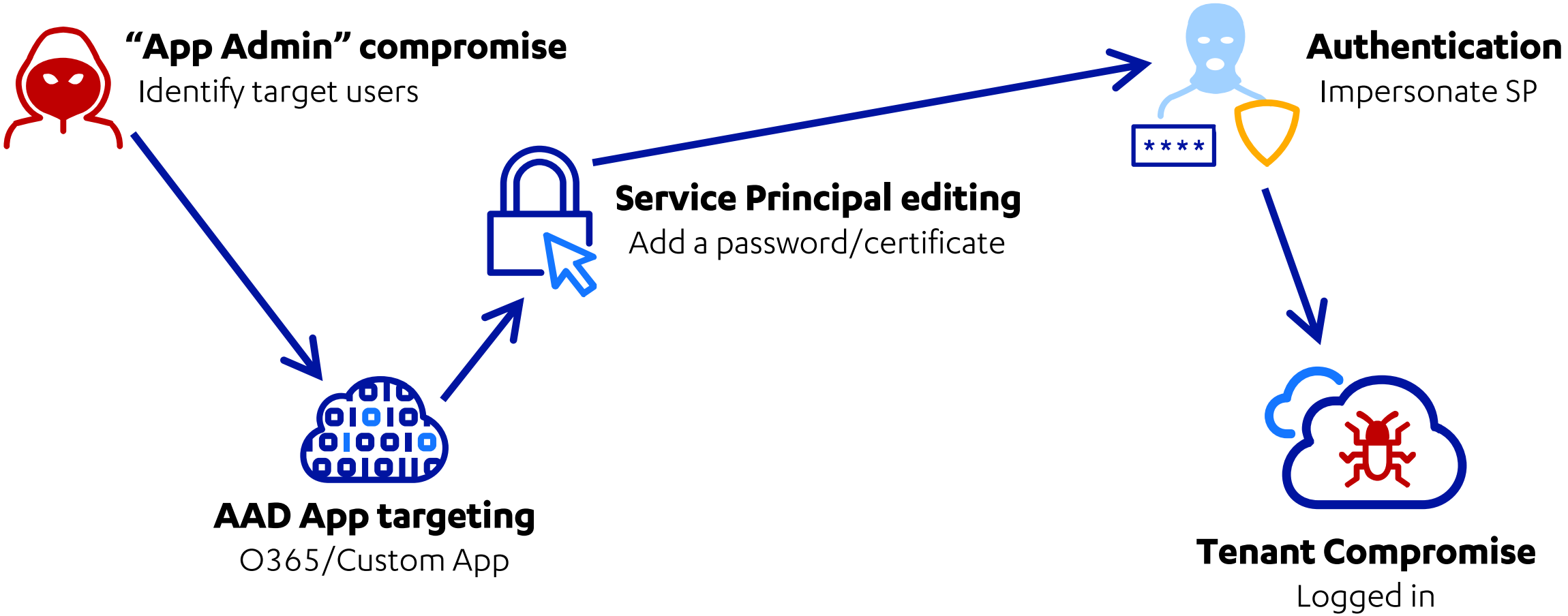


F-Secure

WHY DO WE CARE?

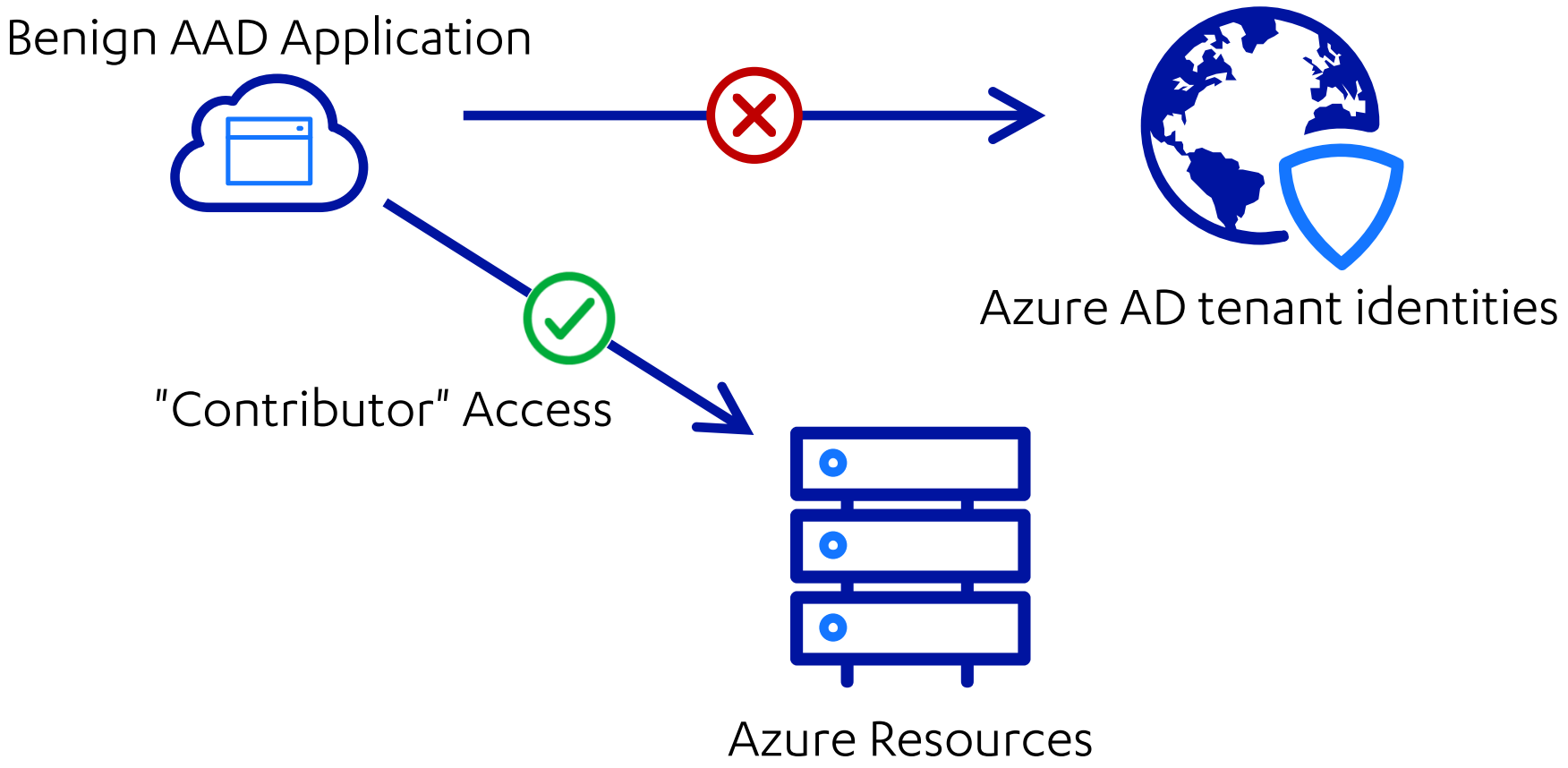
- SPs tend to be overlooked
  - During development
  - Security assessments
- 300+ Apps onboarded with an O365 E3 or E5 tenant license
  - Research in 2019 by Dirkjan [3]
  - However, 2 years later, the situation is not quite the same anymore

ATTACK PATH 1



F-Secure

ATTACK PATH 2



STORMSPOTTER

- Tool for identifying infrastructure and AD components in Azure[4]
- Made by the Azure peeps – neo4j, graphing capabilities
- Cypher queries - creation of visual links among components

STORMSPOTTER

DEMO

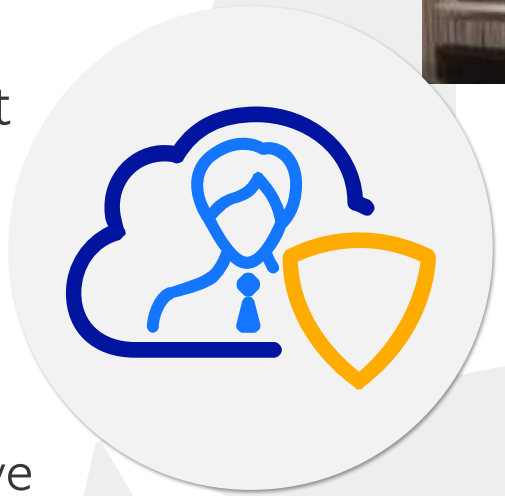
F-Secure

MICROSOFT SERVICE PRINCIPALS

COMMON NAME	PERMISSIONS
Microsoft Rights Management Services	Directory.Read.All Member.Read.Hidden
Office 365 Exchange Online	Directory.Read.All Group.ReadWrite.All User.Read.All
Office 365 SharePoint Online	Files.ReadWrite.All TeamsActivity.Send TeamsAppInstallation.ReadWriteSelfForUser.All
Yammer	Policy.Read.All Reports.Read.All

PREVENTION – USER ACCOUNTS

- Custom roles for users managing applications
  - built-in ones can be quite permissive
  - tailor very specifically
- Disable any AD user's ability to register and consent applications
- Assign "App/Cloud App Admin" and/or "App Developer" accordingly
  - Can still bypass the previous two security toggles above
- PIM, MFA, and CAs (when available for SPs) if possible



F-Secure

PREVENTION – SERVICE PRINCIPALS

- Principle of least privilege - Assign only needed Graph permissions
  - Particularly for admin privileges
- Restrict role assignments for Azure resources
  - "Contributor" by default
  - Remove passwords, if added for any reason
- Perform regular reviews SPs login events
  - Any left with passwords?

F-Secure

DETECTION AND MONITORING?

- Can be quite difficult specifically for this issue - allowed by design
- Your existing logging/monitoring capabilities can detect *some* things
- A tailored set of alerting policies
  - Focus on critical SP's activity, not just user's
- No sign-in logs for 1st party Microsoft Applications

F-Secure

ATTACK PATH IDENTIFICATION CYPHER QUERIES

- `MATCH (a:AADRole)-[r]-(t:AADUser) WHERE (a.name = 'Application Administrator' OR a.name = 'Cloud Application Administrator') RETURN *`
- `MATCH (a:AADRole) WHERE a.name = 'Application Developer' RETURN *`
- `MATCH (a:AADRole)-[r]-(t) WHERE r.roleName = 'Contributor' AND a.objectType = 'ServicePrincipal' OR a.objectType = 'Application' RETURN *`
- `MATCH (a)-[r]-(t) WHERE (r.roleName = 'Contributor' OR r.roleName = 'Owner') AND (a.objectType = 'ServicePrincipal' OR a.objectType = 'Application') RETURN *`
- `MATCH (a) WHERE a.objectType = "ServicePrincipal" AND (a.passwordCredentialCount > 0 OR a.keyCredentialCount > 0) RETURN *`
- `MATCH (w:ResourceGroup)-[p]-(s:Subscription)-[y]-(a:AADUser)-[r]-(g:AADGroup)-[d:MemberOf]-(AADRole) WHERE (y.roleName = "Contributor" OR y.roleName = "Owner") RETURN *`

F-Secure

SP ACTIVITY KQL DETECTION QUERIES

```
// Most active Service Principals (Custom Apps)
AADServicePrincipalSignInLogs
| where TimeGenerated > ago(7d)
| summarize CountPerServicePrincipal = count() by ServicePrincipalName,
ServicePrincipalId, AppId, IPAddress
| order by CountPerServicePrincipal desc
//TimeGenerated
```

```
// Most active AAD Applications (MS Apps)
AADNonInteractiveUserSignInLogs
| where TimeGenerated > ago(7d)
| summarize CountPerServicePrincipal = count() by AppDisplayName, AppId, Identity,
IPAddress, TimeGenerated
//| order by CountPerServicePrincipal desc
```

F-Secure

SP ACTIVITY KQL DETECTION QUERIES

```
// Suspicious activity by SPs

// Look for audit logs in the last x days as needed
// Filter by SP OperationName of interest for these attacks
// Filter by escalation-related OperationName and AAD App Identity

AuditLogs
| where TimeGenerated > ago(7d)
| where OperationName == "Add service principal credentials"
or OperationName == "Remove service principal credentials"
or OperationName == "Add app role assignment to service principal"
or OperationName == "Update service principal"
//| where OperationName == “Add member to group“ and Identity == "Office 365 Exchange Online"
| summarize CountPerServicePrincipal = count() by Identity, OperationName
//TimeGenerated
```

F-Secure

TAKEAWAYS

Service principals are an equally interesting attack vector as privileged users	Proactively identify potential targets of compromise	Prevention of these issues is no easy task
• Aim at identifying anomalous behavior indicating human intervention	• Admin users, Apps deployed, sensitive Azure resources • Tools such as StormSpotter and cypher queries can be of great help	• Build layered defenses [5] • Set up detection around eventual compromise

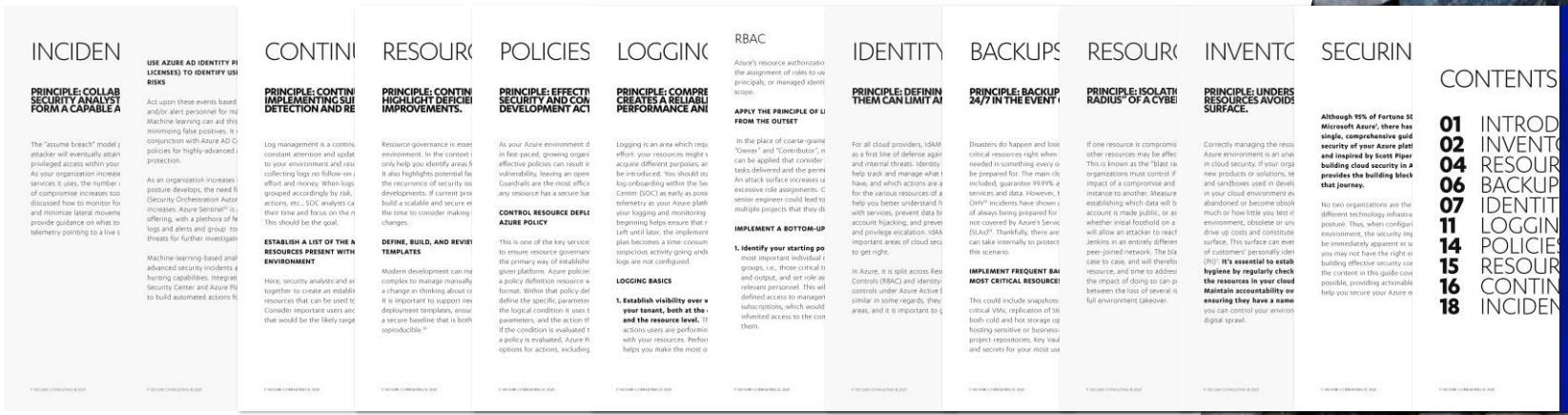
REFERENCES

1. https://www.microsoft.com/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/
2. https://www.microsoft.com/security/blog/2021/03/09/azure-lolbins-protecting-against-the-dual-use-of-virtual-machine-extensions/
3. https://dirkjanm.io/azure-ad-privilege-escalation-application-admin/
4. https://github.com/Azure/Stormspotter
5. https://lnkd.in/e7RPappr
6. Follow us on Twitter for news on the tool release

F-Secure

THE END – THANK YOU!

Questions?



F-Secure


F-Secure®