Secureworks®

Abusing Azure AD Pass-Through Authentication (PTA) Vulnerabilities

@DrAzureAD

https://linkedin.com/in/nestori

About the speaker

Who?

- Dr. Nestori Syynimaa
- Senior Principal Security Researcher @ Secureworks CTU
- Creator of *AADInternals* toolkit
- MVP (Identity & Access), MVR #70

Contact details

- nsyynimaa@secureworks.com
- Twitter: @DrAzureAD
- https://linkedin.com/in/nestori
- https://aadinternals.com

AADInternals

- Admin & hacking toolkit for Azure AD & Microsoft 365
- Open source:
  - https://github.com/gerenios/aadinternals
  - https://aadinternals.com/aadinternals
- MITRE ATT&CK
  - https://attack.mitre.org/software/S0677/

Groups That Use This Software

ID	Name	References
G0016	APT29	[5]

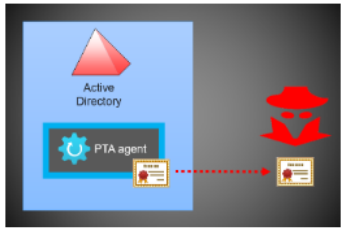
Contents

- Hybrid authentication options
- Pass-through authentication (PTA)
- Abusing PTA
- Detecting & mitigation

AADInternals.com

The ultimate Azure AD / Microsoft 365 hacking and admin toolkit

AAD KILL CHAIN | DOCUMENTATION | LINKS | OSINT | TALKS | TOOLS



Exploiting Azure AD PTA vulnerabilities: Creating backdoor and harvesting credentials

September 20, 2022

In 13 September 2022, **Secureworks** published a Threat Analysis: **Azure Active Directory Pass-Through Authentication Flaws**. The vulnerabilities discovered by our team allows threat actors to gain persistent and undetected access to the target Azure AD tenant.

In this blog post, I'll show how the attack can be conducted using **AADInternals** and standalone Windows server.

Deep-dive to Azure AD Pass-Through Authentication

March 30, 2020

In my earlier **blog**, I explained how Azure AD identity federation works under-the-hood. In this post, I'll be doing the same with Azure AD pass-through authentication (PTA).

Azure Active Directory Pass-Through Authentication Flaws

TUESDAY, SEPTEMBER 13, 2022
BY: COUNTER THREAT UNIT RESEARCH TEAM

Updated: September 20, 2022

Summary

Pass-through authentication (PTA) is one of the Azure Active Directory (Azure AD) hybrid identity authentication methods. PTA relies on PTA agents installed on one or more on-premises servers. Azure AD uses a certificate-based authentication (CBA) to identify each agent. In May 2022, Secureworks® Counter Threat Unit™ (CTU) researchers analyzed how the protocols used by PTA could be exploited. The researchers determined that threat actors could steal the identity of the PTA agent by exporting the certificate used for CBA. The compromised certificate can be used with the attacker-controlled PTA agent to create an undetectable backdoor, allowing threat actors to log in using invalid passwords, gather credentials, and perform remote denial of service (DoS) attacks. Attackers can renew the certificate when it expires to maintain persistence in the network for years. A compromised certificate cannot be revoked by an organization's administrators.

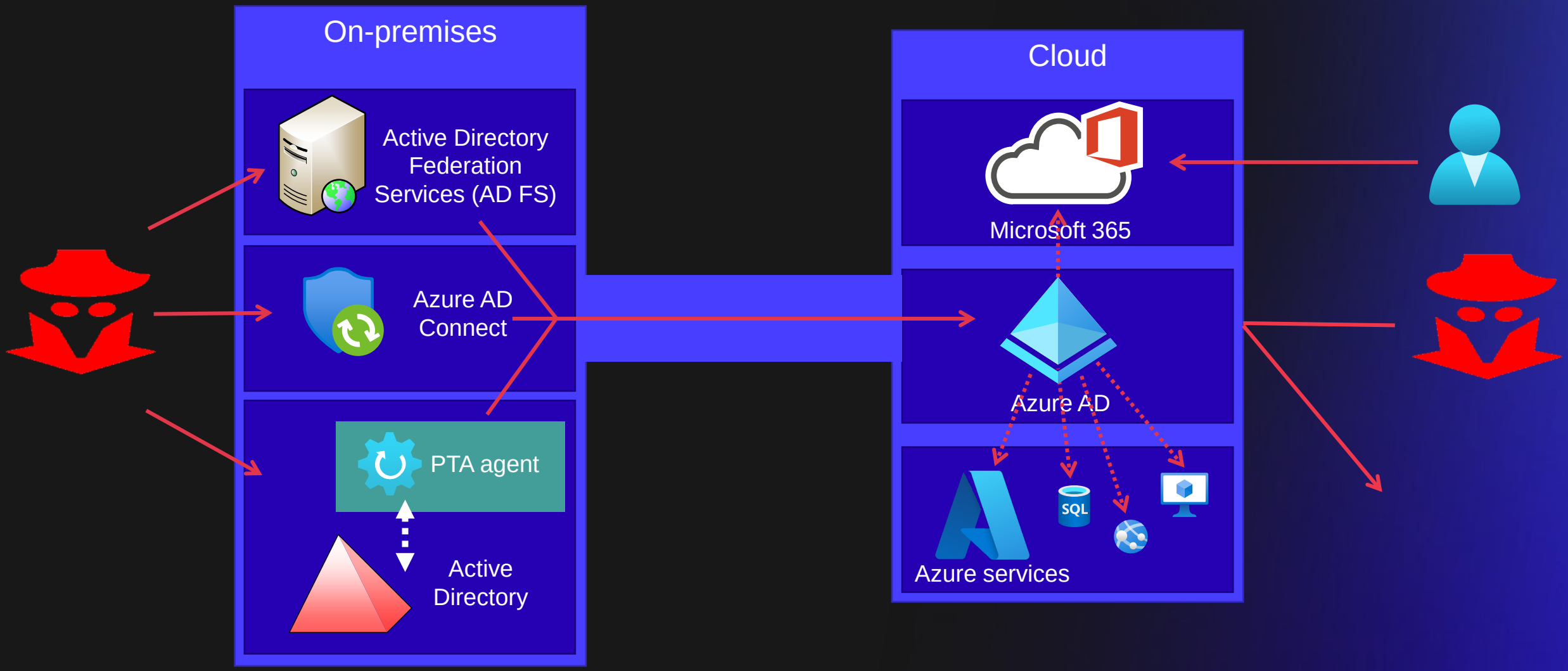
CTU™ researchers shared their findings with Microsoft on May 10, 2022. Microsoft responded on July 2 that PTA is working as intended and gave no indication of plans to address the reported flaws.

Update: On September 20, Microsoft sent an update about their plans to address these issues.

https://aadinternals.com/post/pta/
https://aadinternals.com/post/pta-deepdive/
https://www.secureworks.com/research/azure-active-directory-pass-through-authentication-flaws

Secureworks

(Hybrid) Cloud Security



Hybrid Authentication Options

Identity federation (ADFS)

Azure Active Directory

Active Directory Federation Services (AD FS)

Active Directory

Password-hash synchronization (PHS) *

Azure Active Directory

Azure AD Connect

Active Directory

Pass-through authentication (PTA) *

Azure Active Directory

PTA agent

Active Directory

Certificate Based Authentication (CBA)

Azure Active Directory

Certificate Authority (CA)

* Supports seamless single sign-on

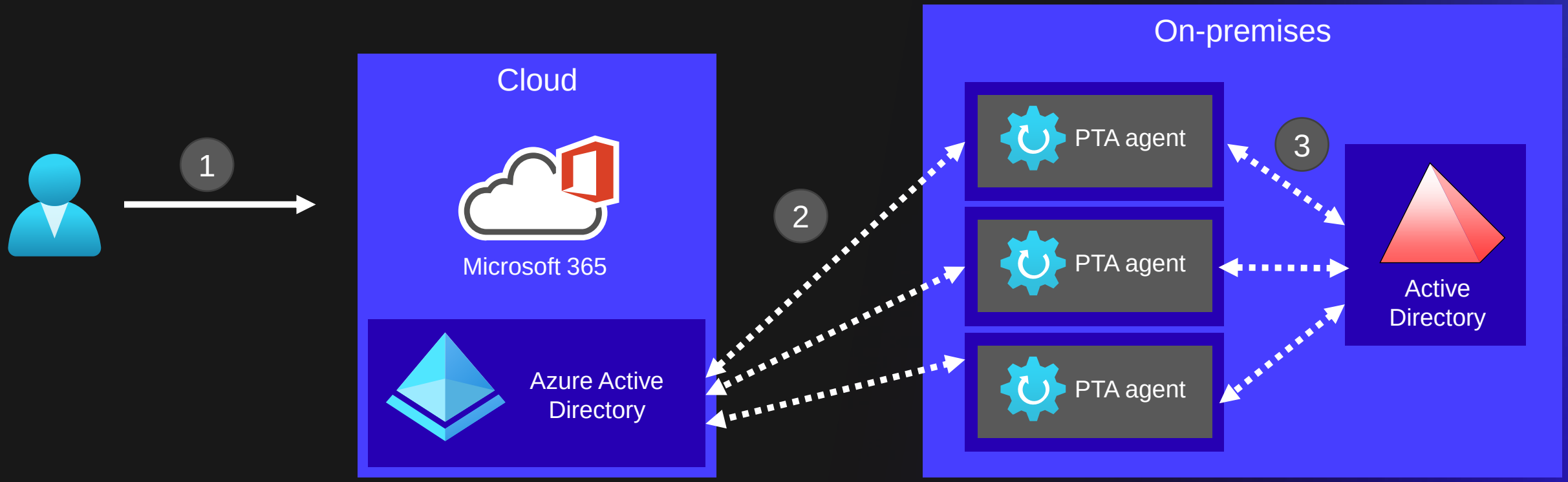
Pass-through authentication (PTA)

- Authentication via agent installed in on-prem server
  - First one installed automatically on Azure AD Connect server
  - A minimum of 3 agents recommended (max 40)

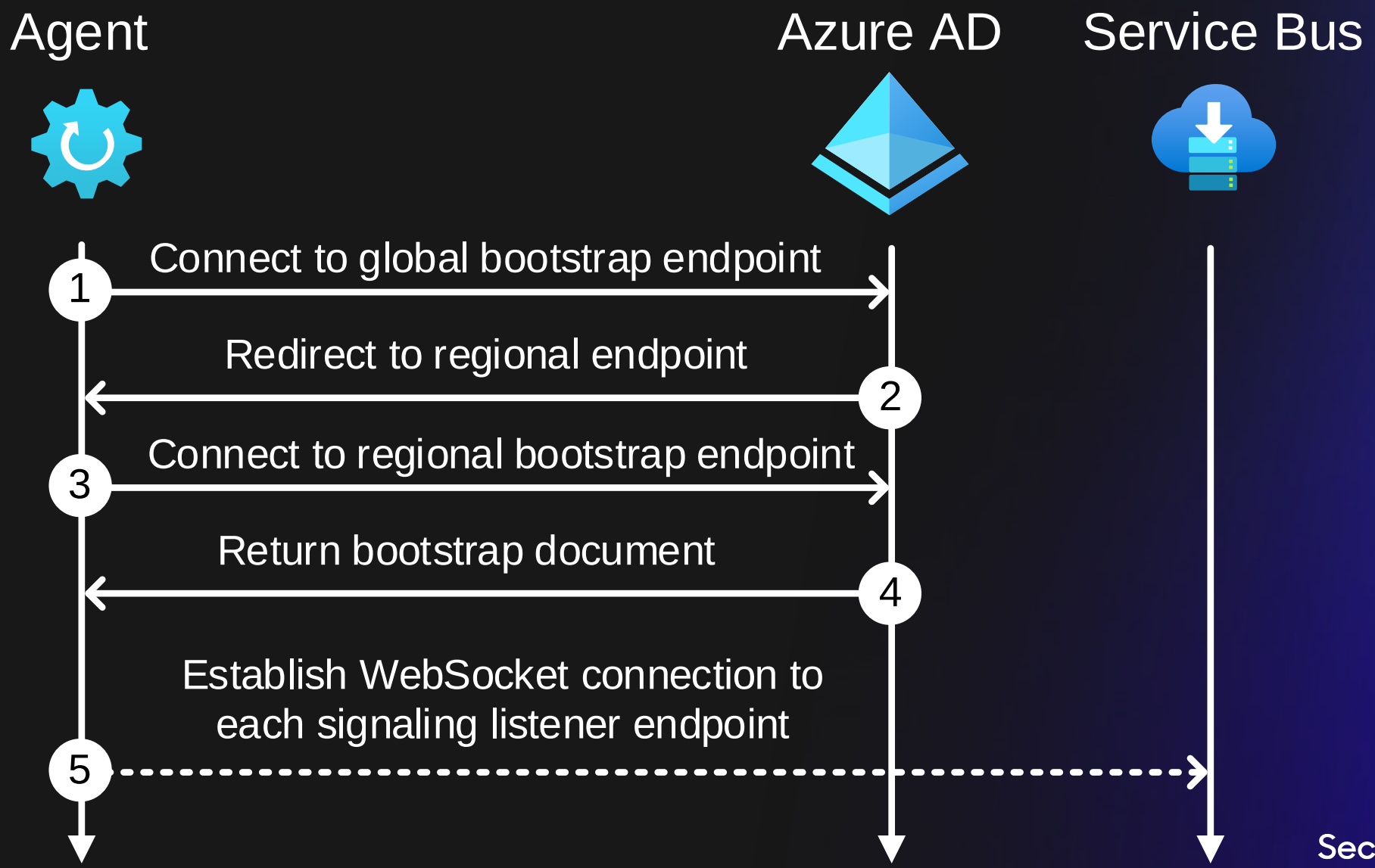
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

High-level PTA architecture

1. User enters credentials
2. Azure AD creates an authentication request
3. Agent passes credentials to *LogonUserW* (network logon)



PTA agent start-up process

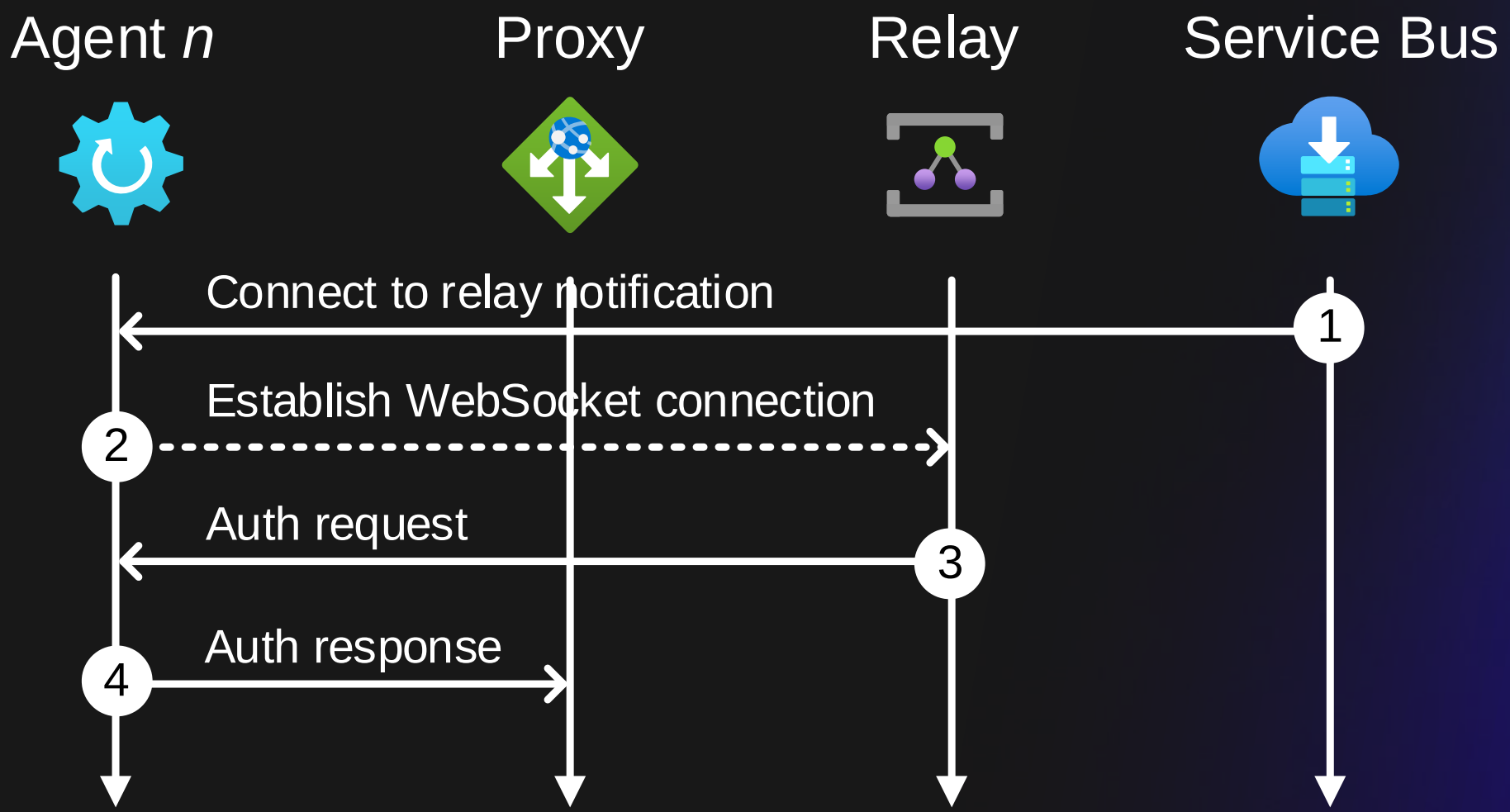


PTA details: bootstrap

- Contains (usually) 8 *SignalingListenerEndpoints*
  - Individual *SharedAccessKey* – doesn't seem to change..

```
<SignalingListenerEndpoints xmlns:a="http://schemas.datacontract.org/2004/07/Microsoft.ApplicationProxy.Common.BootstrapDataM
    <a:SignalingListenerEndpointSettings i:type="a:ServiceBusSignalingListenerEndpointSettings">
        <a:IsAvailable>true</a:IsAvailable>
        <a:Name>his-nam1-eus1/95265eb2-cbfe-4ee4-9552-b0ad287d2669_17d93d40-1389-4f69-b6f6-dcaedfdc4bb7</a:Name>
        <a:Domain>servicebus.windows.net</a:Domain>
        <a:Namespace>his-nam1-eus1</a:Namespace>
        <a:ReliableSessionEnabled>false</a:ReliableSessionEnabled>
        <a:Scheme>sb</a:Scheme>
        <a:ServicePath>95265eb2-cbfe-4ee4-9552-b0ad287d2669_17d93d40-1389-4f69-b6f6-dcaedfdc4bb7</a:ServicePath>
        <a:SharedAccessKey>vEMoAaLnyR8SKd9DqWHsNY6QVzox7z/1F7cn4jvf4gI=</a:SharedAccessKey>
        <a:SharedAccessKeyName>Connector</a:SharedAccessKeyName>
    </a:SignalingListenerEndpointSettings>
    <a:SignalingListenerEndpointSettings i:type="a:ServiceBusSignalingListenerEndpointSettings">
        <a:IsAvailable>true</a:IsAvailable>
        <a:Name>his-nam1-ncus1/95265eb2-cbfe-4ee4-9552-b0ad287d2669_17d93d40-1389-4f69-b6f6-dcaedfdc4bb7</a:Name>
        <a:Domain>servicebus.windows.net</a:Domain>
        <a:Namespace>his-nam1-ncus1</a:Namespace>
        <a:ReliableSessionEnabled>false</a:ReliableSessionEnabled>
        <a:Scheme>sb</a:Scheme>
        <a:ServicePath>95265eb2-cbfe-4ee4-9552-b0ad287d2669_17d93d40-1389-4f69-b6f6-dcaedfdc4bb7</a:ServicePath>
        <a:SharedAccessKey>sEzvw9V5pqxc9AG16Lr4GLRlBtIYjPdm2tf54s/QpOE=</a:SharedAccessKey>
        <a:SharedAccessKeyName>Connector</a:SharedAccessKeyName>
    </a:SignalingListenerEndpointSettings>
    <a:SignalingListenerEndpointSettings i:type="a:ServiceBusSignalingListenerEndpointSettings">
        <a:IsAvailable>true</a:IsAvailable>
```

PTA authentication process



PTA details: Authentication request

- Contains encrypted passwords, one entry per ~~agent~~ certificate
- Key identifier:

  `<agent id>_<certificate thumbprint>`


```
{
    "TrafficProtocol": 2,
    "Domain": "AADSECURITY",
    "EncryptedData": [
        {
            "Base64EncryptedData": "gxFn2UPDMKSBYtz90AllqTmFsOB\\/HsLFUd9gxq8Tn4RSDPX5px\\/7YoywkuSY\\/UWq5acoKVD\\/DYVopruLXFccPo
            "KeyIdentifer": "672843e0-8b25-434f-93e2-5d5071139e09_893657AEAE25D4C913BCF37CB138628772BE1B52"
        },
        {
            "Base64EncryptedData": "KpH2k+loudJy8TLniN1C8XalZnVvwO6gC9m2G6wrZ1Lg5j4z+n29oKSupS11rMR1PJHtw7RN4dIw0jDfkItExsBLakSfTO
            "KeyIdentifer": "672843e0-8b25-434f-93e2-5d5071139e09_0489715DDD57FBEE81DAC0454AA2470B8FD2C86B"
        }
    ],
    "Password": "",
    "UserPrincipalName": "AllanD@[redacted]"
}
```

PTA details: Authentication response

- Successful


```
[{
        "Resource": true,
        "ClaimType": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication",
        "Right": "http://schemas.xmlsoap.org/ws/2005/05/identity/right/identity"
    }, {
        "Resource": "AllanD@                    ",
        "ClaimType": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name",
        "Right": "http://schemas.xmlsoap.org/ws/2005/05/identity/right/identity"
    }
]
```

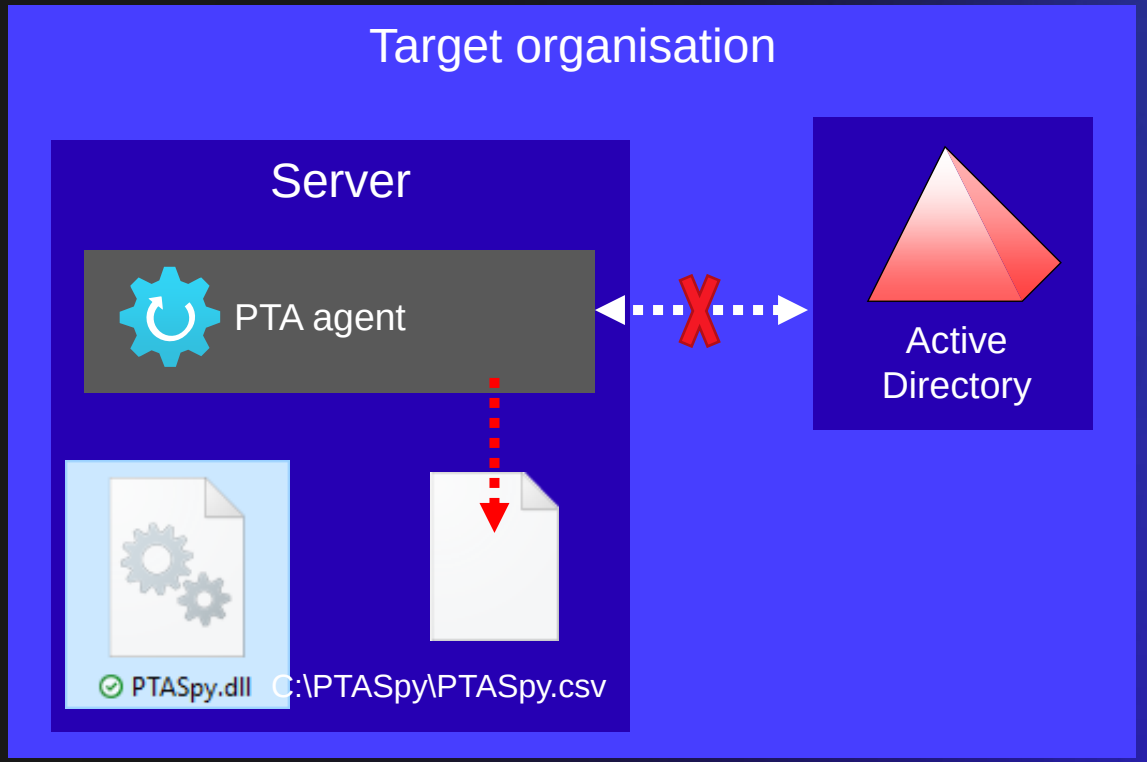

- Failed


```
[
    {
        "Resource": false,
        "ClaimType": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication",
        "Right": "http://schemas.xmlsoap.org/ws/2005/05/identity/right/identity"
    },
    {
        "Resource": 1327,
        "ClaimType": "http://msappproxy.net/ws/2015/02/identity/claims/validationfailurereasoning",
        "Right": "http://schemas.xmlsoap.org/ws/2005/05/identity/right/identity"
    }
]
```

Abusing PTA

AADInternals: PTASpy

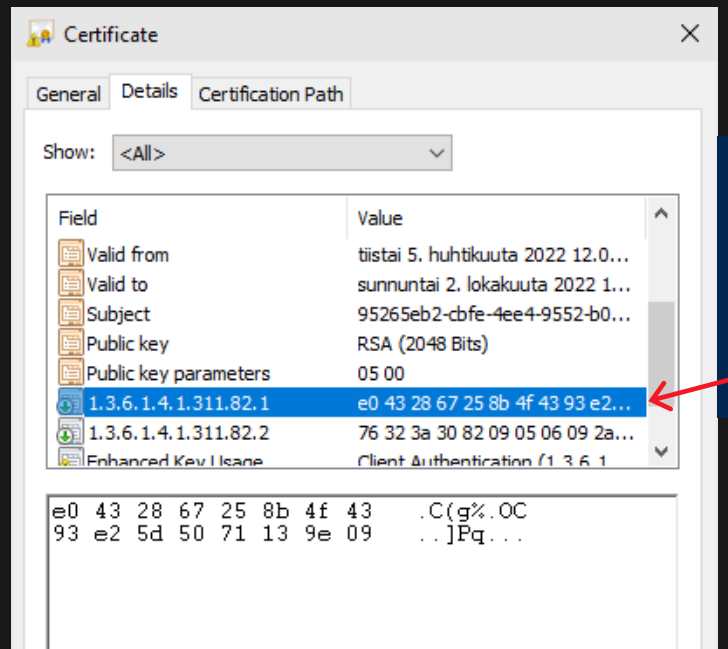
- Since Dec 2019
- Based on work of @_xpn_ (Adam Chester)
- Requires local admin permissions
- Inject *PTASpy.dll* to PTA service
  - Replaces *LogonUserW*
  - Accepts all passwords
  - Saves passwords to .csv



https://github.com/Gerenios/public/blob/master/PTASpy.cpp
https://aadinternals.com/aadinternals/#install-aadintptaspy

What is a PTA agent?

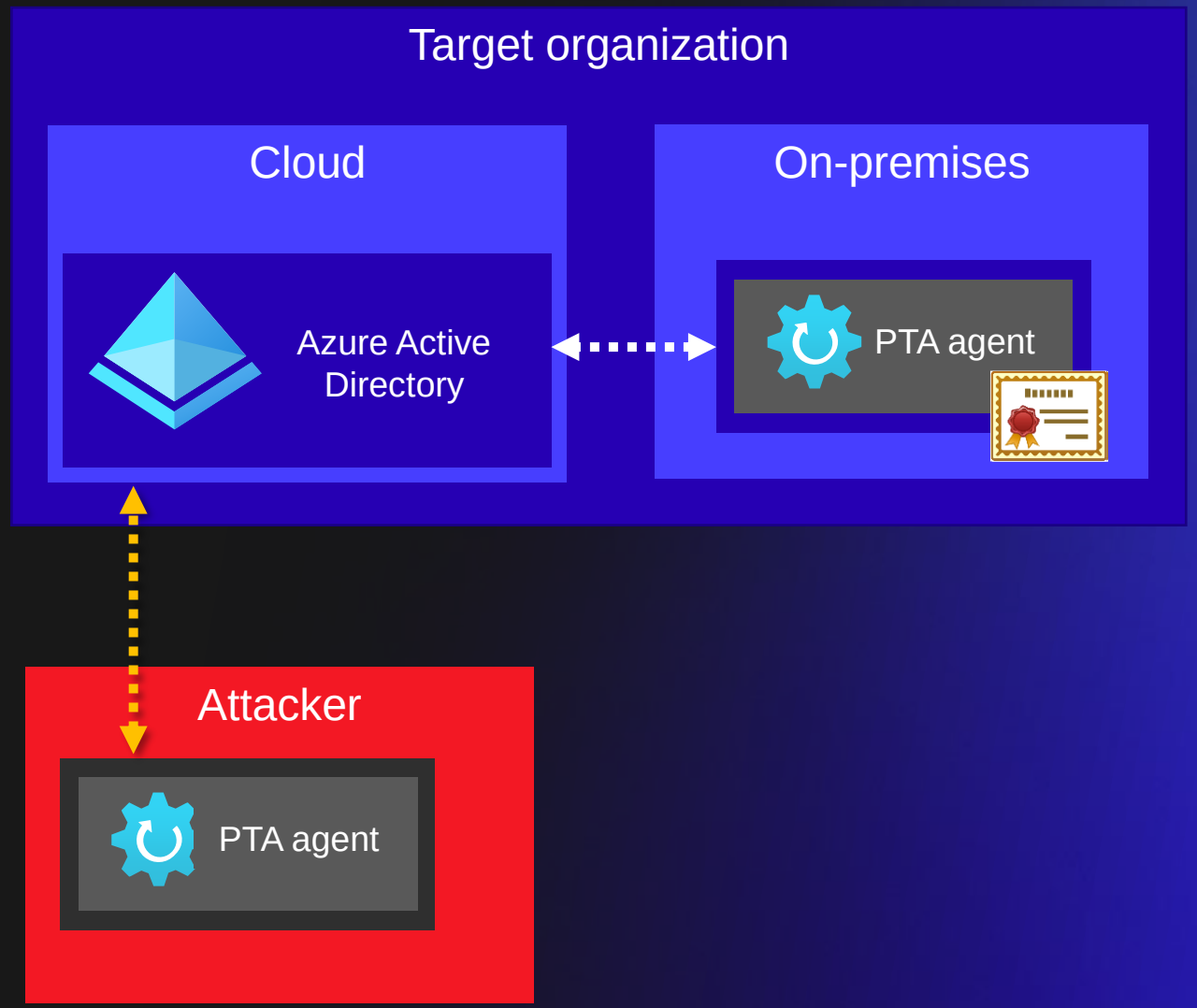
- An object in Azure AD
- Represented by a certificate
  - `Issued to: <tenantid>`
  - `Issued by: HISconnectorRegistrationCA.his.msappproxy.net`




```
id                          : 672843e0-8b25-434f-93e2-5d5071139e09
machineName                 : RSA-DC.aadsecurity.wtf
externalIp                  : 20.106.88.33
status                      : active
supportedPublishingTypes    : {authentication}
```

AADInternals: Stealing PTA agent identity

- Since 2022
- Export PTA agent certificate
  - Requires *local admin* permissions
- Impersonate the PTA agent




I am about to show you how it's done.

Takeaways

- Don’t use PTA
- Treat PTA servers as *Tier 0* servers
- MFA prevents using PTA as a back door *
- Monitor regularly PTA agent:
  - IP changes (AADInternals / MS Graph API)
  - Certificates (PTAAgentDump)
  - Suspicious activity (sign-ins log)
- Contact Microsoft support to remove suspicious agents!

Thank you!

Questions?

Secureworks®