IN CLOUD WE TRUST: COMMON M365 ATTACK TECHNIQUES TO BYPASS DEFENSES

The Most Offensive Con that Ever Offensived – Bypass Edition • Alex Martirosyan

AGENDA

- Whoami
- Cloud Security Risks
- Bypassing the Microsoft Teams splash page
- Conducting Direct Send phishing attacks
- Abusing CDNs and Static Websites
- M365 Defensive Recommendations
- Closing Thoughts

WHOAMI

- 5+ years in offensive security
- IT Audit > Penetration Testing
- Interested in intersection of mathematics and security

Alex Martirosyan,
CRTO , OSCP, GPEN
Lead Penetration Tester, DenSecure
AMartirosyan@wolfandco.com
617.261.8138
https://www.linkedin.com/in/alex-martirosyan/
https://twitter.com/almartiros
https://www.wolfandco.com/services/densecure/

UNDERSTANDING CLOUD SECURITY RISKS

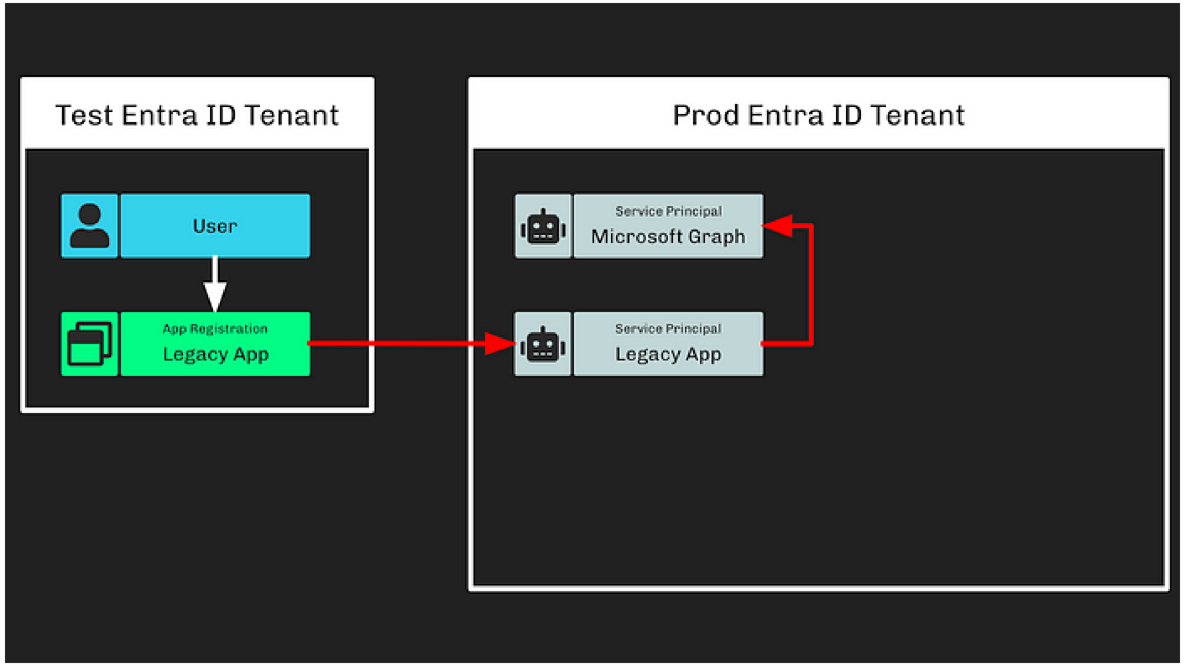
CURRENT LANDSCAPE

CrowdStrike 2023 Global Threat Report Takeaways:

- 71% of attacks were malware-less in 2022
- 50% increase in interactive intrusions (phishing/vishing/etc.)
- Steady increase in “cloud conscious” attack methods
- Average breakout time for interactive intrusion in 2022: 84 minutes

EXAMPLE BREACH

Beginning in late November 2023, the threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold, and then used the account's permissions to access…



https://posts.specterops.io/microsoft-breach-what-happened-what-should-azure-admins-do-da2b7e674ebc

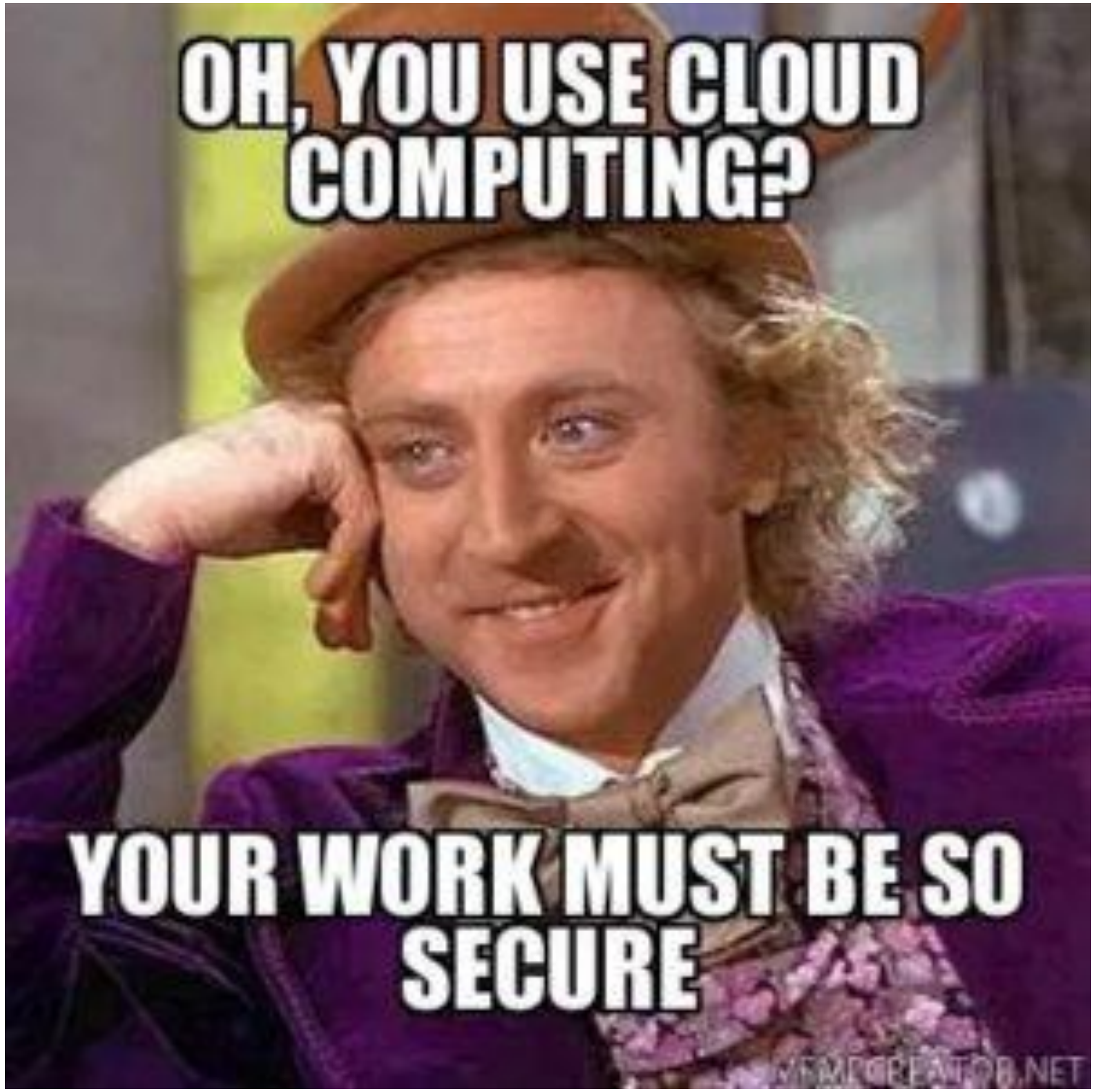
CREDENTIAL THEFT

- In addition to the visibility concerns, think about what an attack can do with credentials for a cloud computing platform.

- What can be accomplished with a compromised credential in a cloud computing environment that differs from an on-prem environment?

CLOUD-SPECIFIC RISKS

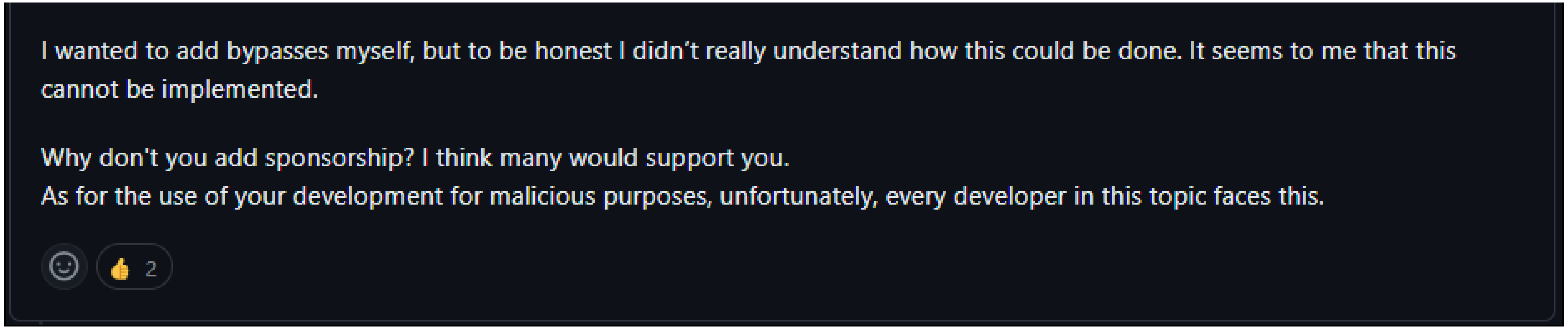
- Reduced Visibility
- Unauthorized Use (Shadow IT)
- Credential Theft
- Vendor Lock-In
- Environment Complexity
- Supply Chain Security



Microsoft Teams Bypass

TEAMS BACKGROUND

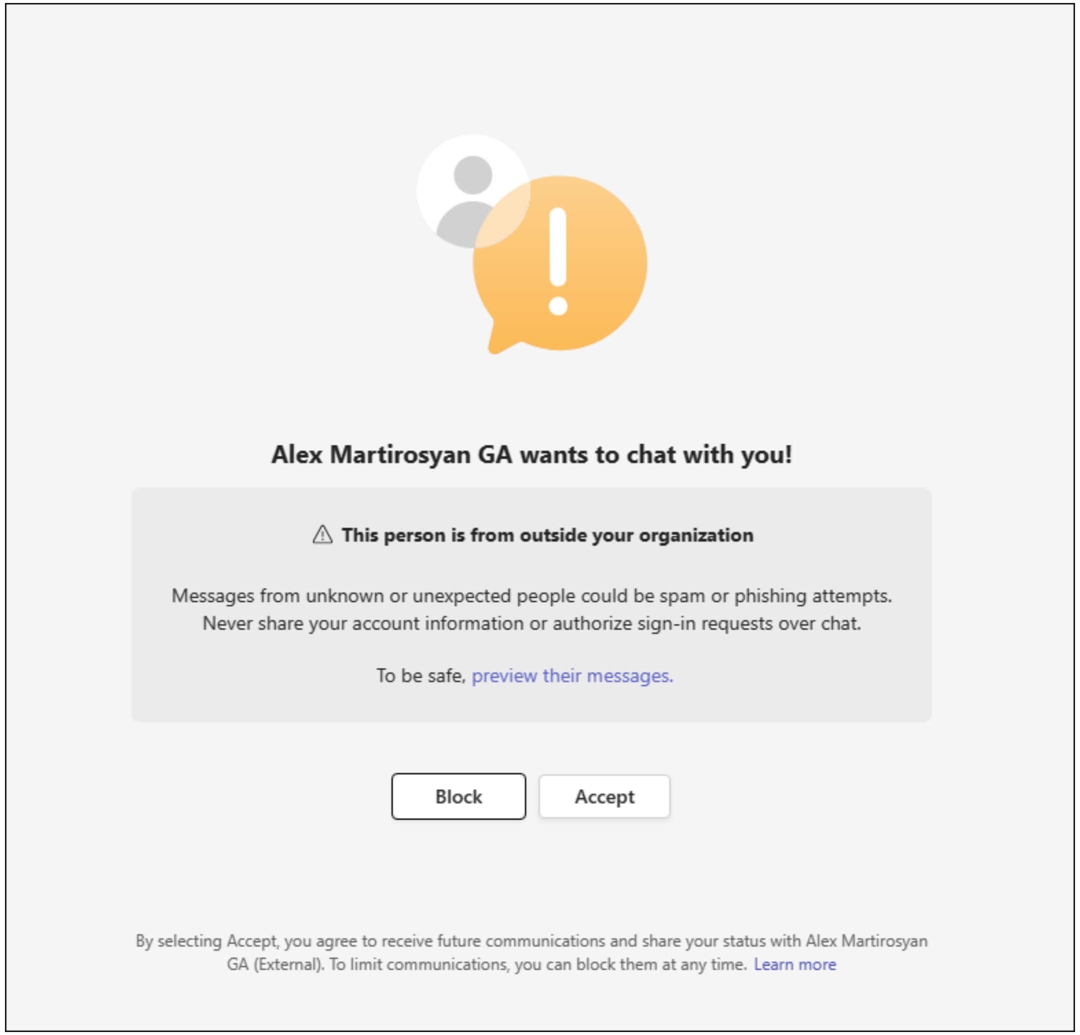
- @pfiatde identified several ways to bypass the initial splash page
- Alex Reid created TeamsPhisher
  - Tool and procedure used by Red Team and APT groups
- Send messages and attachments from external users



I wanted to add bypasses myself, but to be honest I didn’t really understand how this could be done. It seems to me that this cannot be implemented.

Why don't you add sponsorship? I think many would support you.
As for the use of your development for malicious purposes, unfortunately, every developer in this topic faces this.

MESSAGE WARNING



Alex Martirosyan GA wants to chat with you!

⚠ **This person is from outside your organization**

Messages from unknown or unexpected people could be spam or phishing attempts. Never share your account information or authorize sign-in requests over chat.

To be safe, preview their messages.

By selecting Accept, you agree to receive future communications and share your status with Alex Martirosyan GA (External). To limit communications, you can block them at any time. Learn more

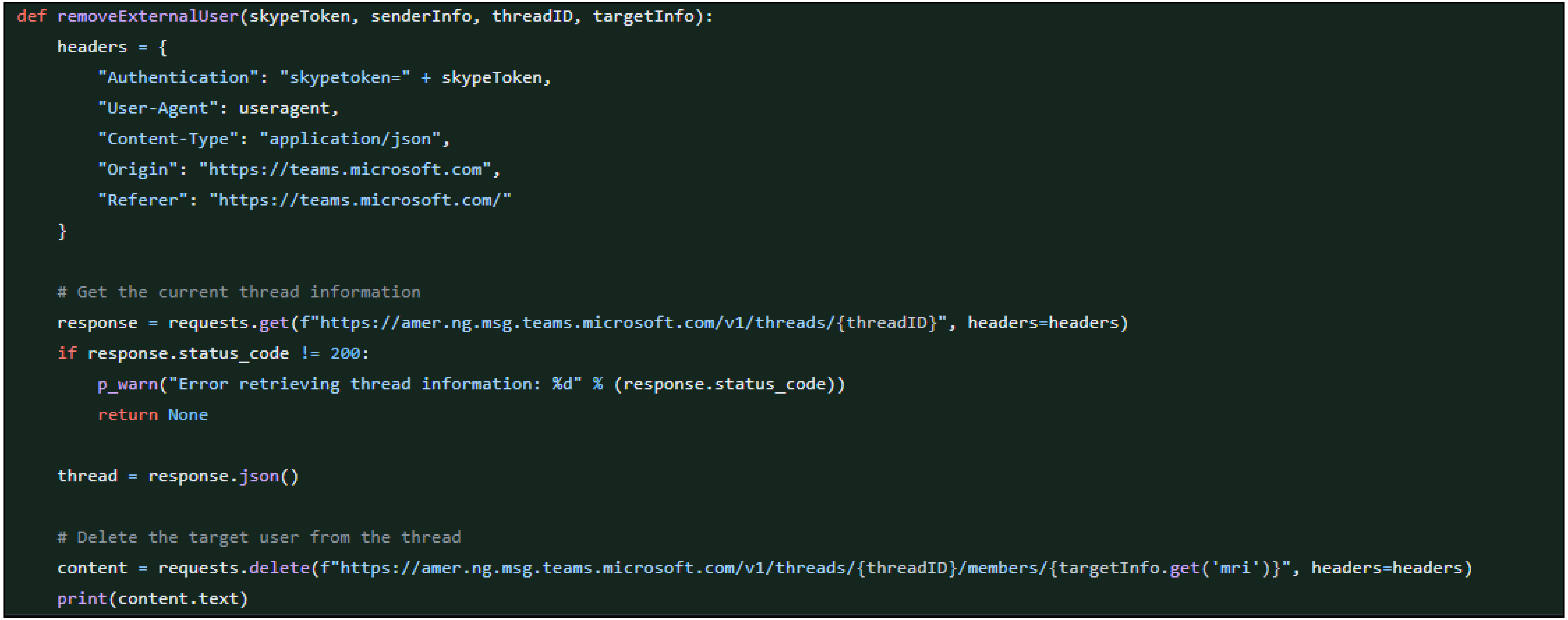
THE BYPASS

- https://badoption.eu/blog/2024/01/12/teams5.html

- Previously:
  - Send a group chat and invite the target twice
  - Send a meeting and message the target

- **<u>WORKING</u>**: Create a group chat and remove user from the chat!

AUTOMATE!



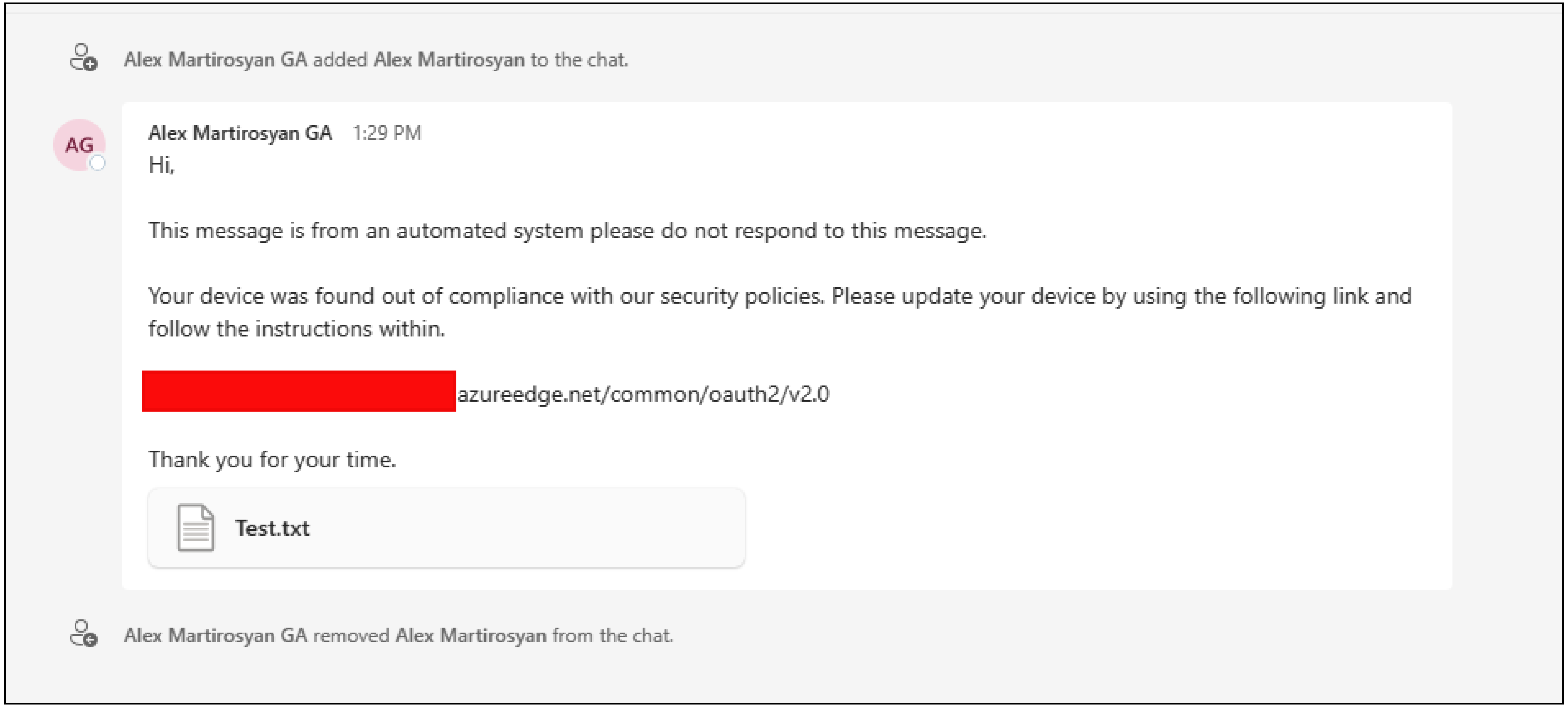
```python
def removeExternalUser(skypeToken, senderInfo, threadID, targetInfo):
    headers = {
        "Authentication": "skypetoken=" + skypeToken,
        "User-Agent": useragent,
        "Content-Type": "application/json",
        "Origin": "https://teams.microsoft.com",
        "Referer": "https://teams.microsoft.com/"
    }

    # Get the current thread information
    response = requests.get(f"https://amer.ng.msg.teams.microsoft.com/v1/threads/{threadID}", headers=headers)
    if response.status_code != 200:
        p_warn("Error retrieving thread information: %d" % (response.status_code))
        return None

    thread = response.json()

    # Delete the target user from the thread
    content = requests.delete(f"https://amer.ng.msg.teams.microsoft.com/v1/threads/{threadID}/members/{targetInfo.get('mri')}", headers=headers)
    print(content.text)
```

INITIAL ACCESS



Alex Martirosyan GA added Alex Martirosyan to the chat.

Alex Martirosyan GA 1:29 PM

Hi,

This message is from an automated system please do not respond to this message.

Your device was found out of compliance with our security policies. Please update your device by using the following link and follow the instructions within.

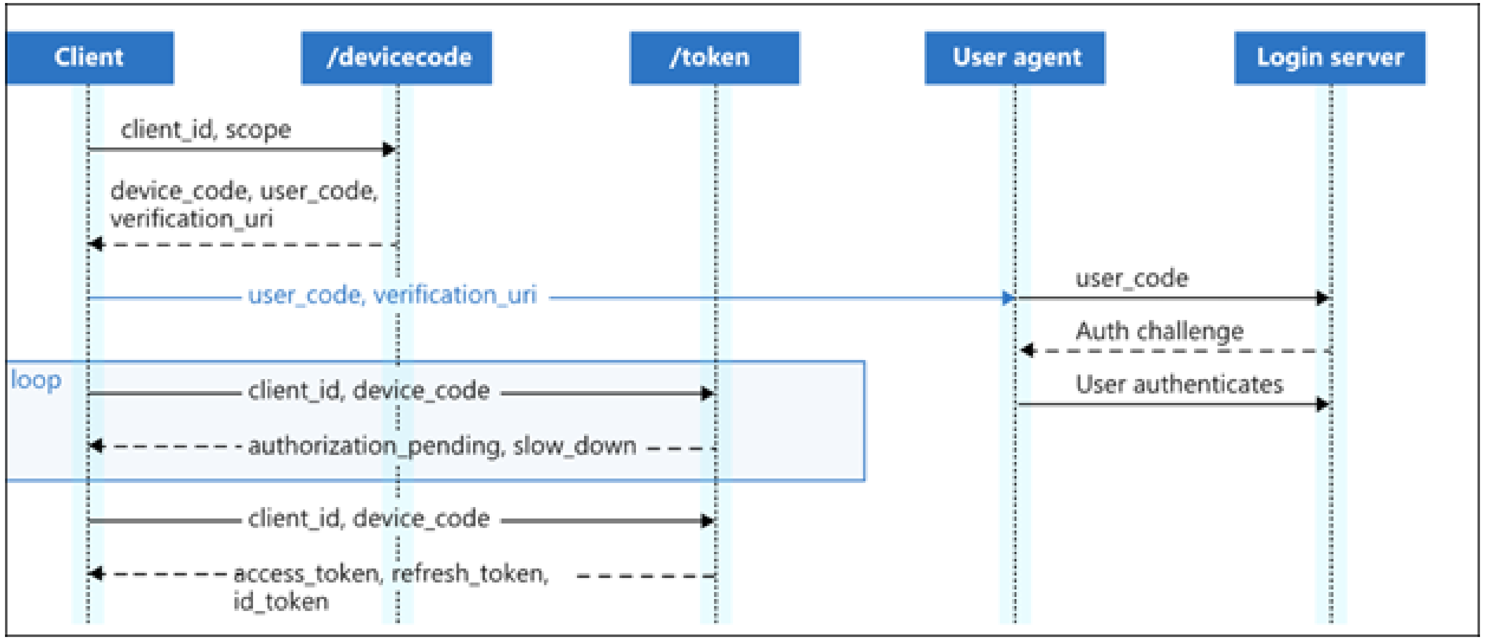
[redacted]azureedge.net/common/oauth2/v2.0

Thank you for your time.

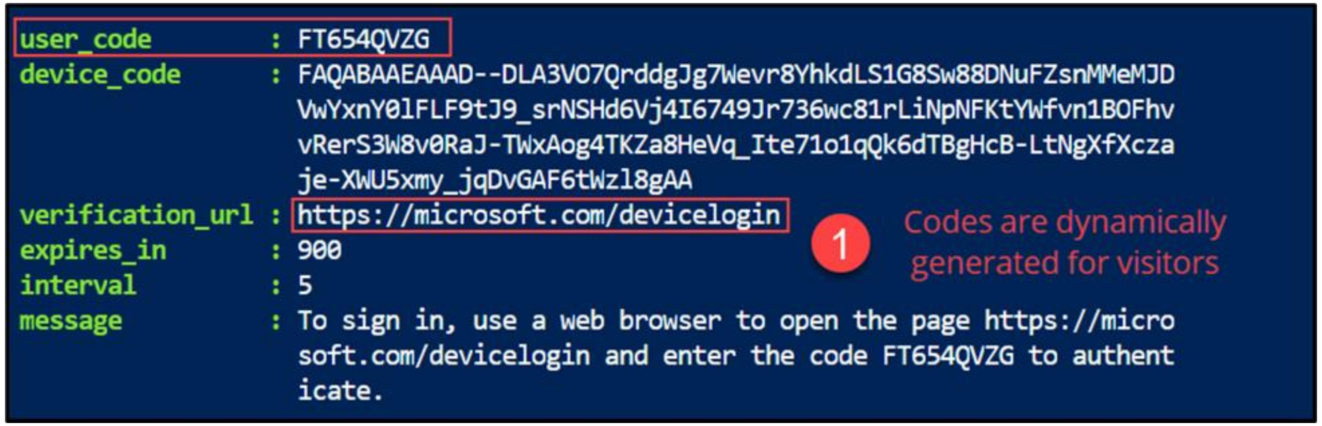
Alex Martirosyan GA removed Alex Martirosyan from the chat.

COMBINE TECHNIQUES

- TeamsPhisher uses Device Code to authenticate the session…

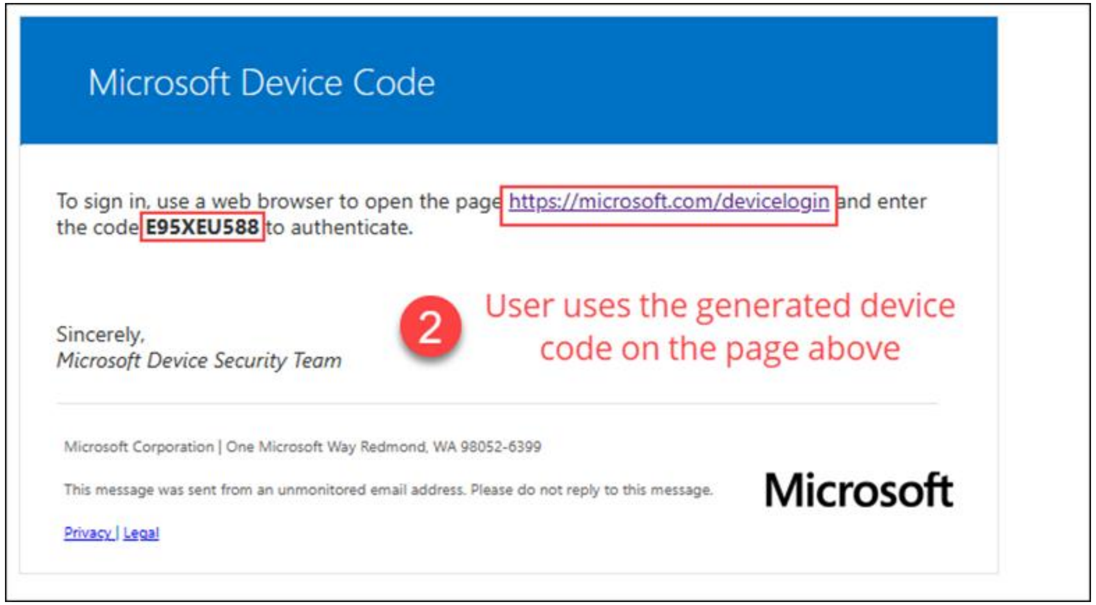


COMBINE TECHNIQUES



```
user_code        : FT654QVZG
device_code      : FAQABAAEAAAD--DLA3VO7QrddgJg7Wevr8YhkdLS1G8Sw88DNuFZsnMMeMJD
                   VwYxnY0lFLF9tJ9_srNSHd6Vj4I6749Jr736wc81rLiNpNFKtYWfvn1BOFhv
                   vRerS3W8v0RaJ-TWxAog4TKZa8HeVq_Ite71o1qQk6dTBgHcB-LtNgXfXcza
                   je-XWU5xmy_jqDvGAF6tWzl8gAA
verification_url : https://microsoft.com/devicelogin
expires_in       : 900
interval         : 5
message          : To sign in, use a web browser to open the page https://micro
                   soft.com/devicelogin and enter the code FT654QVZG to authent
                   icate.
```

1 Codes are dynamically generated for visitors



Microsoft Device Code

To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code **E95XEU588** to authenticate.

Sincerely,
Microsoft Device Security Team

2 User uses the generated device code on the page above

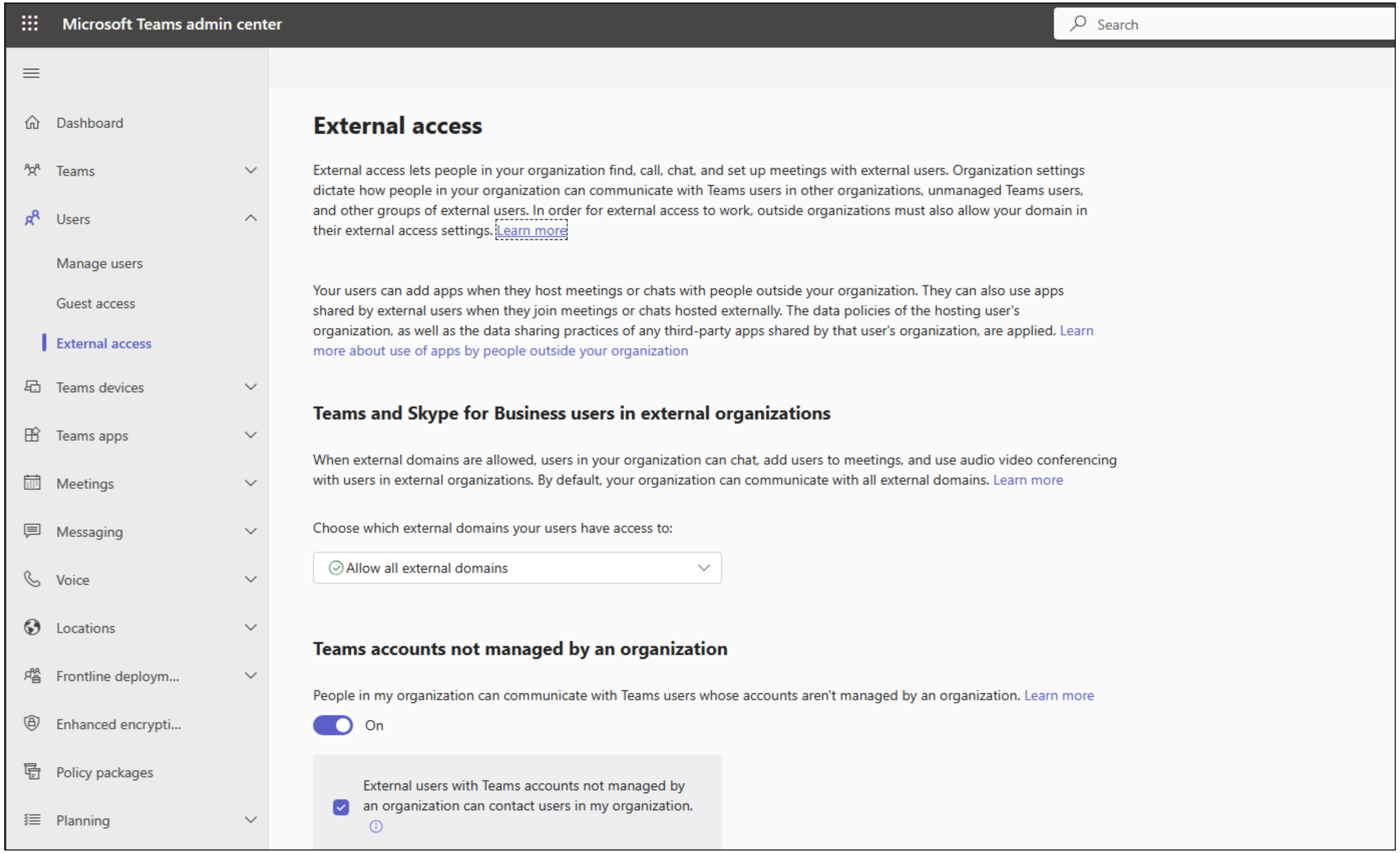
Microsoft Corporation | One Microsoft Way Redmond, WA 98052-6399

This message was sent from an unmonitored email address. Please do not reply to this message.

Microsoft

Privacy | Legal

TEAMS FIX



External access

External access lets people in your organization find, call, chat, and set up meetings with external users. Organization settings dictate how people in your organization can communicate with Teams users in other organizations, unmanaged Teams users, and other groups of external users. In order for external access to work, outside organizations must also allow your domain in their external access settings. Learn more

Your users can add apps when they host meetings or chats with people outside your organization. They can also use apps shared by external users when they join meetings or chats hosted externally. The data policies of the hosting user's organization, as well as the data sharing practices of any third-party apps shared by that user's organization, are applied. Learn more about use of apps by people outside your organization

Teams and Skype for Business users in external organizations

When external domains are allowed, users in your organization can chat, add users to meetings, and use audio video conferencing with users in external organizations. By default, your organization can communicate with all external domains. Learn more

Choose which external domains your users have access to:

Allow all external domains

Teams accounts not managed by an organization

People in my organization can communicate with Teams users whose accounts aren't managed by an organization. Learn more

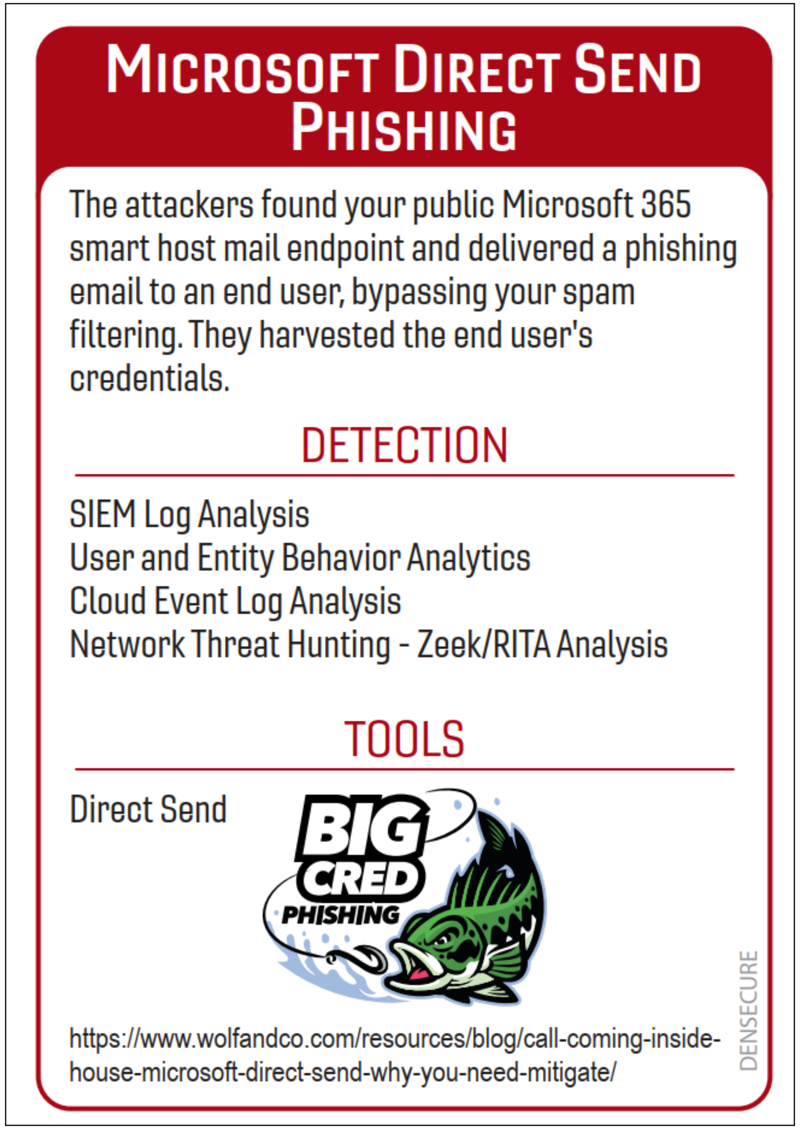
On

☑ External users with Teams accounts not managed by an organization can contact users in my organization.

Direct Send Abuse

BACKGROUND

- Original research by Steve Borosh
- Trivial PowerShell cmdlet to test and spoof emails!
- https://www.blackhillsinfosec.com/spoofing-microsoft-365-like-its-1995/



Microsoft Direct Send Phishing

The attackers found your public Microsoft 365 smart host mail endpoint and delivered a phishing email to an end user, bypassing your spam filtering. They harvested the end user's credentials.

DETECTION

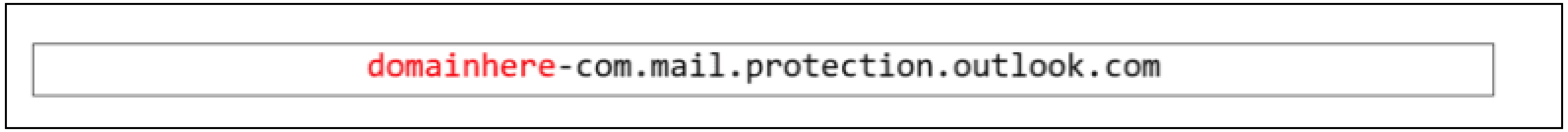
SIEM Log Analysis
User and Entity Behavior Analytics
Cloud Event Log Analysis
Network Threat Hunting - Zeek/RITA Analysis

TOOLS

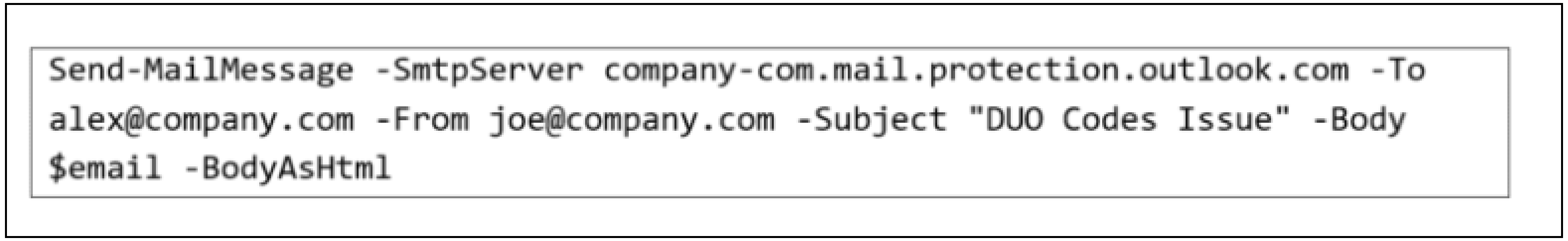
Direct Send

https://www.wolfandco.com/resources/blog/call-coming-inside-house-microsoft-direct-send-why-you-need-mitigate/

BYPASS MAIL GATEWAY



```
domainhere-com.mail.protection.outlook.com
```

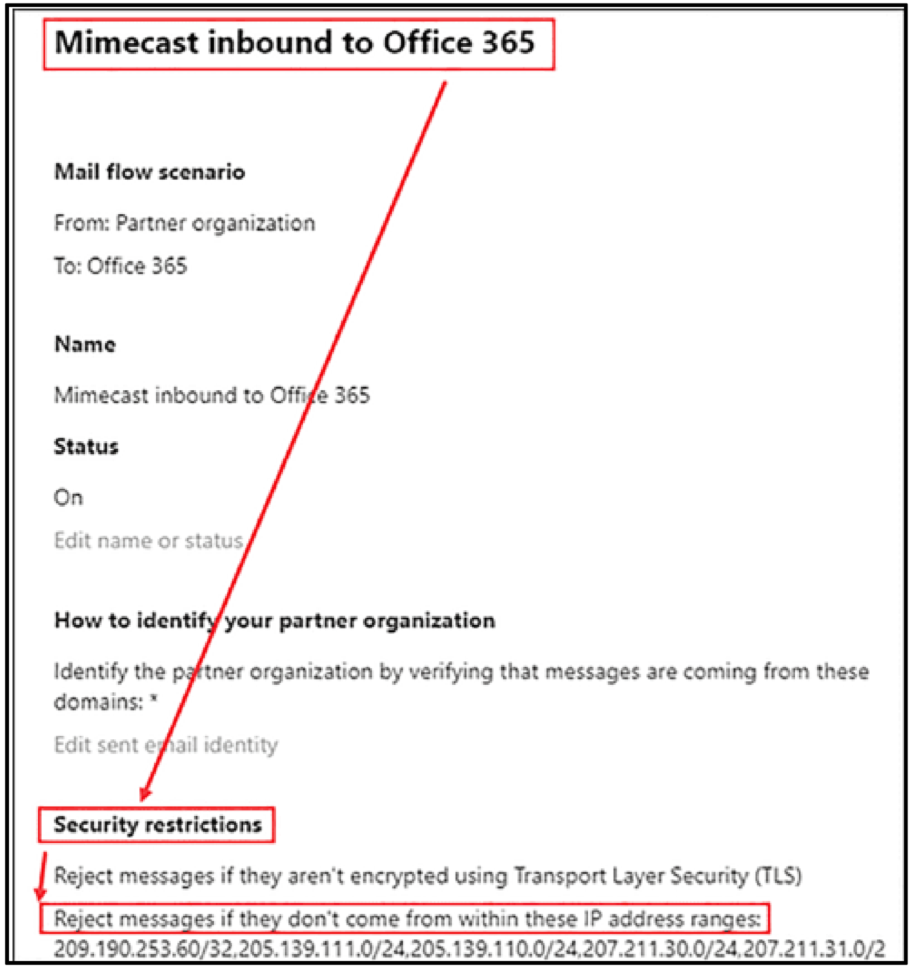


```
Send-MailMessage -SmtpServer company-com.mail.protection.outlook.com -To
alex@company.com -From joe@company.com -Subject "DUO Codes Issue" -Body
$email -BodyAsHtml
```

DIRECT SEND ATTACK

- Spawn an Azure cloud shell
- Identify the correct “smart host”
- Send phishing emails to the target!
  - **Note**: Somewhat of a black box…
  - Results may vary based on pre-text and domains being spoofed

THE FIX



Mimecast inbound to Office 365

Mail flow scenario

From: Partner organization

To: Office 365

Name

Mimecast inbound to Office 365

Status

On

Edit name or status

How to identify your partner organization

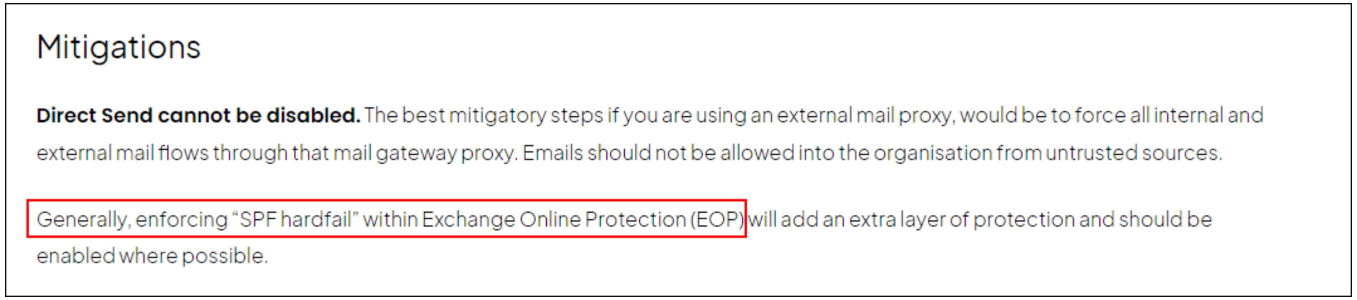
Identify the partner organization by verifying that messages are coming from these domains: *

Edit sent email identity

Security restrictions

Reject messages if they aren't encrypted using Transport Layer Security (TLS)

Reject messages if they don't come from within these IP address ranges:
209.190.253.60/32,205.139.111.0/24,205.139.110.0/24,207.211.30.0/24,207.211.31.0/2



Mitigations

Direct Send cannot be disabled. The best mitigatory steps if you are using an external mail proxy, would be to force all internal and external mail flows through that mail gateway proxy. Emails should not be allowed into the organisation from untrusted sources.

Generally, enforcing "SPF hardfail" within Exchange Online Protection (EOP) will add an extra layer of protection and should be enabled where possible.

https://www.jumpsec.com/guides/microsoft-direct-send-phishing-abuse-primitive/

CDN Abuse

CLOUD CDN

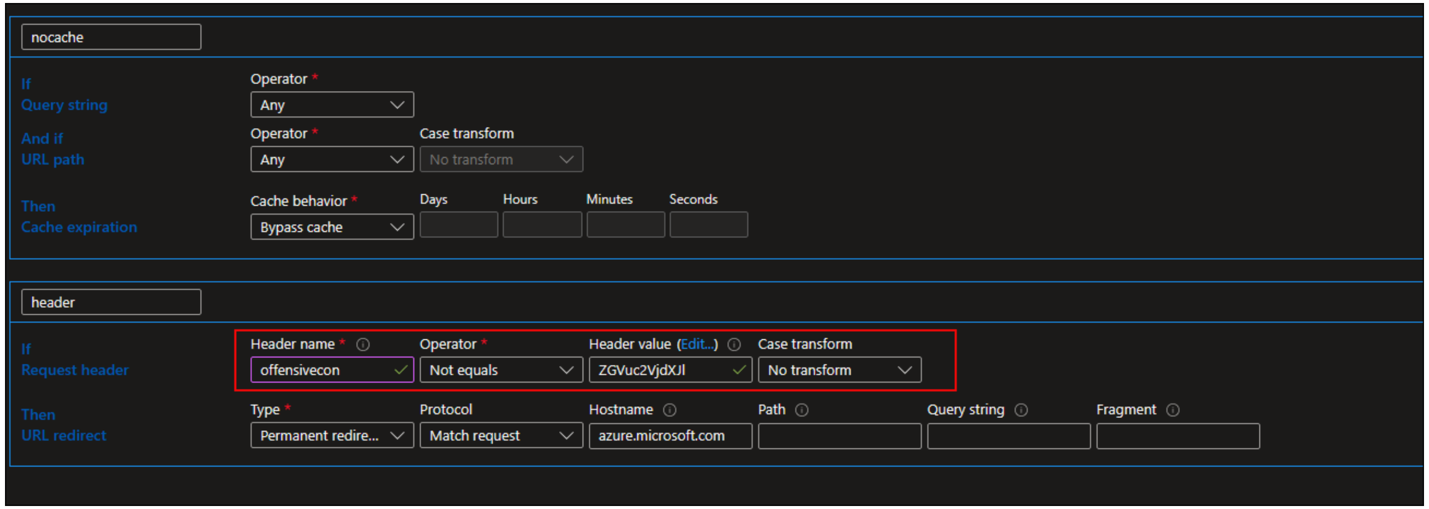
- Already trusted by cloud providers Azure/AWS/etc.
  - azureedge.net
  - cloudfront.net

- Will probably bypass standard web filtering rules

- Use to facilitate social engineering attacks (Teams/Direct Send)

- Use as a redirector for Command and Control!

C2 REDIRECTOR



nocache

If Query string — Operator: Any

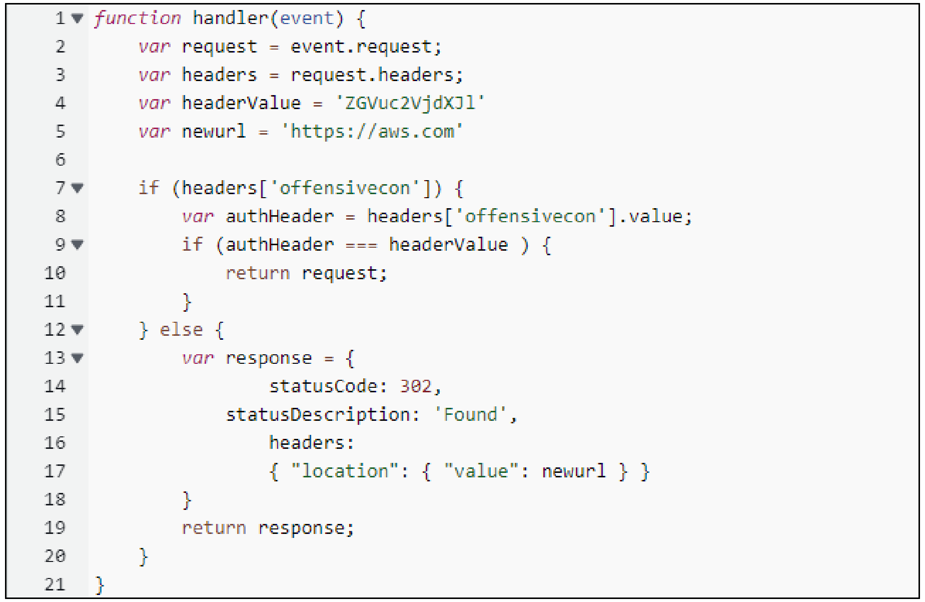
And if URL path — Operator: Any; Case transform: No transform

Then Cache expiration — Cache behavior: Bypass cache; Days; Hours; Minutes; Seconds

header

If Request header — Header name: offensivecon; Operator: Not equals; Header value (Edit...): ZGVuc2VjdXJl; Case transform: No transform

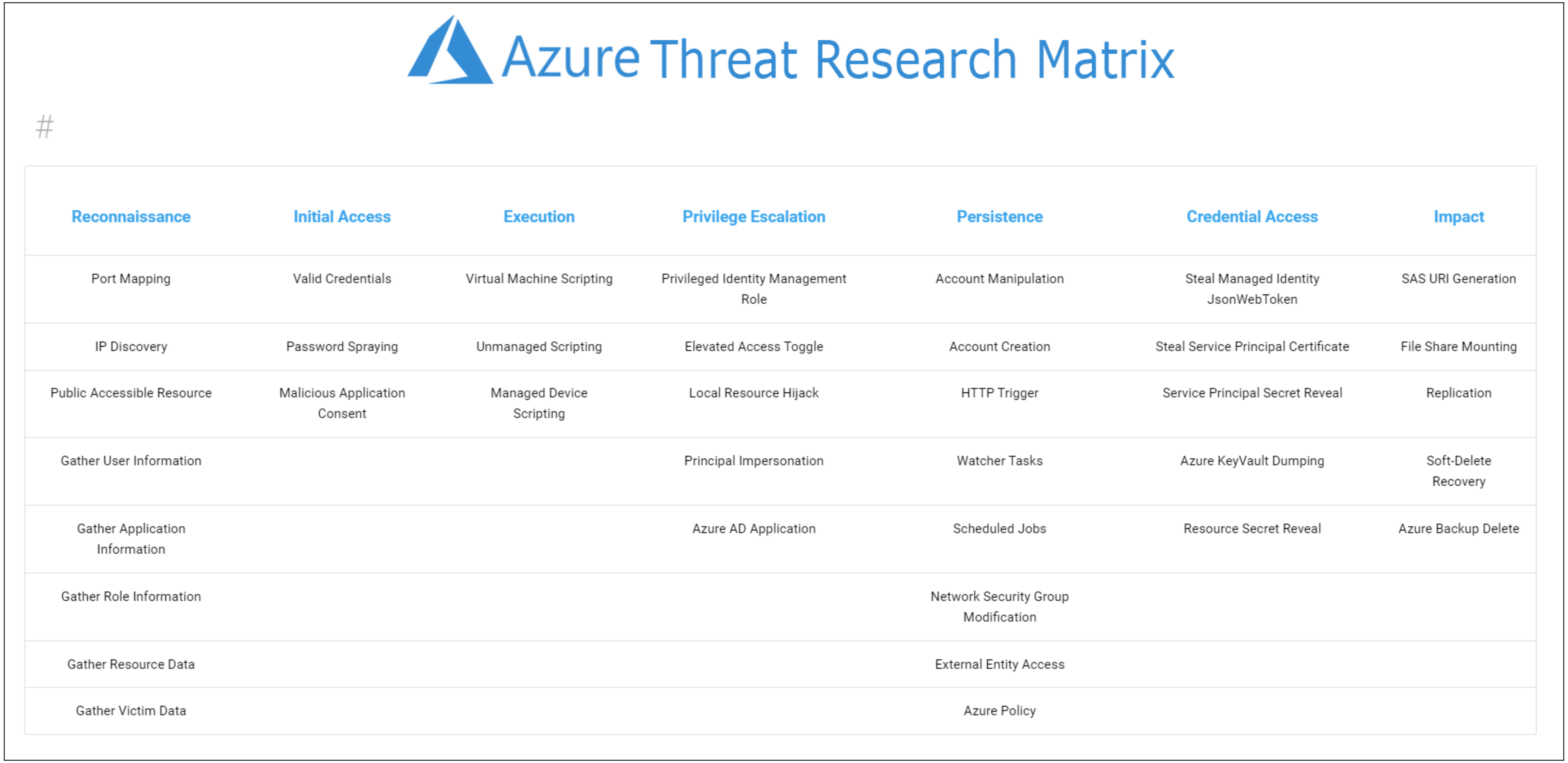
Then URL redirect — Type: Permanent redire...; Protocol: Match request; Hostname: azure.microsoft.com; Path; Query string; Fragment



```
function handler(event) {
    var request = event.request;
    var headers = request.headers;
    var headerValue = 'ZGVuc2VjdXJl'
    var newurl = 'https://aws.com'

    if (headers['offensivecon']) {
        var authHeader = headers['offensivecon'].value;
        if (authHeader === headerValue ) {
            return request;
        }
    } else {
        var response = {
                statusCode: 302,
            statusDescription: 'Found',
                headers:
                { "location": { "value": newurl } }
        }
        return response;
    }
}
```

LEARN FROM OTHERS



Azure Threat Research Matrix

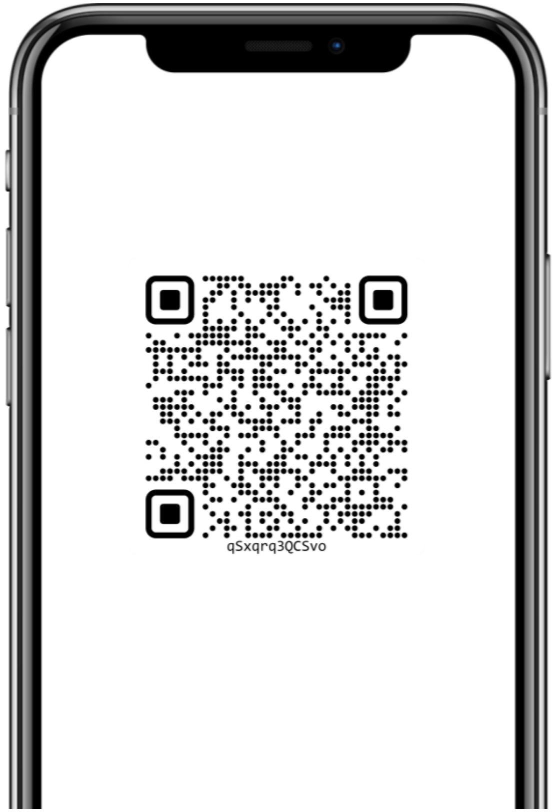
#

Reconnaissance	Initial Access	Execution	Privilege Escalation	Persistence	Credential Access	Impact
Port Mapping	Valid Credentials	Virtual Machine Scripting	Privileged Identity Management Role	Account Manipulation	Steal Managed Identity JsonWebToken	SAS URI Generation
IP Discovery	Password Spraying	Unmanaged Scripting	Elevated Access Toggle	Account Creation	Steal Service Principal Certificate	File Share Mounting
Public Accessible Resource	Malicious Application Consent	Managed Device Scripting	Local Resource Hijack	HTTP Trigger	Service Principal Secret Reveal	Replication
Gather User Information			Principal Impersonation	Watcher Tasks	Azure KeyVault Dumping	Soft-Delete Recovery
Gather Application Information			Azure AD Application	Scheduled Jobs	Resource Secret Reveal	Azure Backup Delete
Gather Role Information				Network Security Group Modification		
Gather Resource Data				External Entity Access		
Gather Victim Data				Azure Policy		

BACKDOORS & BREACHES

https://spearphish-general-store.myshopify.com/collections/backdoors-breaches-incident-response-card-game

QUESTIONS



Alex Martirosyan,
CRTO , OSCP, GPEN
Lead Penetration Tester, DenSecure
AMartirosyan@wolfandco.com
617.261.8138
https://www.linkedin.com/in/alex-martirosyan/
https://twitter.com/almartiros
https://www.wolfandco.com/services/densecure/

ABOUT WOLF & COMPANY, P.C.

1911 WOLF & CO. ESTABLISHED

300+ PROFESSIONALS

3 OFFICES IN:

- ✓ Boston, MA
- ✓ Springfield, MA
- ✓ Livingston, NJ

SERVICES OFFERED IN:

- ✓ Audit
- ✓ Tax
- ✓ Risk Management

ABOUT WOLF & COMPANY, P.C.

111

YEARS IN BUSINESS

- Established in 1911
- Built on quality and integrity
- Succession strategy to remain independent allows us to be with you throughout your business lifecycle

300+

EXPERIENCED, HIGHLY TRAINED PROFESSIONALS

- Lower-than-industry-average staff turnover means a consistent team structure year after year
- Niche team dedicated to your industry

RESOURCES TO LEARN MORE

- Cultures & Values
- Inclusion & Diversity
- Our History
- Social Responsibility
- Thought Leadership
- Wolf Global

Wolf & Company ranked

#2 BEST LARGE FIRM TO WORK FOR

nationwide

accountingTODAY

WOLF & COMPANY, P.C.

den secure by wolf & company, p.c.

ABOUT WOLF & COMPANY, P.C.

SERVICES WE OFFER

We combine industry expertise with service specialization to provide your organization with insight, opportunities, and solutions allowing you to address your unique business needs.

ADVISORY

- Business Continuity Planning
- Cybersecurity
- Enterprise Risk Management
- Environment, Social & Governance
- Internal Audit
- IT Audit
- Model Risk Management
- Outsourced Accounting Solutions
- Penetration Testing
- Regulatory Compliance
- Strategic Planning

ASSURANCE

- Employee Benefit Plan Audits
- Financial Statements Audits
- HITRUST
- PCI DSS
- SOC Reporting

TAX

- Business Tax
- Federal
- International
- State & Local
- Private Client Group

vSUITE

- Virtual Consulting Services
  - Business Continuity Planning (BCP)
  - Virtual Chief Information Security Officer (vCISO)
  - Virtual Chief Privacy Officer (vCPO)
  - Virtual Chief Risk Officer (vCRO)
  - Virtual Vendor Management

WOLFPAC

- Integrated risk management SaaS suite

WOLF & COMPANY, P.C.

den secure by wolf & company, p.c.

WOLF ACCOLADES

Wolf is pleased to have received recognition from a variety of sources for our efforts at providing responsive client service and development of our professionals. Examples of this recognition include:

INSIDE Public Accounting

TOP 100
Accounting Firms

accountingTODAY

TOP 100
Accounting Firms

#2 BEST LARGE FIRM to
Work For Nationwide

TOP FIRMS:
New England

BOSTON BUSINESS JOURNAL

- ✓ Area's Best Places to Work
- ✓ Area's Most Admired Companies
- ✓ Area's Fastest Growing Private Companies
- ✓ Area's Largest I.T. Consulting Firms

Forbes

America's Best
Tax and Accounting
Firms of 2023, 2021

ABOUT DENSECURE

Wolf & Company's IT Assurance & Advisory team of cybersecurity experts, DenSecure™, brings together extensive technical knowledge and industry experience with internationally-recognized frameworks to develop strong cybersecurity programs.

DenSecure's core services include:

- Red Team Assessment
- Application Penetration Testing
- Network Penetration Testing
- Social Engineering
- Threat Emulation
- Assumed Breach Testing

Back to Home ⟶