



# THE SEVEN DEADLY SINS

Major security failures of companies from the perspective of InfoGuard's CSIRT

# 1. SIN

## LACK OF PATCH MANAGEMENT

**ZDNet**



AFRICA

UK

ITALY


SPAIN

MORE ▼

NEWSLETTERS

ALL WRITERS

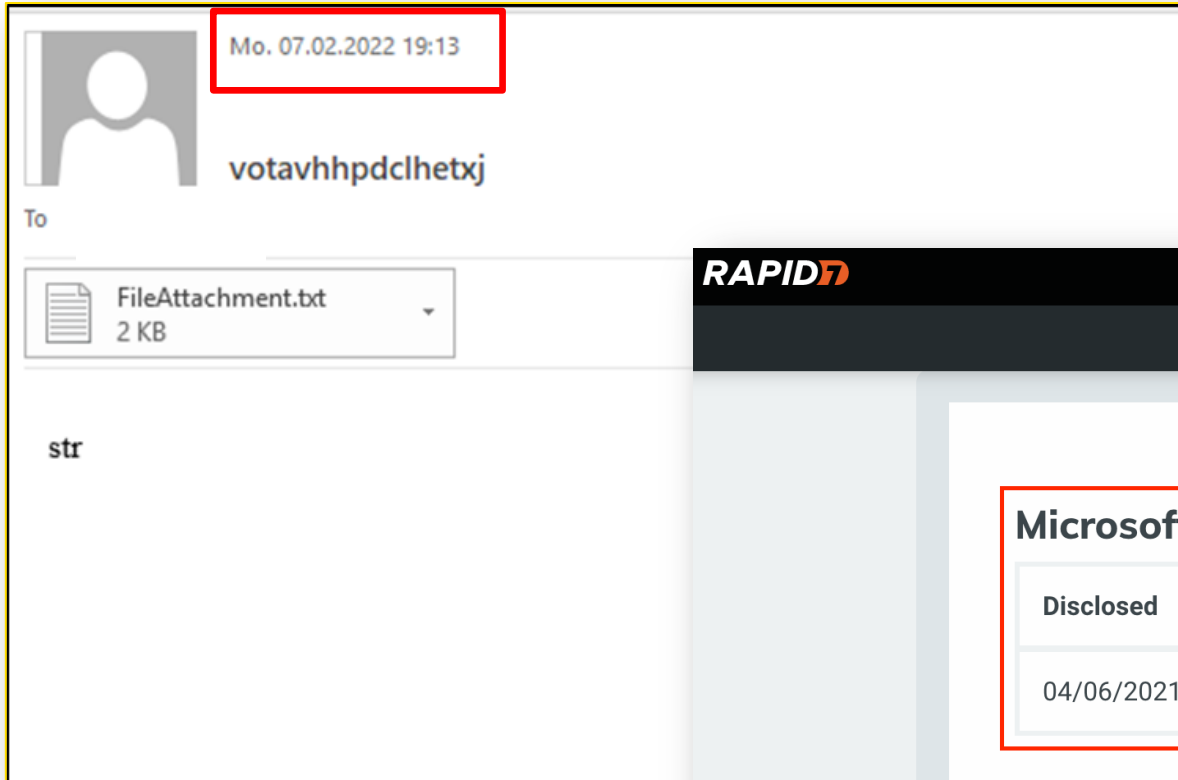


 MUST READ: [Ransomware: Russia told to tackle cyber criminals operating from within its borders](#)

## Cybercriminals scanned for vulnerable Microsoft Exchange servers within five minutes of news going public

Research suggests the cheap hire of cloud services has allowed cyberattackers to quickly pick out targets.

# PARTLY VULNERABLE FOR MONTHS



**RAPID7** PRODUCTS ▾ SERVICES ▾ SUPPORT & RESOURCES ▾ RESEARCH

## Microsoft Exchange ProxyShell RCE

Disclosed	Created
04/06/2021	08/19/2021

### Description

This module exploits a vulnerability on Microsoft Exchange Server that allows an attacker to bypass the authentication (CVE-2021-31207), impersonate an arbitrary user (CVE-2021-34523) and write an arbitrary file (CVE-2021-34473) to achieve the RCE (Remote Code Execution). By taking advantage of this vulnerability, you can execute arbitrary commands on the remote Microsoft Exchange Server. This vulnerability affects Exchange



# FREELY AVAILABLE EXPLOIT CODE

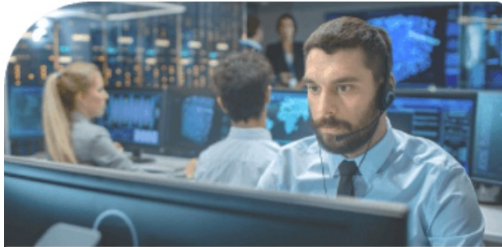
github.com/horizon3ai/proxyshell/blob/master/exchange\_proxyshell.py

```

200
201 class ProxyShell:
202
203     def __init__(self, exchange_url, email, verify=False):
204
205         self.email = None
206         self.emails = []
207         self.exchange_url = exchange_url if exchange_url.startswith('https://') else f'https://{exchange_url}'
208         self.rand_email = f'{rand_string()}@{rand_string()}.{rand_string(3)}'
209         self.sid = None
210         self.legacydn = None
211         self.legacvdns = []
212         self.rand_subj = rand_string(16)
213         self.target_be = None
214         self.servers = {}
215         self.version = None
216         self.versions = {'Exchange2016'}
217         self.domain = None
218         self.domains = set()
219

```

fortiguard.com/psirt/FG-IR-22-377



IR Number	FG-IR-22-377
Date	Oct 10, 2022
Severity	● ● ● ● ● Critical
CVSSv3 Score	9.6
Impact	Execute unauthorized code or commands
CVE ID	CVE-2022-40684
Affected Products	FortiOS : 7.2.1, 7.2.0, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0 FortiProxy : 7.2.0, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0

## PSIRT Advisories

### FortiOS / FortiProxy / FortiSwitchManager - Authentication bypass on administrative interface

#### Summary

An authentication bypass using an alternate path or channel vulnerability [CWE-288] in FortiOS, FortiProxy and FortiSwitchManager may allow an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests.

#### Exploitation Status:

Fortinet is aware of an instance where this vulnerability was exploited, and recommends immediately validating your systems against the following indicator of compromise in the device's logs:

`user="Local_Process_Access"`

horizon3ai / CVE-2022-40684 Public

[Code](#) [Pull requests](#) [Actions](#) [Projects](#) [Security](#) [Insights](#)

History for CVE-2022-40684 / CVE-2022-40684.py

○ Commits on Oct 13, 2022

**Add POC and readme**

zach committed 3 days ago

○ End of commit history for this file



**Florian Roth** ⚡ @cyb3rops · 5h



Public Twitter List "Cyber"

- my curated list of of cyber security experts with high signal to noise ratio
- 195 members, 11k followers
- use this list if your main feed is too noisy
- tip: use it as a separate panel in [tweetdeck.twitter.com](https://tweetdeck.twitter.com)

[twitter.com/i/lists/201875...](https://twitter.com/i/lists/201875...)

# PATCHING



**SophosLabs** @SophosLabs · Jun 22



Conclusions:

There are likely many latent ProxyLogon and/or ProxyShell breaches that are currently unknown.

The fact is that for both vulnerabilities, patching does not remove existing web shells, it only removes the vulnerability. 9/12



**SophosLabs** @SophosLabs · Jun 22



Widespread, easy to exploit vulnerabilities like ProxyLogon and ProxyShell are two prime examples of why organizations need to prioritize patching of exposed services or move to cloud services (where patching is done automatically). 10/12



# EMERGENCY PATCHES



## **2. SIN**

**LACK OF MULTI-FACTOR  
AUTHENTICATION**

# BUSINESS EMAIL COMPROMISE

2021 INTERNET CRIME REPORT

9

## THREAT OVERVIEWS FOR 2021

### BUSINESS EMAIL COMPROMISE (BEC)



In 2021, the IC3 received 19,954 Business Email Compromise (BEC)/ Email Account Compromise (EAC) complaints with adjusted losses at nearly \$2.4 billion. BEC/EAC is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

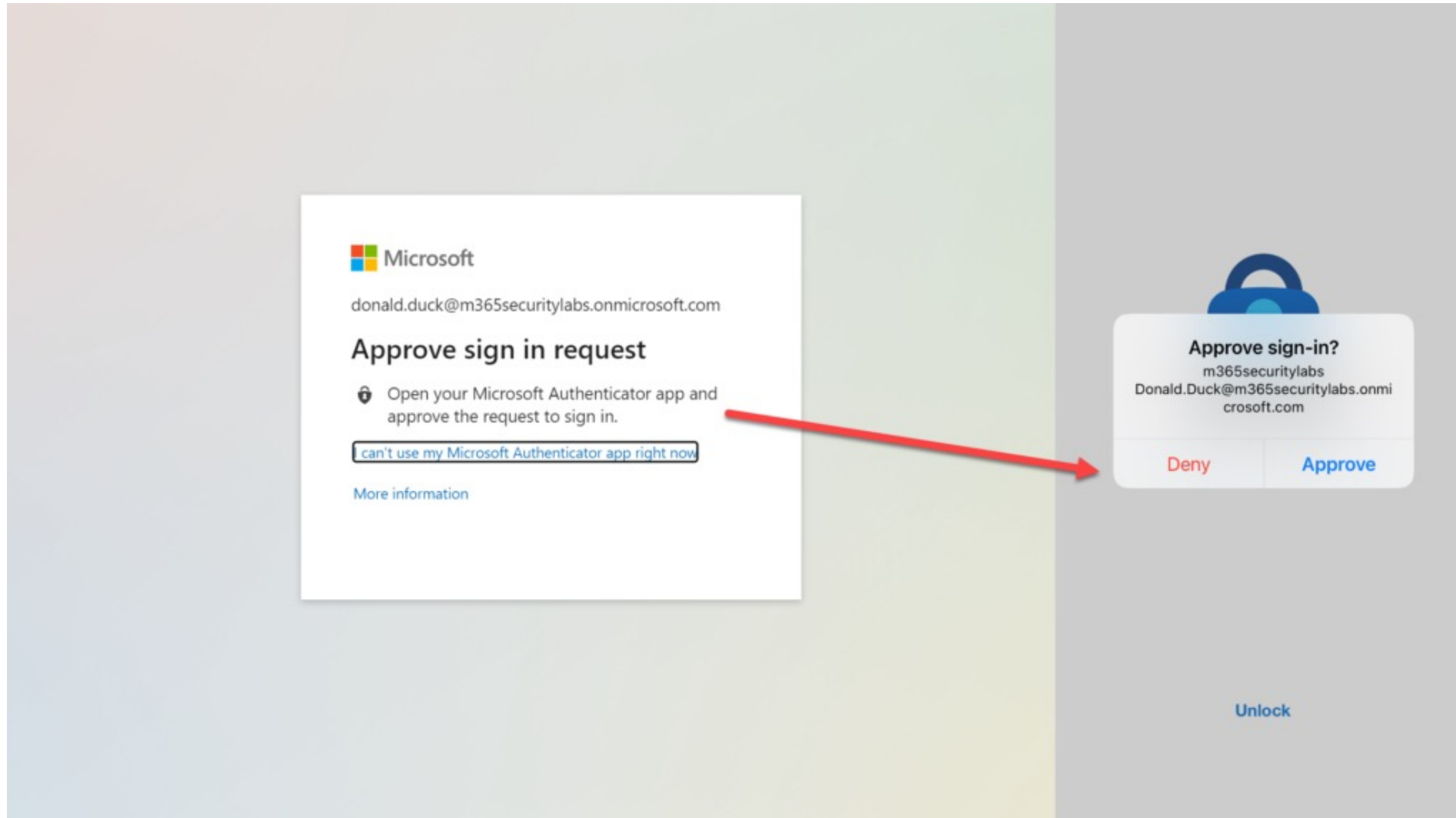
# MFA – MFA – MFA

---





# BYPASSING MFA





## BYPASSING MFA

### LAPSUS\$ Chat

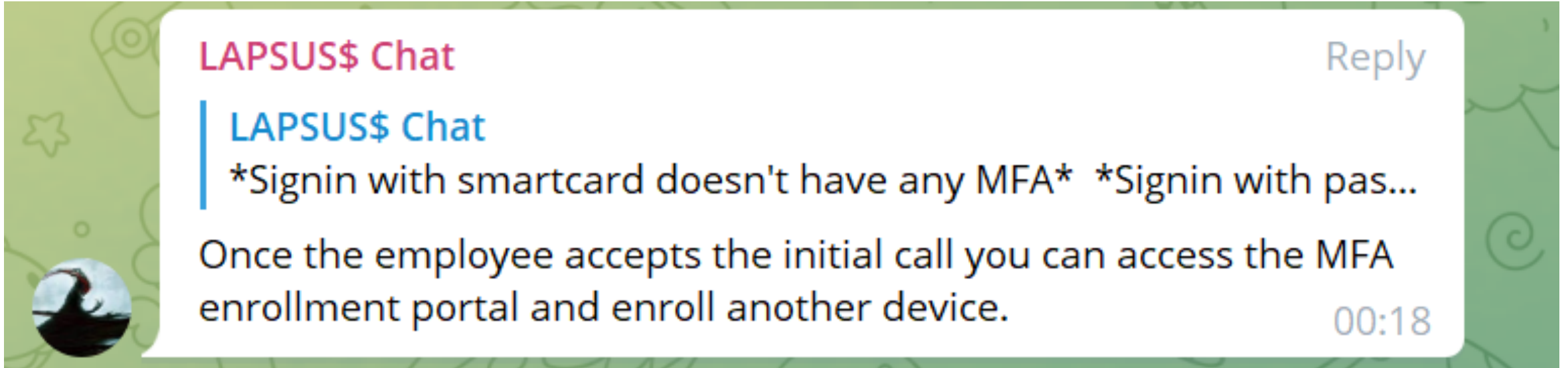
they must have some mfa right?

\*Signin with smartcard doesn't have any MFA\*

\*Signin with password will issue MFA through a phone call or authentication app. - However no limit is placed on the amount of calls that can be made, call the employee 100 times at 1am while he is trying to sleep and he will more than likely accept it\*

edited 00:17

# BYPASSING MFA



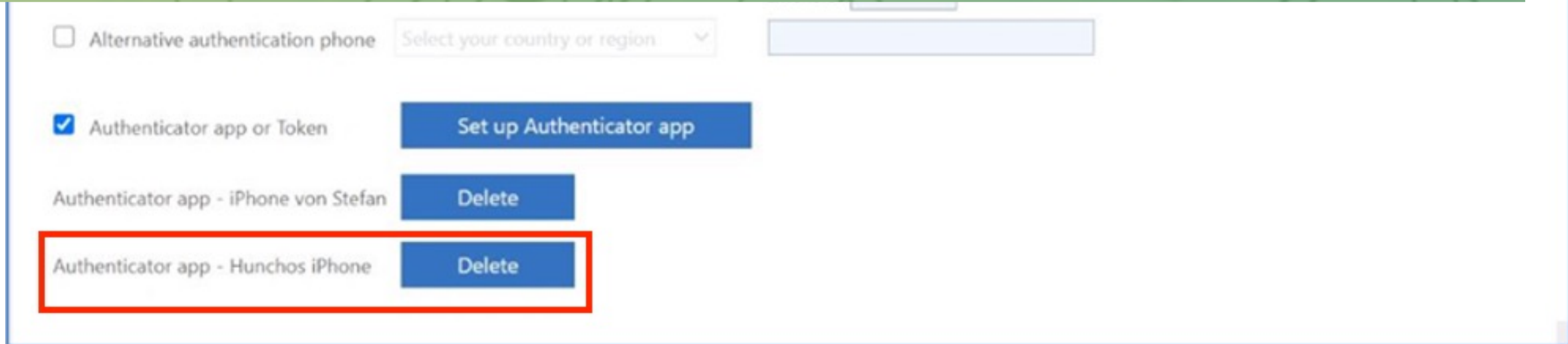
**LAPSUS\$ Chat** Reply

**LAPSUS\$ Chat**

\*Signin with smartcard doesn't have any MFA\* \*Signin with pas...

Once the employee accepts the initial call you can access the MFA enrollment portal and enroll another device.

00:18



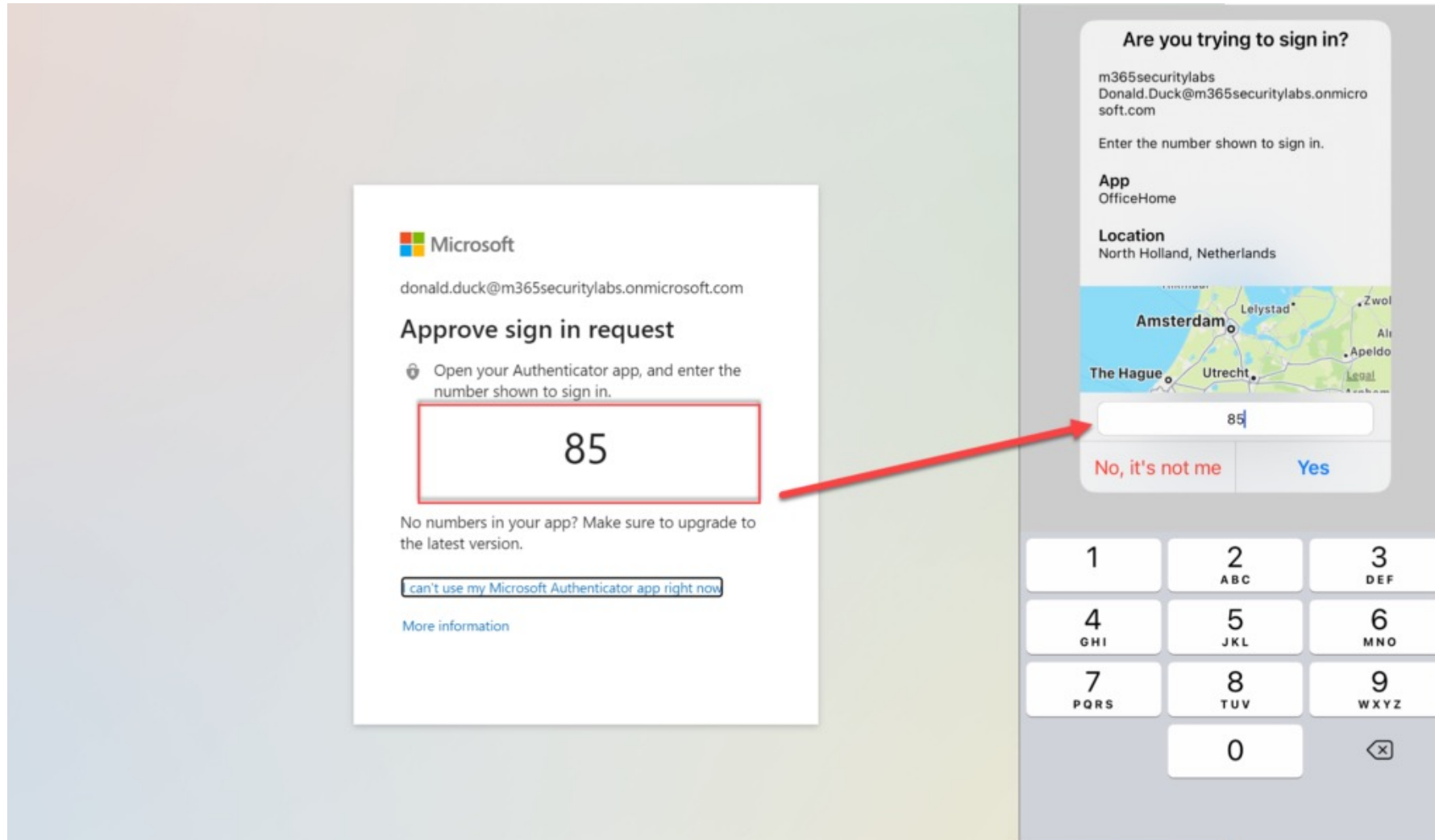
Alternative authentication phone

Authenticator app or Token

Authenticator app - iPhone von Stefan

**Authenticator app - Hunchos iPhone**

# IMPROVED MFA

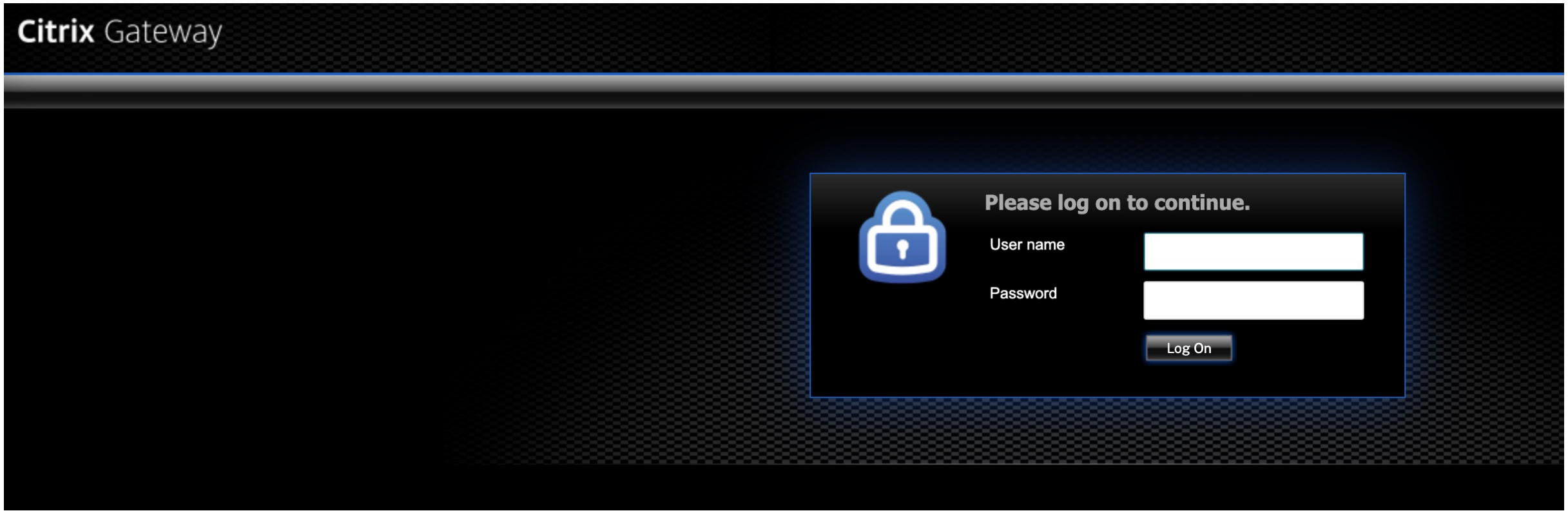


# VPN MFA

**PROTECTING THE GATEWAY TO THE  
KINGDOM**



# REMOTE ACCESS





## **3. SIN**

**IGNORING AV-MESSAGES**

# HIGH RISK KEYWORDS

## Antivirus Event Analysis Cheat Sheet

Version 1.7.2

Florian Roth @cyb3rops



Attribute	Less Relevant	Relevant	Highly Relevant		
<b>Virus Type</b>	HTML Iframe Keygen Joke Adware Clickjacking Crypto FakeAV	Trojan Backdoor Agent Malware JS Creds PS PowerShell Exploit Ransom	PassView Tool-Netcat Tool-Nmap RemAdm NetTool Crypto Scan	HackTool HTool HKTL PWCrack SecurityTool Clearloqs PHP/BackDoor ASP/BackDoor JSP/BackDoor Backdoor.PHP	CobaltStrike Keylogger MeteTool Meterpreter Metasploit PowerSSH Mimikatz PowerSploit PSWTool PWDump

# ONE OF THESE HIGH RISK KEYWORDS

Hallo zusammen,

heute Nacht zwischen 21:08 und 21:35 gingen 5 Antimalware Warnungen bei uns ein.  
Die Warnungen betreffen ausschließlich den Server „...“.

Gemäß Windows Defender Antivirus handelte es sich dabei um folgende Hack Tools:

<https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=HackTool%3aWin32%2fMimikatz.D&threatid=2147729891&enterprise=0>

<https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=HackTool%3aPowerShell%2fPsAttack.A&threatid=2147722658&enterprise=0>

Normalerweise wird der Defender mit der Bedrohung klar kommen.

Da es sich bei dem System um einen DC handelt und wir darauf keinen Zugriff haben, bitten wir Sie auf dem betroffenen Server nochmals einen Fullscan durchzuführen.

Teilen Sie uns bitte das Ergebnis mit.

# ASSESSMENT OF INFECTIONS

Collection	Threat Name	Severity	Threat Category	Collection Member Count	Computers Infected
All Desk...	Program:Win32/Contebrew.A!ml	High	Potential Unwan...	479	1
All Syste...	Program:Win32/Contebrew.A!ml	High	Potential Unwan...	496	1
COL_AM...	Program:Win32/Contebrew.A!ml	High	Potential Unwan...	271	1
All Desk...	Behavior:Win32/CobaltStrike.D!sms	Severe	Behavior	479	1
All Syste...	Behavior:Win32/CobaltStrike.D!sms	Severe	Behavior	496	1
COL_AM...	Behavior:Win32/CobaltStrike.D!sms	Severe	Behavior	271	1
All Desk...	Trojan:Win32/Sabsik.FL.A!ml	Severe	Trojan	479	1
All Syste...	Trojan:Win32/Sabsik.FL.A!ml	Severe	Trojan	496	1
COL_AM...	Trojan:Win32/Sabsik.FL.A!ml	Severe	Trojan	271	1



# 4. SIN

# AD HARDENING



# PASSWORDS IN THE GPO

## Obfuscated Passwords

The password in GPO are obfuscated, not encrypted. Consider any passwords listed here as compromised and change it immediately.

Show  entries

Search:

GPO Name ↑↓	Password origin ↑↓	UserName ↑↓	Password ↑↓	Changed ↑↓
allgemeine_Client_Einstellungen ?	groups.xml	support	Help [REDACTED]	2013-11-13 17:09:02Z
allgemeine_Client_Einstellungen ?	groups.xml	ladmin	Sw1s [REDACTED]	2013-11-13 17:34:36Z

## Domain Administrators

### Direct User Members

Show  entries

SamAccountName ↑↓	Enabled ↑↓	Active ↑↓	Pwd never Expired ↑↓	Locked ↑↓	Smart Card required ↑↓	Serv acco
support	YES	YES	YES	NO	NO	NO

Showing 1 to 1 of 1 entries (filtered from 10 total entries)

# SERVICE ACCOUNTS

## Domain Administrators

Show 10 entries

SamAccountName	Enabled	Active	Pwd never Expired	Locked	Smart Card required	Service account
srv_task_admin2	YES	YES	YES	NO	NO	YES

# NO PASSWORD CHANGE

Account <span style="float: right;">↕</span>	Creation <span style="float: right;">↕</span>	LastChanged
Administrator	2003-12-02 08:24:59Z	2003-12-02 11:40:38Z
CitrixIMS	2003-12-03 12:17:47Z	2003-12-03 13:18:06Z
REM_Batch	2003-12-08 14:47:53Z	2003-12-08 15:47:53Z
CLUSTERADMIN	2003-12-29 12:47:58Z	2003-12-29 13:47:58Z
BackupExec	2004-10-08 12:19:00Z	2004-10-08 14:19:00Z

# NO TIERING MODEL

```
mimikatz 2.2.0 x64 (oe.eo)

.#####.   mimikatz 2.2.0 (x64) #19041 May 18 2021 17:07:45
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # ts::logonpasswords
!!! Warning, false positive can be listed !!!

Domain      : purple
UserName     : pentestlab
Password/Pin: Password123

mimikatz # _
```

## IT'S COMPLICATED



Chirag Savla · Jul 24, 2021 · 15 min read



# Fantastic Windows Logon types and Where to Find Credentials in Them

Hello All,

In this blog post we will explore and learn about various Windows Logon Types and understand how are these logon type events are generated. We will also see if we can extract credentials from individual logon types. We will be using our [Active Directory Attack Defense Lab](#) for all the demos.

## **5. SIN**

**NO IN-DEPTH ANALYSIS  
AFTER AN INCIDENT**



# PASSWORD RESET

EXPLOITS AND VULNERABILITIES

## 500,000 Fortinet VPN credentials exposed: Turn off, patch, reset passwords

Posted: September 9, 2021 by [Pieter Arntz](#)

A threat actor has leaked a list of almost 500,000 Fortinet VPN credentials, stolen from 87,000 vulnerable FortiGate SSL-VPN devices. The breach list provides raw access to organizations in 74 countries, including the USA, India, Taiwan, Italy, France, and Israel, with almost 3,000 US entities affected.

According to [Fortinet](#) the credentials were obtained from systems that remained unpatched against [CVE-2018-13379](#) at the time of the actor's scan. **Even if the devices have since been patched, if the passwords were not reset, they remain vulnerable.**

# PATCHING TOO LATE – FORENSIC INVESTIGATION

EXCH13 ● connected analyst

HttpProxy

- ReportingWebService
- autodiscover
- bin
- ecp
- ews
- mapi
- oab
- owa
  - auth
    - 15.0.1178
    - Current
- powershell
- pushnotifications
- rpc
- sync

Name	Size	Mode	mtime	atime	ctime	btime
e1ae7e73e0.aspx	2087	-rwxr-xr-x	2021-03-07T19:23:05.810465Z	2021-03-07T19:23:05.810465Z	2021-03-07T19:23:20.4053702Z	2021-03-07T19:23:05.810465Z
Current	0	drwxr-xr-x	2016-11-06T21:45:24.2816309Z	2016-11-06T21:45:24.2816309Z	2021-03-07T19:23:20.4053702Z	2016-11-06T21:45:23.6722173Z

Stats | **Textview** | HexView

\\.\C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\e1ae7e73e0.aspx

<b>Size</b>	2087	<b>Properties</b>	
<b>Mode</b>	-rwxr-xr-x	<b>mft</b>	340288-128-3
<b>Mtime</b>	2021-03-07T19:23:05.810465Z	<b>name_type</b>	POSIX
<b>Atime</b>	2021-03-07T19:23:05.810465Z	<b>SHA256</b>	86968194f77671fbb382f9377a7a4369ab36d7589c0bfcddf5ad45633445f1ef
<b>Ctime</b>	2021-03-07T19:23:20.4053702Z	<b>MD5</b>	4e3b7ba4d6f96120beec4e61d9c397c0
<b>Last Collected</b>	2021-03-12 13:34:12 UTC		



# LEAKED CREDENTIALS

---

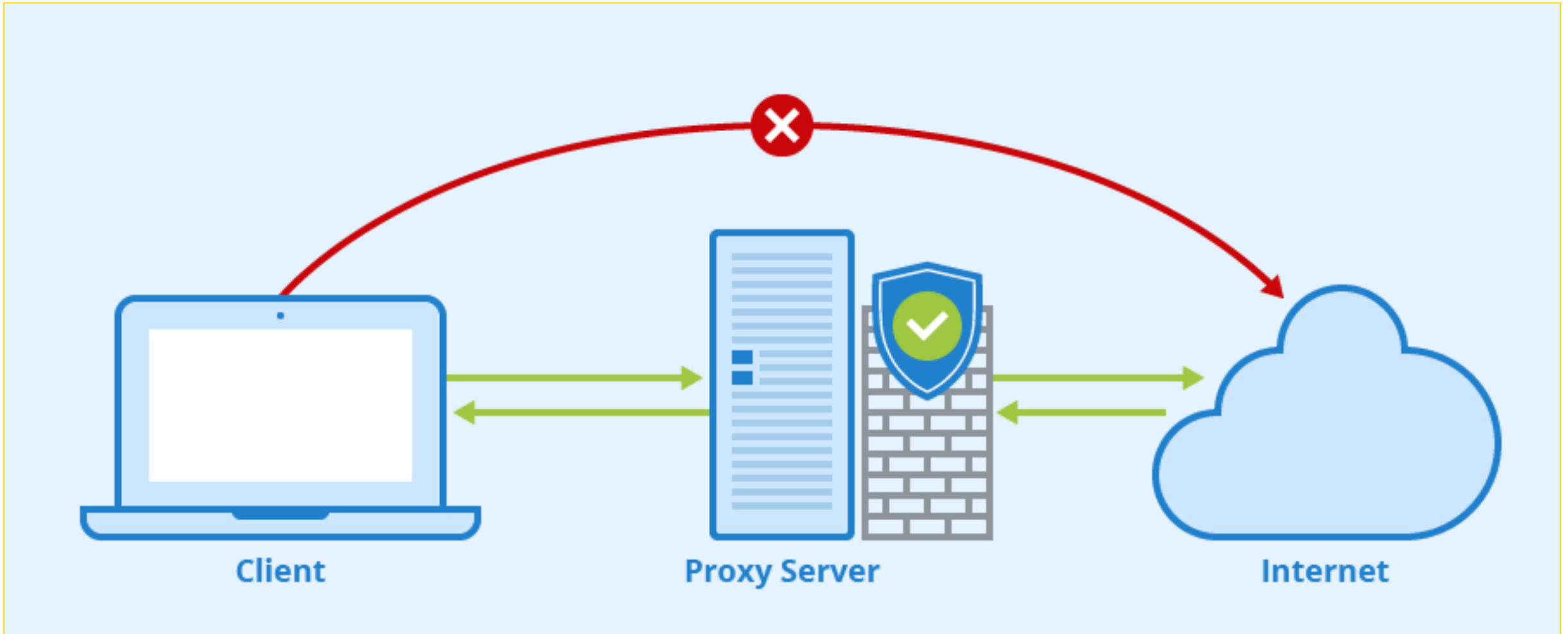




**6. SIN**

**DIRECT ACCESS  
TO THE INTERNET**

## GOOD ANALYSIS POSSIBILITIES



# PROXY CATEGORIES

information about adoption, immigration information, and immigration services.

## **Hacking**

Sites that distribute, promote or provide tools or other information intended to help gain unauthorized or illegal access to computers, computer networks, or computerized communication and control systems. Also includes sites with instructions for creating or distributing malware or information on performing cyber attacks.

## **Health**

Sites that provide advice and information on general health such as fitness and well-being, personal health, medical services, over-the-counter and prescription medications, health effects of both legal and illegal drug use, alternative and complementary therapies, medical information about ailments, dentistry, optometry, and general psychiatry. Also includes self-help and support organizations dedicated to a disease or health condition.

## **Humor/Jokes**

Sites that primarily focus on comedy, jokes, fun, etc. This may include sites containing jokes of adult or mature nature. Sites containing humorous Adult/Mature content also have an Adult/Mature category rating.

## **Informational**

Sites that provide content that is informational in nature and does not provide a way to

equipment, and other Web-enabled devices. Also includes security camera feeds, which are dually categorized as TV/Video Streams.

## **Internet Telephony**

Sites that facilitate Internet telephony or provide Internet telephony services such as voice over IP (VOIP).

## **Intimate Apparel/Swimsuit**

Sites that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. This does not include sites selling undergarments as a subsection of other products offered.

## **Job Search/Careers**

Sites that provide assistance in finding employment and tools for locating prospective employers.

## **Malicious Outbound Data/Botnets**

Sites to which botnets or other malware (as defined in the Malicious Sources category) send data or from which they receive command-and-control instructions. Includes sites that contain serious privacy issues, such as “phone home” sites to which software can connect and send user information. Usually does not include sites that can be categorized as Malicious Sources.

## **Malicious Sources/Malnets**

Sites that host or distribute malware or whose purpose for existence is as part of a malicious network (malnet) or the malware

ecosystem. Malware is defined as software

# USER AGENT ANALYSIS

	Data
	GET /gates HTTP/1.1
	Data Raw: 48 6f 73 74 3a 20 34 35 2e 31 35 33 2e 32 34 33 2e 39 33 0d 0a Data Ascii: Host: 45.153.243.93
	Data Raw: 55 73 65 72 2d 41 67 65 6e 74 3a 20 43 51 50 43 50 69 68 4c 51 77 0d 0a Data Ascii: User-Agent: CQPCPihLQw
	Data Raw: 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31 37 36 0d 0a Data Ascii: Content-Length: 176
	Data Raw: 0d 0a Data Ascii:
	Data Raw: 65 13 30 26 8c a2 51 de 18 a0 6c d4 69 b8 27 06 9d 13 95 9f b5 a3 8c 90 9d 60 16 c7 a0 d9 16 51 3d 7a 5d f3 cf a3 6c ab 7c 54 50 c3 01 25 ef 22 fe 66 06 b3 ec 61 17 97 57 a7 1b 8d 58 53 46 23 6b 63 4f 65 77 f9 91 af 1c d9 cf 6f 4d b2 8c 31 3b c1 6b 04 21 4c 37 cf 8e 69 45 07 9f 6f 88 32



# DIFFICULT EXFILTRATION

---



# DNS BEACONING



BUY NOW

FEATURES

SCREENSHOTS

TRAINING

SUPPORT

BLOG



Download

Community Kit

Core Impact

Contact Us



## Hacking through a **Straw** (Pivoting over DNS)

Posted on [July 9, 2013](#) by [Raphael Mudge](#)

Last month, I announced [Beacon's ability to control a host over DNS](#). I see Beacon as a low and slow lifeline to get an active session, when it's needed. Sometimes though, Beacon is all you have. There are times when Meterpreter gets caught too quickly or just can't get past the network egress restrictions.

## 7. SIN

**NO EDR / SOC**



# ENDPOINT DETECTION AND RESPONSE – 24/7 SOC

---



# EDR DETECTION

## #0252-0219 Indication of well known hacking tools based on file names

Detects the dropping of several well known hacking tools based on file names.

EDRaaS - Deploy EDRaaS - Stable

### Details

Type	Platforms	MITRE Technique(s)	Alerts over 30 days	Unresolved Alerts	Total Alerts	Imported
Tanium Signal v1.0	Windows	None	10	65	72	1/6/20

Alerts Quick Scans (0) **Definition** Suppression Rules Engine Analysis

AND

group() File Operation *Is NOT* "delete"

OR

group() File Path *Contains* "metasploit"

group() File Path *Contains* "sharphound"

group() File Path *Contains* "mimikatz"

group() File Path *Contains* "bloodhound"

## #0253-0220 Indication of well known hacking tools based on process execution

Detects the execution of several well known hacking tools based on common names.

EDRaaS - Deploy EDRaaS - Stable

### Details

Type	Platforms	MITRE Technique(s)	Alerts over 30 days	Unresolved Alerts	Total Alerts	Imported Date	Version
Tanium Signal v1.0	Windows	None	0	20	20	1/6/2021 5:31 PM	4

Alerts Quick Scans (0) **Definition** Suppression Rules Engine Analysis

OR

Process Path *Contains* "metasploit"

Process Path *Contains* "sharphound"

Process Path *Contains* "mimikatz"

Process Path *Contains* "bloodhound"

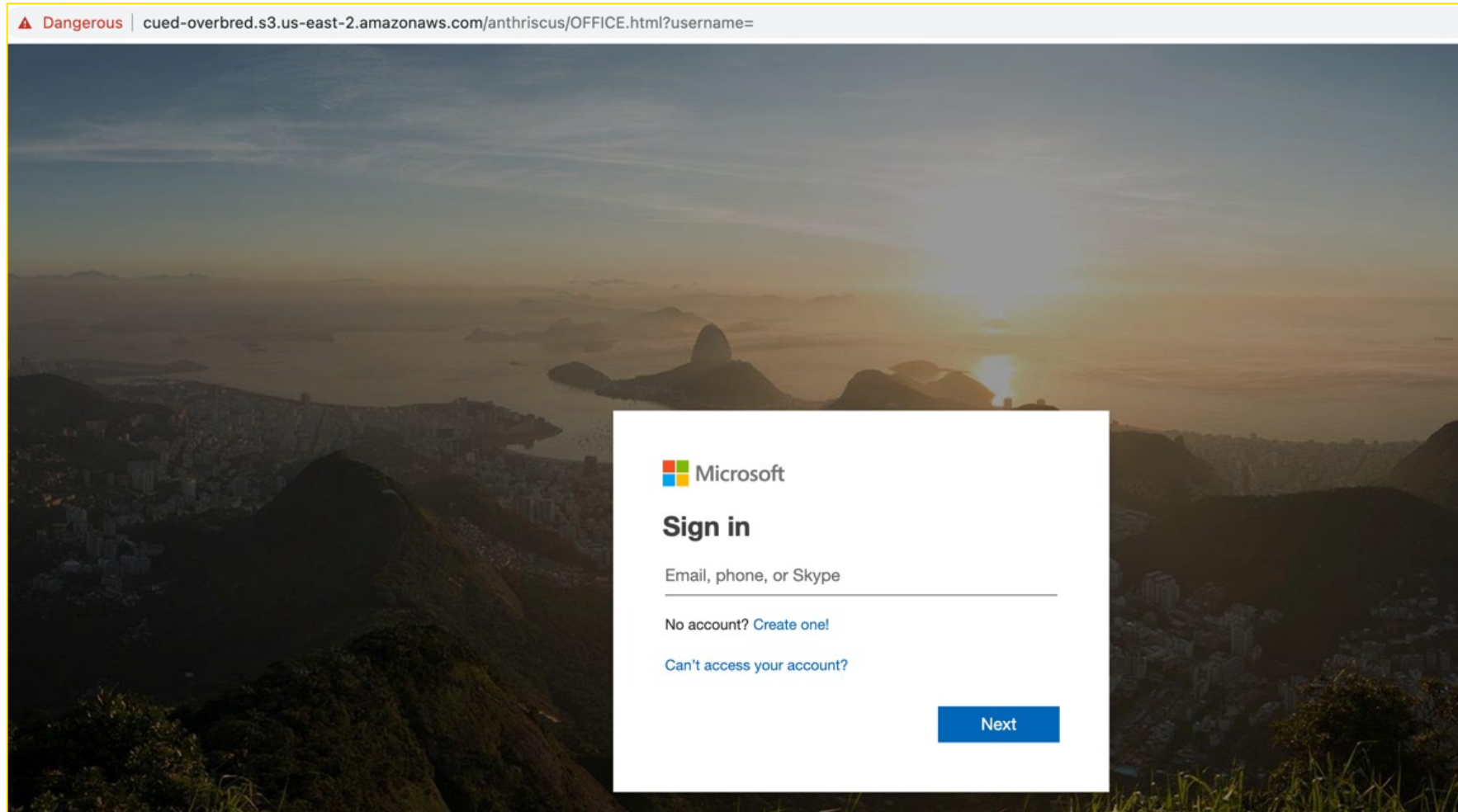
# AV NAMING CONVENTIONS

Ad-Aware	! Trojan.GenericKD.48615413	AhnLab-V3	! Malware/Win.Generic.C5001141
ALYac	! Trojan.GenericKD.48615413	Antiy-AVL	! Trojan/Generic.ASMalwS.353E907
Avast	! FileRepMalware [Misc]	AVG	! FileRepMalware [Misc]
BitDefender	! Trojan.GenericKD.48615413	CrowdStrike Falcon	! Win/malicious_confidence_100% (W)
Cybereason	! Malicious.d509cc	Emsisoft	! Trojan.GenericKD.48615413 (B)
eScan	! Trojan.GenericKD.48615413	ESET-NOD32	! A Variant Of MSIL/Riskware.SharpHound.B
Fortinet	! Riskware/SharpHound	GData	! Trojan.GenericKD.48615413
K7AntiVirus	! Riskware ( 00584baa1 )	K7GW	! Riskware ( 00584baa1 )
Kaspersky	! UDS:DangerousObject.Multi.Generic	Lionic	! Trojan.Multi.Generic.4lc
Malwarebytes	! HackTool.SharpHound.Feye	MAX	! Malware (ai Score=87)
MaxSecure	! Trojan.Malware.1728101.susgen	McAfee	! RDN/Generic.dx
McAfee-GW-Edition	! RDN/Generic.dx	Microsoft	! VirTool:MSIL/SharpHound
Palo Alto Networks	! Generic.ml	Panda	! Trj/GdSda.A
Sangfor Engine Zero	! Riskware.Win32.Agent.ky	SecureAge APEX	! Malicious
Sophos	! BloodHoundAD (PUA)	Symantec	! ML.Attribute.HighConfidence
Trellix (FireEye)	! Trojan.GenericKD.48615413	TrendMicro	! TROJ_GEN.R03FC0PCB22

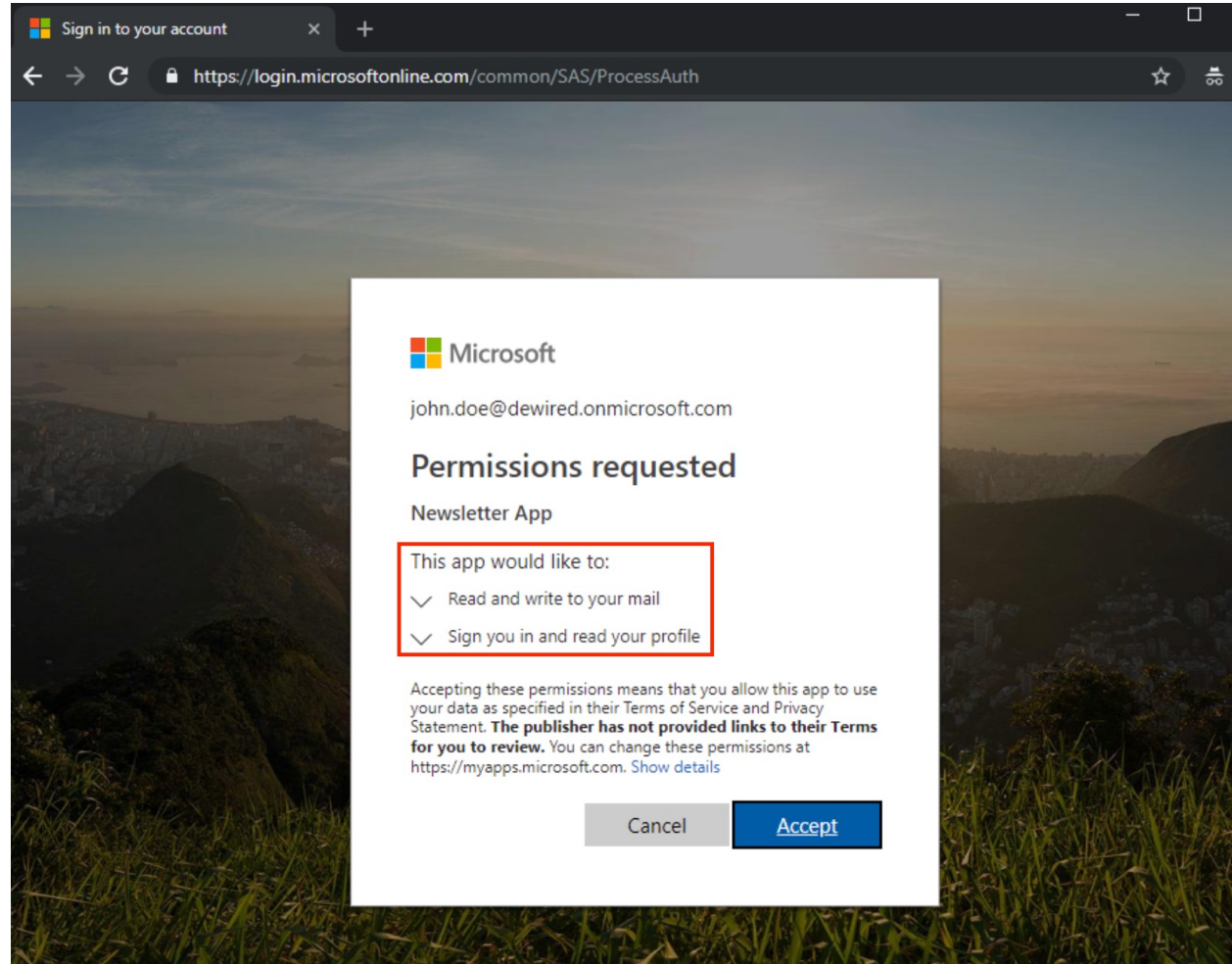


**ONE MORE THING...**

# PHISHING – «COLD COFFEE»



# ILLICIT CONSENT GRANT – ONE CLICK IS ALL IT TAKES



# ILLICIT CONSENT GRANT – ONE CLICK IS ALL IT TAKES



Microsoft Security Intelligence   
@MsftSecIntel



Microsoft is tracking a recent consent phishing campaign, reported by [@ffforward](#), that abuses OAuth request links to trick users into granting consent to an app named 'Upgrade'. The app governance feature in Microsoft Defender for Cloud Apps flagged the app's unusual behavior.



**App with suspicious OAuth scope was flagged high-risk by Machine Learning model, made graph calls to read email and created Inbox Rule**

■ ■ ■ Medium ● Unknown ● New



Manage alert



Link alert to another incident



Consult a threat expert



# AZURE ATTACK MATRIX

## AZURE AD & M365 ATTACK MATRIX

Reconnaissance	Initial Access	Discovery	Actions	Persistence
Azure AD PowerShell	Bruteforce via OWA	Enumerate Users / Roles / Permissions	Change MFA App Settings	Golden SAML
Enumerate Domains	Bruteforce EWS	Enumerate MFA Settings	Enumerate Teams / OneDrive / SharePoint / Email / Skype etc	Malicious App Registrations
Enumerate Users	Bruteforce OAuth	Enumerate Azure Tenants	Downgrade License	User Account Creation
Enumerate Tennant Domain	Bruteforce via AAD Sign in form	Enumerate Azure Subscriptions	Impersonate Users	Modifying Conditional Access
Enumerate Login Information	Bruteforce through Autologon API	Enumerate Conditional Access Policies	Assign Service Principal Role	Adding Service Principals with Read/Write
	Phishing Emails (Login / OAuth App)	Enumerate Applications	User Access Administrator Role Toggle	Mailbox Rule Creations
	Golden SAML	Pass the PRT	eDiscovery Abuse	Mailbox Folder Permission
	MFA Bypass via IMAP/POP	Pass the Cert	Access Azure Subscriptions	Mail Flow (Transport Rules)
	PTA: Skeleton Keys		Executions of Scripts on Azure VMs	Executions of Scripts on Azure VMs
	Compromise Azure AD Connect		DoS Azure AD	Creating Service Principal





# STEPHAN BERGER

## HEAD OF INVESTIGATIONS

---



### InfoGuard AG

Lindenstrasse 10  
6340 Baar / Switzerland

info@infoguard.ch  
www.infoguard.ch

Stephan.Berger@infoguard.ch  
Mobile +41 79 718 72 37

#### LinkedIn

<https://www.linkedin.com/in/stephan-berger-59575a20a/>

#### Twitter

<https://twitter.com/malmoeb>

Zweigniederlassung Bern  
Staufferstrasse 141  
3014 Bern / Switzerland

**InfoGuard**  
SWISS CYBER SECURITY