

RANSOMWARE IN SWITZERLAND AND AROUND THE WORLD



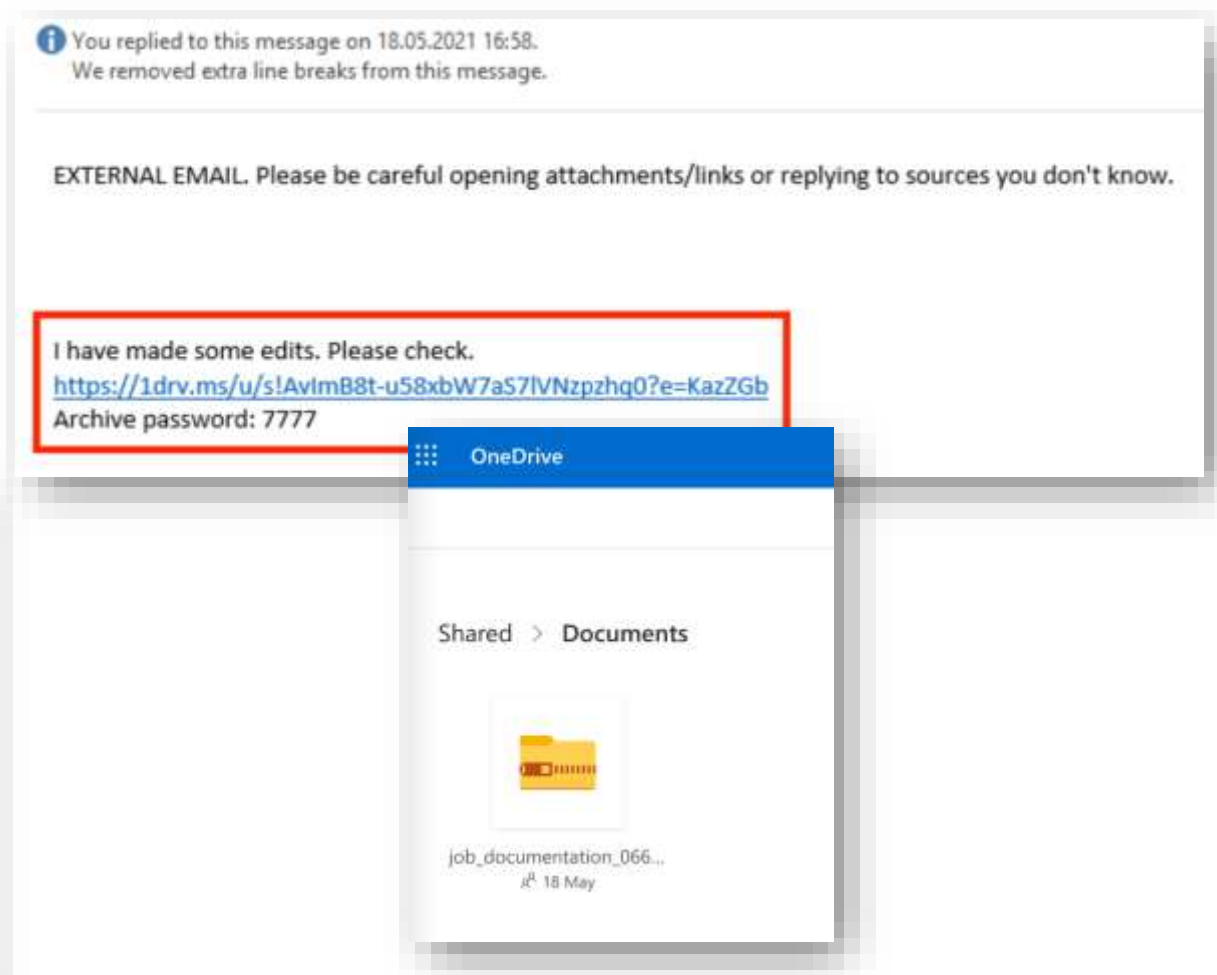
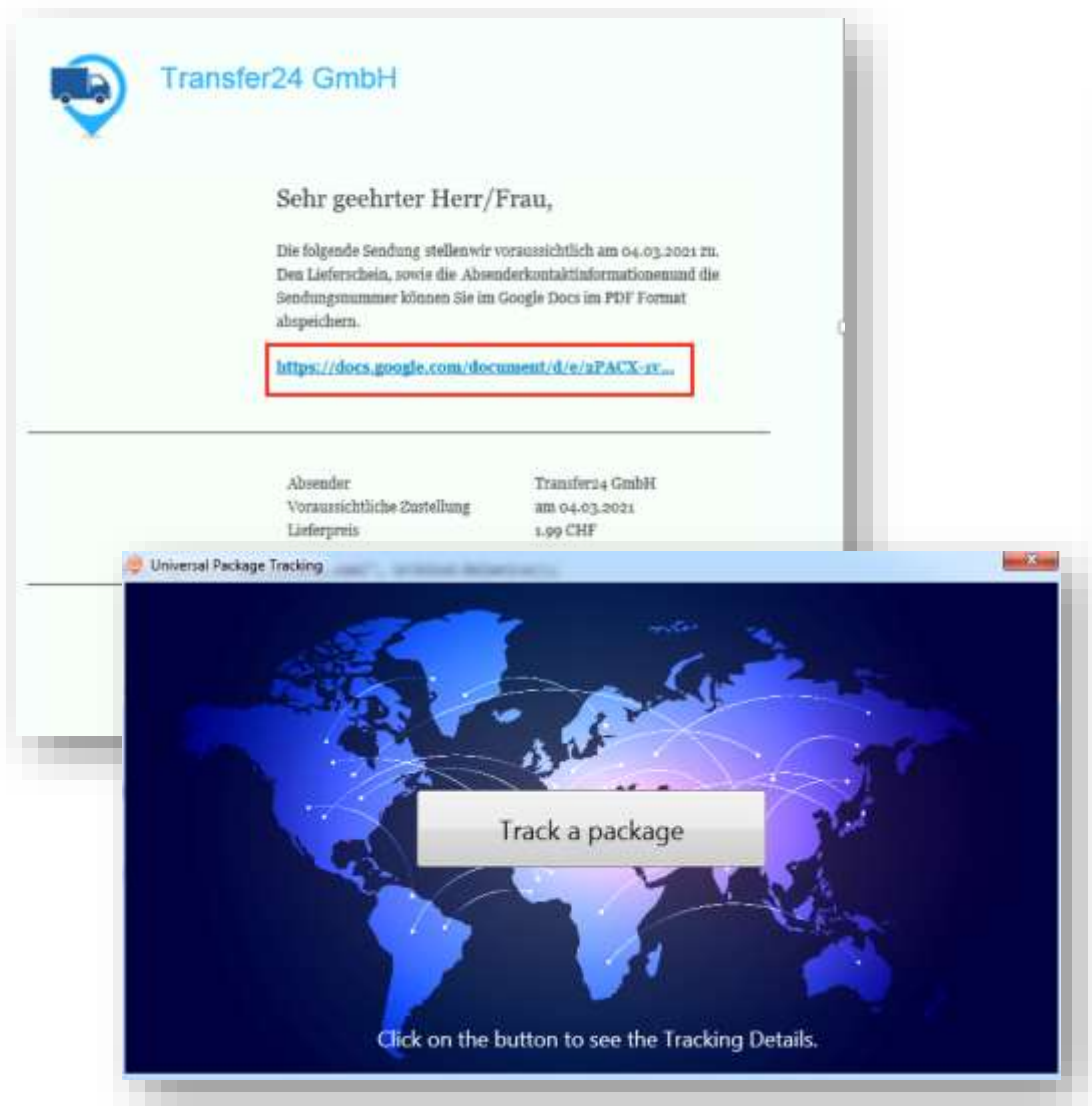
Insights, Facts and Findings

Initial Entry



Source: https://en.wikipedia.org/wiki/Fort_Bourtange

Phishing / Malicious documents



Vulnerabilities

EXCH13 connected analyst

HttpProxy

- ReportingWebService
- autodiscover
- bin
- ecp
- ews
- mapi
- oab
- owa
- auth
- 15.0.1178
- Current
- powershell
- pushnotifications
- rpc
- sync
- Poplmap
- GroupMetrics
- Logging
- Mailbox
- Public
- RemoteScripts
- Scripts
- Setup
- TransportRoles
- UnifiedMessaging
- Working

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

Size	2087
Mode	-rwxr-xr-x
Mtime	2021-03-07T19:23:05.810465Z
Atime	2021-03-07T19:23:05.810465Z
Ctime	2021-03-07T19:23:20.4053702Z
Last Collected	2021-03-12 13:34:12 UTC

Properties

mft	340288-128-3
name_type	POSIX
SHA256	86968194f77671fbb382f9377a7a4369ab36d7589c0bfcddf5ad45633445f1ef
MD5	4e3b7ba4d6f96120beec4e61d9c397c0

Administrator: Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. Alle Rechte vorbehalten.

```
PS C:\Users\adm.kithaus\SBS> cd "C:\Program Files\Microsoft\Exchange Server\U15\FrontEnd\HttpProxy\owa\auth"
PS C:\Program Files\Microsoft\Exchange Server\U15\FrontEnd\HttpProxy\owa\auth> dir
```

Verzeichnis: C:\Program Files\Microsoft\Exchange Server\U15\FrontEnd\HttpProxy\owa\auth

Mode	LastWriteTime	Length	Name
d----	06.11.2016 22:44		15.0.1170
d----	06.11.2016 22:45		Current
-a---	09.03.2016 00:34	7716	errorFE.aspx
-a---	09.03.2016 00:34	7220	ExpiredPassword.aspx
-a---	09.03.2016 00:34	110	getidtoken.htm
-a---	09.03.2016 00:34	5254	logoff.aspx
-a---	09.03.2016 00:34	15766	login.aspx
-a---	09.03.2016 00:34	1897	OutlookCH.aspx
-a---	09.03.2016 00:34	332	RedirSuiteServiceProxy.aspx
-a---	09.03.2016 00:34	4475	signout.aspx
-a---	09.03.2016 00:34	4694	SumFeedback.aspx

```
PS C:\Program Files\Microsoft\Exchange Server\U15\FrontEnd\HttpProxy\owa\auth> dir -hidden
```

Verzeichnis: C:\Program Files\Microsoft\Exchange Server\U15\FrontEnd\HttpProxy\owa\auth

Mode	LastWriteTime	Length	Name
-a---	07.03.2021 20:23	2007	e1ae7e73e8.aspx

```
PS C:\Program Files\Microsoft\Exchange Server\U15\FrontEnd\HttpProxy\owa\auth> del .\e1ae7e73e8.aspx
```

del : Das Element C:\Program Files\Microsoft\Exchange Server\U15\FrontEnd\HttpProxy\owa\auth\e1ae7e73e8.aspx kann nicht entfernt werden: Sie besitzen keine ausreichenden Zugriffsberechtigungen zum Ausführen dieses Vorgangs.

Die Zeile:1 Zeichen:1
+ del .\e1ae7e73e8.aspx
+ ~~~~~
+ CategoryInfo : PermissionDenied: (C:\Program File...e1ae7e73e8.aspx:FileInfo) (Remove-Item), InvalidOperationException
+ FullyQualifiedErrorId : RemoveFileSystemItemUnauthorizedAccess,Microsoft.PowerShell.Commands.RemoveItemCommand

```
PS C:\Program Files\Microsoft\Exchange Server\U15\FrontEnd\HttpProxy\owa\auth>
```

Extended Perimeter

SHODAN

Explore

Downloads

Pricing

Search...

Account

20.71.

Regular View

Raw Data

History

// TAGS: cloud self-signed

// LAST UPDATE: 2021-07-04

General Information

Cloud Provider

Azure

Cloud Region

westeurope

Cloud Service

AzureCloud

Country

Netherlands

City

Amsterdam

Organization

Microsoft Corporation

ISP

Microsoft Corporation

ASN

AS8075

Open Ports

3389

// 3389 / TCP

~1660128709 | 2021-07-04T11:04:06.474800

Remote Desktop Protocol

\x03\x00\x00\x13\x0e\xad\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00

SSL Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

36:85:3a:8d:f6:d6:19:bb:46:c7:f9:95:c3:64:45:34

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=prdwinsgnt01 [REDACTED]

Validity

Not Before: Jun 4 13:23:38 2021 GMT

Not After : Dec 4 13:23:38 2021 GMT

Subject: CN=prdwinsgnt01 [REDACTED]

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

Key Points

- MFA all the things



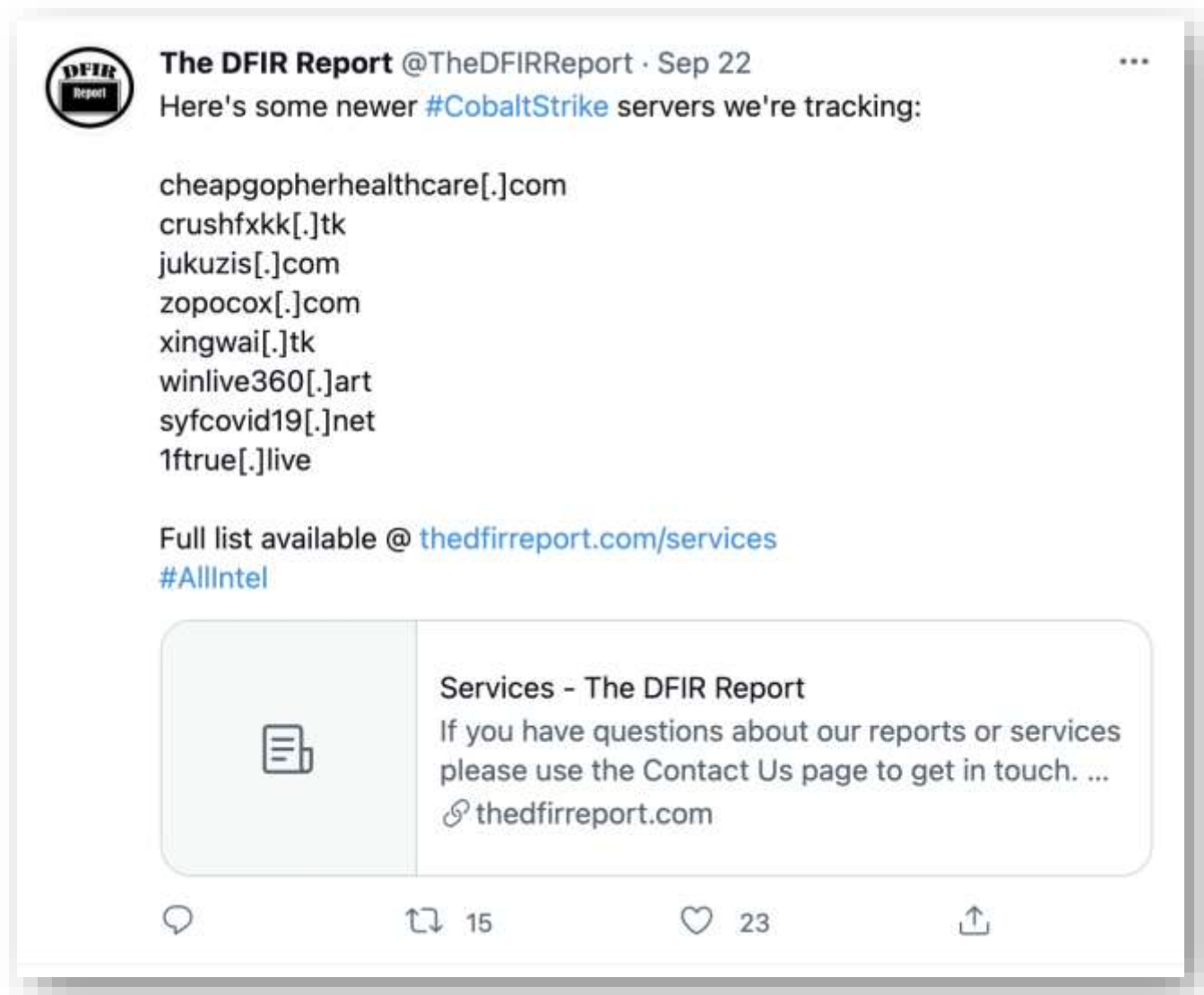
- Assume breach – even after applying patches
 - And change **all** passwords
 - And **check** that you changed all passwords
- Extend asset management to the Cloud (automate what you can)

Persistent Access and Backdoors



Remote Desktop Solutions



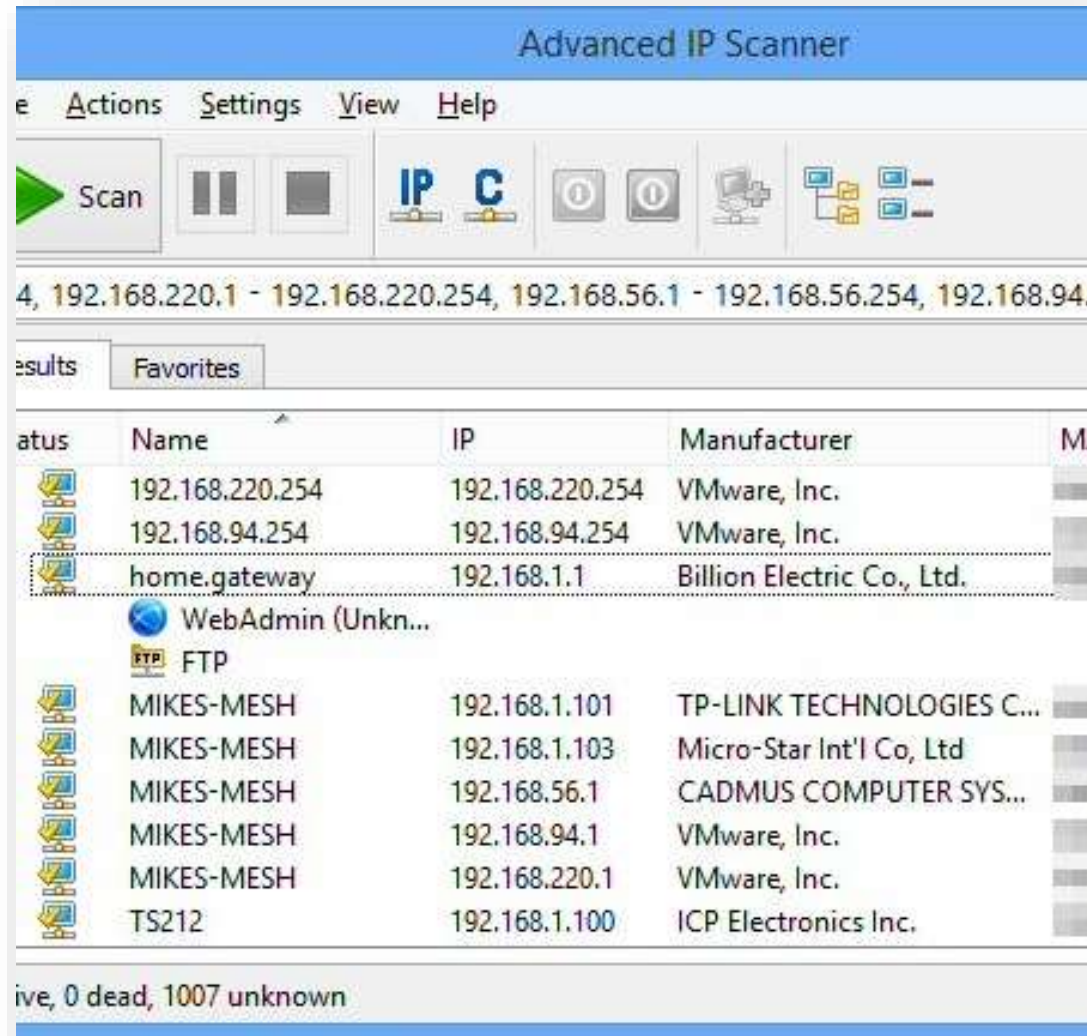


Key Points

- Monitor connections to known remote desktop providers
 - Proxy-Logs
 - Firewall
- Use freely available data – as an example, the Cobalt-Strike IP list
 - Firewall
- Remote desktop software may write connection data
 - For example, the AnyDesk Traces file
 - May be useful in the event of an incident



Reconnaissance inside the network



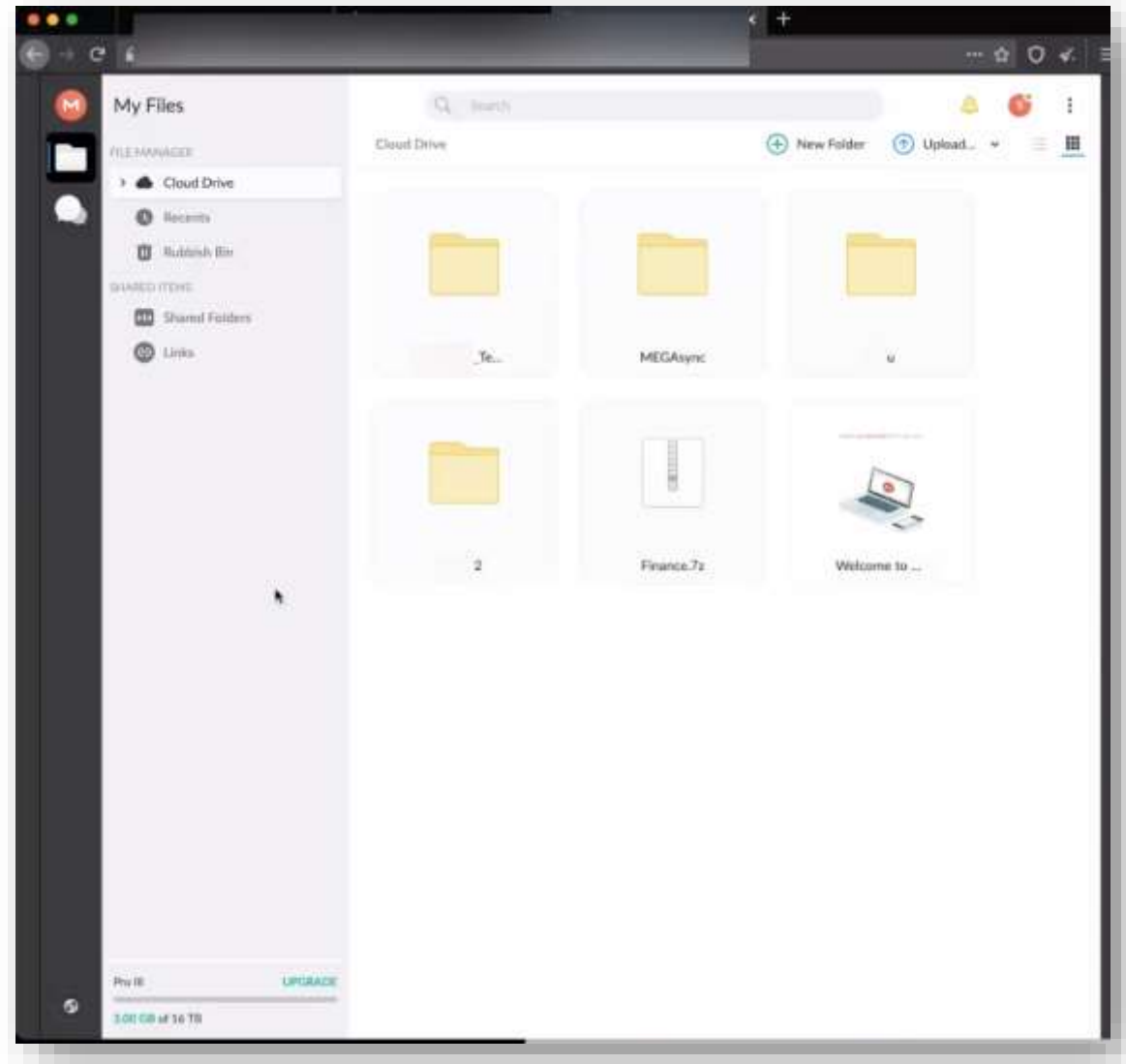
Key Points

- High CPU load
 - Check the processes on the host
- Softperfect license file
 - Tracking adversaries through various breaches
- Advanced IP scanner
 - Stores the last scanned IP-Ranges within the registry
(Useful for Incident Responder)





Exfiltration – The other side around



Key Points

- Blocking (if possible) of known Upload-Providers
 - Mega.NZ
 - Yandex
- The configuration file for the cloud exporter might still be on disk
 - Or it could be carved out of the file system
 - May give you an advantage during negotiations



Antivirus Event Analysis Cheat Sheet

Version 1.7.2

Florian Roth @cyb3rops

Attribute	Less Relevant	Relevant		Highly Relevant	
Virus Type	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 Clearlogs PHP/BackDoor ASP/BackDoor JSP/BackDoor Backdoor.PHP Backdoor.ASP Backdoor.JSP	CobaltStrike Keylogger MeteTool Meterpreter Metasploit PowerSSH Mimikatz PowerSploit PSWTool PWDump Swrort Rozena

AV-Logs

Multi-stage incident involving Credential access & Discovery on one endp...	High	2 investigation states	Credential access. Discovery...	v-vpn-11.dom.local	patrick.kraenzlin	5/7	Antivirus.Endpoint	11.03.21, 07:02	11.03.21, 07:14
Malicious credential theft tool execution detected	High	Unsupported alert ...	Credential access	v-vpn-11.DOM.LO...	patrick.kraen...	-	Endpoint	11.03.21, 07:03	11.03.21, 07:14
Malicious credential theft tool execution detected	High	Unsupported alert ...	Credential access	v-vpn-11.DOM.LOCAL		-	Endpoint	11.03.21, 07:08	11.03.21, 07:08
Password stealing from files	Medium	Unsupported alert ...	Discovery	v-vpn-11.dom.local	patrick.kraenzlin	-	Endpoint	11.03.21, 07:06	11.03.21, 07:06
Password stealing from files	Medium	Unsupported alert ...	Discovery	v-vpn-11.dom.local	patrick.kraenzlin	-	Endpoint	11.03.21, 07:06	11.03.21, 07:06
File backups were deleted on one endpoint	Medium	N/A	Defense evasion	v-www-001.dom.local	Administrator	1/1	Endpoint	20.03.21, 03:23	
File backups were deleted	Medium	Unsupported OS	Defense evasion	v-www-001.dom.local	Administrator	-	Endpoint	20.03.21, 03:23	
File backups were deleted on one endpoint	Medium	N/A	Defense evasion	s-dc-001.dom.local	Administrator	1/1	Endpoint	20.03.21, 02:28	
File backups were deleted	Medium	Unsupported OS	Defense evasion	s-dc-001.dom.local	Administrator	-	Endpoint	20.03.21, 02:28	

Key Points

- AV usually detects one or more steps of the attackers
- The alarms are either
 - a. not heeded
 - b. not understood
 - c. or not connected to a monitoring system at all
- Good (and underestimated) alert system





Get Active Directory Security at 80% in 20% of the time

Active directory is quickly becoming a critical failure point in any big sized company, as it is both complex and costly to secure..

- Check for stored passwords – from Zero to Hero Domain Administrator

KEY POINTS

Obfuscated Passwords

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

Show 10 entries

GPO Name ↑↓	Password origin ↑↓	UserName ↑↓
allgemeine_Client_Einstellungen ?	groups.xml	support
allgemeine_Client_Einstellungen ?	groups.xml	ladmin

Domain Administrators

Direct User Members

Show 10 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)

INFOGUARD Cyber Defence Center

InfoGuard
SWISS CYBER SECURITY



- Swiss CDC
- 7x24

- 250m²
- 45 employees



ISO 27001
ISAE 3000 TYPE 2

Questions?



INFOGUARD – the Swiss cyber security expert



Stephan Berger
Senior Cyber Security Analyst

InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz

Telefon +41 41 749 19 00

