Rapport de Threat Intelligence

Scénario :

Un attaquant effectue une reconnaissance en collectant des informations sur les employés, la structure et les systèmes de l'organisation cible. L'attaquant utilise les moteurs de recherche, les réseaux sociaux et d'autres sources pour recueillir des informations sur les employés, leurs rôles et la structure de l'organisation. L'attaquant sélectionne des individus spécifiques au sein de l'organisation comme cibles de l'attaque de phishing sur la base des informations recueillies. L'attaquant usurpe les adresses courriel pour donner l'impression que les courriels de phishing sont légitimes et dignes de confiance. L'attaquant envoie des courriels de phishing aux personnes ciblées, contenant un lien ou une pièce jointe malveillante. Si une victime clique sur le lien malveillant ou ouvre la pièce jointe, l'attaquant exploite les vulnérabilités pour accéder au système de la victime via un logiciel malveillant qui vise à garder un pied dans le système. L'attaquant établit ensuite une connexion de commande et de contrôle (C2) pour maintenir le contrôle sur le système compromis. L'attaquant exfiltre les données sensibles du système compromis vers un serveur distant. Pour éviter d'être détecté, l'attaquant masque les traces en supprimant les journaux et autres traces de l'attaque. Suite à cette attaque, la Blue Team a pu ramasser les informations/preuves suivantes :

Courriel utilisé pour le phishing :

Urgent: Verify Your Account to Prevent Service Disruption

Dear [Employee Name],

We recently detected unusual activity on your account. To ensure the security of your account and prevent any service disruption, please click on the following link to verify your account information.

Malicious Link: http://x4z9can.cn/4812/

Thank you for your prompt attention to this matter.

Best regards,

John Doe

XYZ Company

Log 1:

Timestamp: 2023-10-15T15:23:45

Source IP: 192.168.1.100

Destination IP: x4z9can.cn (malicious site)

URL: http://x4z9can.cn/4812/

User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.99 Safari/537.36

Event Type: Malicious Site Access

Description: Detected an attempt to access a known malicious site hosting a downloader. The URL pattern matches a known malware pattern: 'http://x4z9can.cn/4812/'

Log 2:

Timestamp: 2023-10-01T15:50:00

Source IP: 192.168.1.150

Destination IP: c2-malicious-server.com

Destination Port: 4444

Protocol: TCP

Event Type: Reverse Shell Command and Control Attempt

Log 3:

Timestamp: 2023-10-01T16:05:00

Source IP: 192.168.1.200

Destination IP: 203.0.113.42

Protocol: TCP

Source Port: 12345

Destination Port: 4444

Reason: Suspicious Outbound Connection

Objectifs :

Attribution de l'attaque : utiliser les normes de renseignement sur les menaces pour analyser les modèles d'attaque et les motivations des attaquants.

Recommandations de mitigation : développer et mettre en œuvre des contre-mesures basées sur les renseignements sur les menaces pour atténuer les impacts actuels et futurs des attaques.

Partage d'informations : partager des renseignements pertinents sur les menaces avec des organisations externes, telles que d'autres institutions financières, à l'aide de STIX et TAXII.

Analyse des indicateurs de compromission (IoC) : exploiter OpenIOC et CybOX pour analyser et partager les IoC liés à l'attaque, facilitant ainsi la détection et la prévention.

Étapes :

Analyse CAPEC : identifier et analyser les entrées CAPEC pertinentes associées aux modèles d'attaque observés. Rechercher des modèles qui correspondent aux tactiques sophistiquées utilisées par les auteurs de menaces avancées et ainsi qu'aux motivations.

Stratégie de mitigation : élaborer une stratégie de mitigation basée sur l'analyse CAPEC. Mettre en œuvre des contrôles et des mesures de sécurité pour empêcher d'autres accès non autorisés et violations de données.

Intégration STIX et TAXII : créer un document STIX qui résume les informations pertinentes sur les menaces, y compris les indicateurs de compromission, les modèles d'attaque et les acteurs de menace attribués. Utiliser TAXII pour partager ce document STIX avec des partenaires de confiance du secteur financier.

Intégration OpenIOC et CybOX : générer des fichiers OpenIOC contenant des IoC dérivés de l'analyse CAPEC. De plus, utilisez CybOX pour représenter les cyber-observables associés à l'attaque.

Partage de renseignements sur les menaces : utiliser le protocole TAXII pour partager des renseignements sur les menaces avec des institutions financières externes. Partager les

IoC, les TTP et d'autres informations pertinentes pour renforcer la défense collective contre l'acteur menaçant.

Surveillance continue : mettre en œuvre une surveillance continue du trafic réseau et des systèmes à l'aide des IoC développés et des renseignements sur les menaces. Utiliser OpenIOC et CybOX pour mettre à jour et affiner les règles de détection.

Analyse post-incident : réaliser une analyse post-incident à l'aide des données STIX et TAXII échangées. Évaluer l'efficacité des renseignements partagés sur les menaces pour améliorer la posture de sécurité de votre organisation et des entités collaboratrices.

1. **Analyse CAPEC :**

The reported attack is comparable to multiple items in the Common Attack Pattern Enumeration and Classification (CAPEC). This hazard is connected with the following attack patterns:

1. CAPEC-98 Information Phishing, the attacker started the attack by gathering employee information and deceiving targets with phishing methods. The purpose of the phishing emails was to deceive users into clicking on a malicious link.
2. CAPEC-559 Client confidence Exploitation, the attacker took advantage of employee confidence by sending emails that looked to emanate from a genuine source within the firm. This exploitation of trust aided the phishing attack's success.
3. CAPEC-564 Command and Control, after a user clicked on the malicious link, the attacker established a command and control (C2) connection in order to gain control of the infected machine.
4. CAPEC-579 Extraction The attacker leveraged the C2 connection to exfiltrate sensitive data from the compromised system to a remote server through the C2 channel.

2. Recommandations de mitigation :

a. Prioritize staff training to prevent information phishing, educate them on phishing dangers, and underline the need of avoiding suspicious links and files. For increased security, use powerful email filters to proactively reject phishing communications, routinely update detection rules, and implement multi-factor authentication (MFA).
b. To protect against client confidence exploitation, deploy robust email authentication protocols such as SPF, DKIM, and DMARC to check incoming emails. Employees should be educated on email security best practices on a regular basis, including confirming sender identities and reporting questionable communications.

c. Limit lateral attacker mobility by mitigating command and control threats through network segmentation. Install Intrusion Detection and Prevention Systems (IDPS) to monitor network traffic for anomalies and configure them to prevent or alert on command and control attempts.
d. Counter data extraction threats with data encryption for sensitive information. Utilize Endpoint Detection and Response (EDR) solutions to monitor endpoint activity and respond automatically to suspicious behavior. Implement Data Loss Prevention (DLP) solutions to prevent unauthorized data exfiltration. Establish a robust incident response plan covering identification, containment, eradication, and recovery procedures for various security incidents, including phishing, command and control, and data exfiltration. Regularly test and update the plan to adapt to evolving threats.

3. **Partage d'informations :**

a. STIX :

....

b. TAXII :

....

4. Indicator of Compromise (IoC) Analysis:

https://iocbucket.com/openioceditor

a. OpenIOC :

```
<ioc xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
xmlns:xsd='http://www.w3.org/2001/XMLSchema'
xmlns='http://schemas.mandiant.com/2010/ioc' id='38e4a177-36a0-4412-a967-
8c73c1c01d9d' last-modified='2023-10-05T00:57:35.213Z'> <short_description>Exercice
INF8108</short_description> <description>Exercice INF8108</description>
<authored_by>Équipe zoom</authored_by> <authored_date>2023-10-
05T00:57:35.213Z</authored_date> <links/> <definition> <Indicator operator='OR'
id='a699aaa7-f0ec-431f-9fb3-11d6966addde'> <IndicatorItem condition='contains'
id='7de938e8-cdb9-40c3-b87b-70b7c95a2e48'> <Context document='UrlHistoryItem'
search='UrlHistoryItem/URL' type='mir'/> <Content
type='string'>http://x4z9can.cn/4812/</Content> </IndicatorItem> <IndicatorItem
condition='contains' id='87a1c327-22ad-4c5f-9d30-b5f4b2e96032'> <Context
document='UrlHistoryItem' search='UrlHistoryItem/BrowserName' type='mir'/> <Content
type='string'>Mozilla</Content> </IndicatorItem> <IndicatorItem condition='contains'
id='f40216c9-acf9-437d-b8ab-5fdb38edc67f'> <Context document='UrlHistoryItem'
search='UrlHistoryItem/BrowserVersion' type='mir'/> <Content
type='string'>5.0</Content> </IndicatorItem> <IndicatorItem condition='contains'
id='bb18ad29-6fb9-4135-8b25-c94d818eb22a'> <Context document='UrlHistoryItem'
search='UrlHistoryItem/BrowserName' type='mir'/> <Content
```

```
type='string'>Chrome</Content> </IndicatorItem> <IndicatorItem condition='contains'
id='0b76b9e1-a257-43fd-b075-581e1c7957e9'> <Context document='UrlHistoryItem'
search='UrlHistoryItem/BrowserVersion' type='mir'/> <Content
type='string'>99.0.9999.99</Content> </IndicatorItem> <IndicatorItem
condition='contains' id='00854da0-f221-4739-a094-f2ce089cbe80'> <Context
document='UrlHistoryItem' search='UrlHistoryItem/BrowserName' type='mir'/> <Content
type='string'>Safari</Content> </IndicatorItem> <IndicatorItem condition='contains'
id='da3c1b8d-6bd7-4f7a-a210-586d0e2911fe'> <Context document='UrlHistoryItem'
search='UrlHistoryItem/BrowserVersion' type='mir'/> <Content
type='string'>537.36</Content> </IndicatorItem> <IndicatorItem condition='contains'
id='01d9e936-e6aa-433d-83d2-c16ff7cec8ce'> <Context document='PortItem'
search='PortItem/localIP' type='mir'/> <Content type='string'>192.168.1.100</Content>
</IndicatorItem> <IndicatorItem condition='contains' id='ae76453a-c08f-4794-adc2-
8529a393f33a'> <Context document='RegistryItem' search='RegistryItem/detectedAnomaly'
type='mir'/> <Content type='string'>Malicious Site Access</Content> </IndicatorItem>
<IndicatorItem condition='contains' id='908ec0f7-09cd-46b2-82b3-f8c90781a60f'>
<Context document='SystemInfoItem' search='SystemInfoItem/OS' type='mir'/> <Content
type='string'>Windows NT 10.0; Win64; x64</Content> </IndicatorItem> <IndicatorItem
condition='contains' id='fa13b1f0-8f4c-46bd-8e26-33af42b835e0'> <Context
document='UrlHistoryItem' search='UrlHistoryItem/LastVisitDateLocal' type='mir'/>
<Content type='date'>2023-10-15T15:23:45</Content> </IndicatorItem> <Indicator
operator='AND' id='b9f44a71-17c0-46ef-a53a-91058007288d'> <IndicatorItem
condition='contains' id='116b071f-dce0-43bd-b401-3d836054ad24'> <Context
document='UrlHistoryItem' search='UrlHistoryItem/LastVisitDateLocal' type='mir'/>
<Content type='date'>2023-10-01T15:50:00</Content> </IndicatorItem> <IndicatorItem
condition='contains' id='976b192c-7db6-4877-a81b-05d02ff0caac'> <Context
document='PortItem' search='PortItem/localIP' type='mir'/> <Content
type='string'>192.168.1.150</Content> </IndicatorItem> <IndicatorItem
condition='contains' id='ec357187-b59f-415b-ad3f-3276f1329548'> <Context
document='RouteEntryItem' search='RouteEntryItem/Destination' type='mir'/> <Content
type='IP'>c2-malicious-server.com</Content> </IndicatorItem> <IndicatorItem
condition='contains' id='0a731cec-6551-418c-b01e-43312cd17354'> <Context
document='PortItem' search='PortItem/remotePort' type='mir'/> <Content
type='int'>4444</Content> </IndicatorItem> <IndicatorItem condition='contains'
id='b03e4a91-0292-4a1d-8b41-32f46dff55a1'> <Context document='PortItem'
search='PortItem/protocol' type='mir'/> <Content type='string'>TCP</Content>
</IndicatorItem> <IndicatorItem condition='contains' id='6a01e387-d4e3-4112-99ad-
155f27d928ad'> <Context document='RegistryItem' search='RegistryItem/detectedAnomaly'
type='mir'/> <Content type='string'>Reverse Shell Command and Control
Attempt</Content> </IndicatorItem> </Indicator> <Indicator operator='AND'
id='27c96ceb-ad12-4602-a89a-6da45fa00e12'> <IndicatorItem condition='contains'
id='239b8ea5-1e34-4ed6-8c4d-d346e7a871ff'> <Context document='UrlHistoryItem'
search='UrlHistoryItem/LastVisitDate' type='mir'/> <Content type='date'>2023-10-
01T16:05:00</Content> </IndicatorItem> <IndicatorItem condition='contains'
id='7fa926b8-6908-4faf-9577-16e5c3e866d1'> <Context document='PortItem'
search='PortItem/localIP' type='mir'/> <Content type='string'>192.168.1.200</Content>
</IndicatorItem> <IndicatorItem condition='contains' id='83f43db3-38a0-4071-b8e3-
a18b629fb0d9'> <Context document='RouteEntryItem' search='RouteEntryItem/Destination'
type='mir'/> <Content type='IP'>203.0.113.42</Content> </IndicatorItem>
<IndicatorItem condition='contains' id='4889310d-5c46-4186-bed8-7de0c55f784e'>
<Context document='RouteEntryItem' search='RouteEntryItem/Protocol' type='mir'/>
```

```
<Content type='string'>TCP</Content> </IndicatorItem> <IndicatorItem
condition='contains' id='c553b96e-762c-488c-a79e-fd0ffb8401bc'> <Context
document='PortItem' search='PortItem/localPort' type='mir'/> <Content
type='int'>12345</Content> </IndicatorItem> </Indicator> </Indicator> </definition>
</ioc>
```

b. CybOX Representation :

https://github.com/CybOXProject/schemas

```
<cybox:Observables
xmlns:cybox="http://cybox.mitre.org/cybox-2" >

<!-- Observable malicous URL -->
<cybox:Observable id="example:Observable-1">
<cybox:Object id="example:Object-1">
<cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">
<URIObj:Value>http://x4z9can.cn/4812/</URIObj:Value>
</cybox:Properties>
</cybox:Object>
</cybox:Observable>
<!-- Observable desstination IP -->
<cybox:Observable id="example:Observable-2">
<cybox:Object id="example:Object-2">
<cybox:Properties xsi:type="URIObject:URIObjectType" type="URL">
<URIObject:Value condition="Equals">c2-malicious-server.com</URIObject:Value>
</cybox:Properties>
</cybox:Object>
</cybox:Observable>
<!-- Observable suspicious Port -->
<cybox:Observable id="example:Observable-3">
```

```
<cybox:Object id="example:Object-3">
<cybox:Properties xsi:type="PortObj:PortObjectType">
<PortObj:Port_Value>4444</PortObj:Port_Value>
</cybox:Properties>
</cybox:Object>
</cybox:Observable>

<!-- Observable suspicious TCP connection -->
<cybox:Observable id="example:Observable-4"></cybox:Observable>
<cybox:Object id="example:Object-4">
<cybox:Properties xsi:type="NetworkConnectionObj:NetworkConnectionObjectType">
<NetworkConnectionObj:Layer3_Protocol
datatype="string">IPv4</NetworkConnectionObj:Layer3_Protocol>
<NetworkConnectionObj:Layer4_Protocol
datatype="string">TCP</NetworkConnectionObj:Layer4_Protocol>
<NetworkConnectionObj:Source_Socket_Address>
<SocketAddressObj:IP_Address>
<AddressObj:Address_Value>192.168.1.200</AddressObj:Address_Value>
</SocketAddressObj:IP_Address>
<SocketAddressObj:Port>
<PortObj:Port_Value>12345</PortObj:Port_Value>
</SocketAddressObj:Port>
</NetworkConnectionObj:Source_Socket_Address>
<NetworkConnectionObj:Destination_Socket_Address>
<SocketAddressObj:IP_Address>
<AddressObj:Address_Value>203.0.113.42</AddressObj:Address_Value>
</SocketAddressObj:IP_Address>
<SocketAddressObj:Port>
<PortObj:Port_Value>4444</PortObj:Port_Value>
```

</SocketAddressObj:Port>

</NetworkConnectionObj:Destination_Socket_Address>

</cybox:Properties>

</cybox:Object>

</cybox:Observable>

<!-- Observable suspicious mail -->

<cybox:Observable id="example:Obervable-5">

<cybox:Object id="example:Object-5">

<cybox:Properties xsi:type="EmailMessageObj:EmailMessageObjectType">

<EmailMessageObj:Header>

<EmailMessageObj:From category="e-mail">

<AddrObj:Address_Value condition="Equals" apply_condition="ANY">john.doe@XYZcompagny.com</AddrObj:Address_Value>

</EmailMessageObj:From>

<EmailMessageObj:Subject condition="Equals" >Urgent: Verify Your Account to Prevent Service Disruption</EmailMessageObj:Subject>

</EmailMessageObj:Header>

</cybox:Properties>

</cybox:Object>

</cybox:Observable>

</cybox:Observables>