Sep 13 2023

NETMANAGEIT

Intelligence Report

Attacker combines phone, email lures into believable, complex attack chain

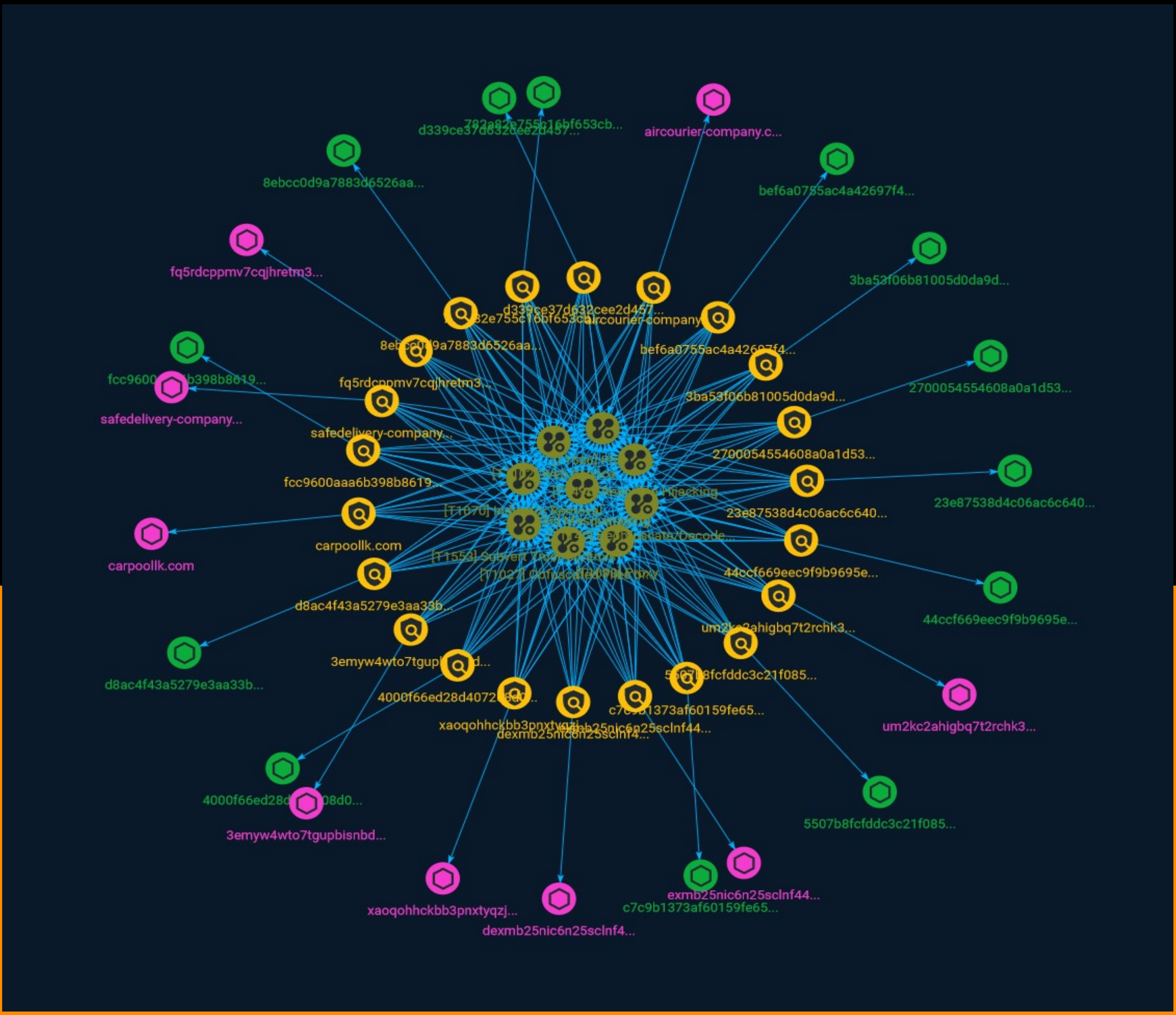

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Sophos X-Ops is investigating an attack on a Swiss government agency that compromised a computer and sent a malicious email message to an employee's computer, before the attacker pulled the plug on the computer.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

Name

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Proxy

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

Subvert Trust Controls

ID

T1553

Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

Name

Resource Hijacking

ID

T1496

Description

Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR)

Name
Obfuscated Files or Information
ID
T1027
Description
Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)
Name
Web Service
ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Indicator

Name

3emyw4wto7tgupbisnbdbkbyaamb7p7dpxp6lnfqwyemskmmar3fugad.onion

Pattern Type

stix

Pattern

[domain-name:value = '3emyw4wto7tgupbisnbdbkbyaamb7p7dpxp6lnfqwyemskmmar3fugad.onion']

Name

aircourier-company.com

Pattern Type

stix

Pattern

[domain-name:value = 'aircourier-company.com']

Name

c7c9b1373af60159fe65915116a961be0e74c3719c2f482c91ca88dd738bff78

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c7c9b1373af60159fe65915116a961be0e74c3719c2f482c91ca88dd738bff78']

Name

safedelivery-company.com

Pattern Type

stix

Pattern

[domain-name:value = 'safedelivery-company.com']

Name

2700054554608a0a1d53fd65067b19d3a1dc0297d6bcfcc4292eec37cde07c18

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2700054554608a0a1d53fd65067b19d3a1dc0297d6bcfcc4292eec37cde07c18']

Name

xaoqohhckbb3pnxtyqzj6pkuzckt2urbeiyd5xlanmw52expmohl7dyd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'xaoqohhckbb3pnxtyqzj6pkuzckt2urbeiyd5xlanmw52expmohl7dyd.onion']

Name

782a82e755c16bf653cb3ab5a65bb58638a16cf2b04e1f1cf454b9bced91a81b

Description

research_pe_signed_outside_timestamp

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '782a82e755c16bf653cb3ab5a65bb58638a16cf2b04e1f1cf454b9bced91a81b']

Name

um2kc2ahigbq7t2rchk3tnxnjzvrddbhxkcy573dqxci44wvi4ge5cad.onion

Pattern Type

stix

Pattern

[domain-name:value =
'um2kc2ahigbq7t2rchk3tnxnjzvrddbhxkcy573dqxci44wvi4ge5cad.onion']

Name

carpoollk.com

Pattern Type

stix

Pattern

[domain-name:value = 'carpoollk.com']

Name

bef6a0755ac4a42697f45843562cc7ce7d1454a85bddc458d2cd99658cf57b71

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'bef6a0755ac4a42697f45843562cc7ce7d1454a85bddc458d2cd99658cf57b71']

Name

exmb25nic6n25sclnf44rrgynquns7u3zjqa33x3uztwbmsuptf7gyid.onion

Pattern Type

stix

Pattern

[domain-name:value =
'exmb25nic6n25sclnf44rrgynquns7u3zjqa33x3uztwbmsuptf7gyid.onion']

Name

fq5rdcppmv7cqjhretm3owbnj4hskcv37bcgx5rpbdbhqfefzix4tiyd.onion

Pattern Type

stix

Pattern

[domain-name:value =
'fq5rdcppmv7cqjhretm3owbnj4hskcv37bcgx5rpbdbhqfefzix4tiyd.onion']

Name

23e87538d4c06ac6c640fe8dbe6992bf652ecdcaa1f0cf9b5e5108d0655fe2c7

Description

research_pe_signed_outside_timestamp

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '23e87538d4c06ac6c640fe8dbe6992bf652ecdcaa1f0cf9b5e5108d0655fe2c7']

Name

4000f66ed28d407208d0e87875ffa0a55d4079955089e6c2a6d5a057b33841f6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4000f66ed28d407208d0e87875ffa0a55d4079955089e6c2a6d5a057b33841f6']

Name

d339ce37d632cee2d457c21b8dbe04fe69930cde0cea13a96593403130abdb54

Description

Nullsoft_NSIS

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd339ce37d632cee2d457c21b8dbe04fe69930cde0cea13a96593403130abdb54']

Name

5507b8fcfddc3c21f08551a2388fdf4c41fd13531dfed1d6b6d20388440f34db

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5507b8fcfddc3c21f08551a2388fdf4c41fd13531dfed1d6b6d20388440f34db']

Name

fcc9600aaa6b398b861962bb5ef8cd88072be3c619c235e890909e4f12374005

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fcc9600aaa6b398b861962bb5ef8cd88072be3c619c235e890909e4f12374005']

Name

3ba53f06b81005d0da9dc2e83feb4dd983884ef5533fcec2e8e3772e1ee1a615

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'3ba53f06b81005d0da9dc2e83feb4dd983884ef5533fcec2e8e3772e1ee1a615']

Name

dexmb25nic6n25sclnf44rrgynquns7u3zjqa33x3uztwbmsuptf7gyid.onion

Pattern Type

stix

Pattern

[domain-name:value =
'dexmb25nic6n25sclnf44rrgynquns7u3zjqa33x3uztwbmsuptf7gyid.onion']

Name

8ebcc0d9a7883d6526aad38492aa6f2d2192a817591aeb4b971cb2ba3d447ef0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'8ebcc0d9a7883d6526aad38492aa6f2d2192a817591aeb4b971cb2ba3d447ef0']

Name

44ccf669eec9f9b9695e0eb255b729df14f63485d85faf5375b5e7efb35a9d3e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'44ccf669eec9f9b9695e0eb255b729df14f63485d85faf5375b5e7efb35a9d3e']

Name

d8ac4f43a5279e3aa33b2a743e17e1c59ba170c74965c45feca529fd8e817140

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'd8ac4f43a5279e3aa33b2a743e17e1c59ba170c74965c45feca529fd8e817140']

Domain-Name

Value
exmb25nic6n25sclnf44rrgynquns7u3zjqa33x3uztwbmsuptf7gyid.onion
3emyw4wto7tgupbisnbdbkbyaamb7p7dpxp6lnfqwyemskmmar3fugad.onion
aircourier-company.com
dexmb25nic6n25sclnf44rrgynquns7u3zjqa33x3uztwbmsuptf7gyid.onion
safedelivery-company.com
carpoollk.com
fq5rdcppmv7cqjhretm3owbnj4hskcv37bcgx5rpbdbhqfefzix4tiyd.onion
xaoqohhckbb3pnxtyqzj6pkuzckt2urbeiyd5xlanmw52expmohl7dyd.onion
um2kc2ahigbq7t2rchk3tnxnjzvrddbhxkcy573dqxci44wvi4ge5cad.onion

StixFile

Value
5507b8fcfddc3c21f08551a2388fdf4c41fd13531dfed1d6b6d20388440f34db
782a82e755c16bf653cb3ab5a65bb58638a16cf2b04e1f1cf454b9bced91a81b
8ebcc0d9a7883d6526aad38492aa6f2d2192a817591aeb4b971cb2ba3d447ef0
4000f66ed28d407208d0e87875ffa0a55d4079955089e6c2a6d5a057b33841f6
3ba53f06b81005d0da9dc2e83feb4dd983884ef5533fcec2e8e3772e1ee1a615
c7c9b1373af60159fe65915116a961be0e74c3719c2f482c91ca88dd738bff78
bef6a0755ac4a42697f45843562cc7ce7d1454a85bddc458d2cd99658cf57b71
2700054554608a0a1d53fd65067b19d3a1dc0297d6bcfcc4292eec37cde07c18
44ccf669eec9f9b9695e0eb255b729df14f63485d85faf5375b5e7efb35a9d3e
d8ac4f43a5279e3aa33b2a743e17e1c59ba170c74965c45feca529fd8e817140
d339ce37d632cee2d457c21b8dbe04fe69930cde0cea13a96593403130abdb54
fcc9600aaa6b398b861962bb5ef8cd88072be3c619c235e890909e4f12374005
23e87538d4c06ac6c640fe8dbe6992bf652ecdcaa1f0cf9b5e5108d0655fe2c7

External References

- https://otx.alienvault.com/pulse/6501bfd29568305b0a5a9c4f
- https://news.sophos.com/en-us/2023/08/10/image-spam-attack/
- https://github.com/sophoslabs/IoCs/blob/master/IOC_imagespam.csv