Dec 12 2023

NETMANAGEIT

Intelligence Report

MrAnon Stealer Spreads via Email with Fake Hotel Booking PDF.

Table of contents

Overview

Entities

Observables

External References

Overview

Description

FortiGuard Labs uncovers a sophisticated phishing campaign deploying MrAnon Stealer via fake booking PDF. The threat actor sends phishing emails with fake room booking details, aiming at specific regions. The malware uses PowerGUI and cx-Freeze tools to create a complex process that involves .NET executable files and PowerShell scripts. The attacker also uses tricks like false error messages to hide successful infections. The malware downloads and extracts files from a specific domain to run a harmful Python script.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

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

Masquerade as Legitimate Application

ID

T1444

Description

An adversary could distribute developed malware by masquerading the malware as a legitimate application. This can be done in two different ways: by embedding the malware in a legitimate application, or by pretending to be a legitimate application. Embedding the malware in a legitimate application is done by downloading the application, disassembling it, adding the malicious code, and then re-assembling it.(Citation: Zhou) The app would appear to be the original app, but would contain additional malicious functionality. The adversary could then publish the malicious application to app stores or use another delivery method. Pretending to be a legitimate application relies heavily on lack of scrutinization by the user. Typically, a malicious app pretending to be a legitimate one will have many similar details as the legitimate one, such as name, icon, and description. (Citation: Palo Alto HenBox) Malicious applications may also masquerade as legitimate applications when requesting access to the accessibility service in order to appear as legitimate to the user, increasing the likelihood that the access will be granted.

Indicator

Name
48e09b8043c0d5dfc2047b573112ead889b112108507d400d2ce3db18987f6c9
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '48e09b8043c0d5dfc2047b573112ead889b112108507d400d2ce3db18987f6c9']
Name
96ec8ef2338d36b7122a76b0398d97e8d0ed55c85e31649ea00e57d6b1f53628
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '96ec8ef2338d36b7122a76b0398d97e8d0ed55c85e31649ea00e57d6b1f53628']
Name

45ee224e571d0fd3a72af1d7a7718e61a1aad03b449cf85377411d51c135bb22

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '45ee224e571d0fd3a72af1d7a7718e61a1aad03b449cf85377411d51c135bb22']

Name

0efba3964f4b760965e94b4d1a597e6cd16241b8c8bf77a664d6216d1420b312

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0efba3964f4b760965e94b4d1a597e6cd16241b8c8bf77a664d6216d1420b312']

Name

8a8c9acf09c84ab5ea4c098eace93888a88b82a1485255073c93ce6080d05ec7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8a8c9acf09c84ab5ea4c098eace93888a88b82a1485255073c93ce6080d05ec7']

Name

anonbin.ir

Pattern Type

stix

Pattern

[domain-name:value = 'anonbin.ir']

Name

8b71525ca378463784ce2d81a8371714580c58f0d305a2aa4630dc964c8c0ee0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8b71525ca378463784ce2d81a8371714580c58f0d305a2aa4630dc964c8c0ee0']

Name

anoncrypter.com

Pattern Type

stix

Pattern
[domain-name:value = 'anoncrypter.com']
Name
075e40be20b4bc5826aa0b031c0ba8355711c66c947bbbaf926b92edb2844cb0
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '075e40be20b4bc5826aa0b031c0ba8355711c66c947bbbaf926b92edb2844cb0']

Domain-Name

Value
anonbin.ir
anoncrypter.com

StixFile

Value
45ee224e571d0fd3a72af1d7a7718e61a1aad03b449cf85377411d51c135bb22
075e40be20b4bc5826aa0b031c0ba8355711c66c947bbbaf926b92edb2844cb0
8a8c9acf09c84ab5ea4c098eace93888a88b82a1485255073c93ce6080d05ec7
8b71525ca378463784ce2d81a8371714580c58f0d305a2aa4630dc964c8c0ee0
48e09b8043c0d5dfc2047b573112ead889b112108507d400d2ce3db18987f6c9
0efba3964f4b760965e94b4d1a597e6cd16241b8c8bf77a664d6216d1420b312
96ec8ef2338d36b7122a76b0398d97e8d0ed55c85e31649ea00e57d6b1f53628

External References

- https://otx.alienvault.com/pulse/657882055fb217d3766c1f56
- https://www.fortinet.com/blog/threat-research/mranon-stealer-spreads-via-email-with-fake-hotel-booking-pdf