Dec 12 2023

NETMANAGEIT

Intelligence Report

Security Brief: TA4557 Targets Recruiters Directly via Email

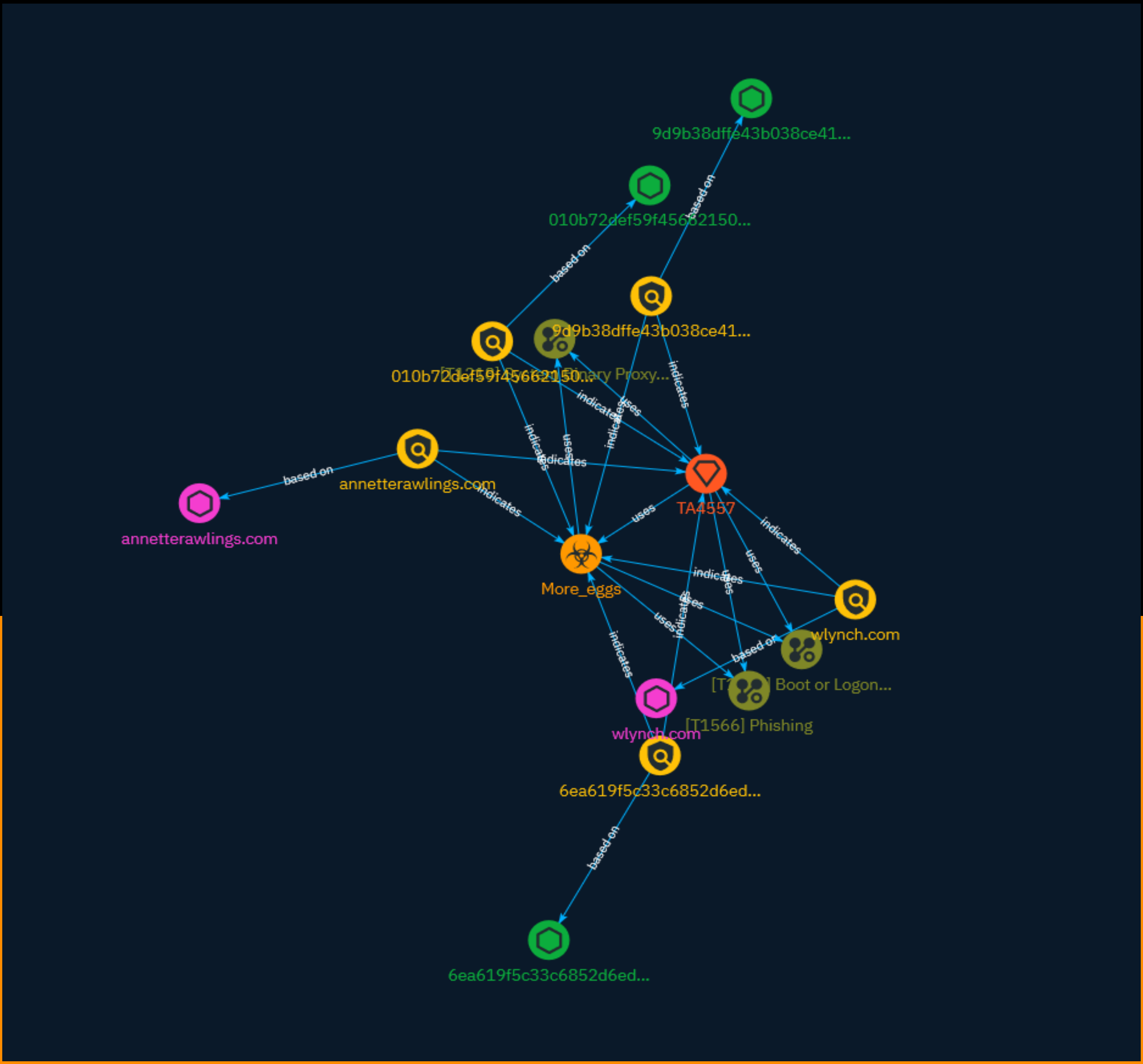

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Since at least October 2023, TA4557 began using a new technique of targeting recruiters with direct emails that ultimately lead to malware delivery. The initial emails are benign and express interest in an open role. If the target replies, the attack chain commences.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Boot or Logon Autostart Execution
ID
T1547
Description
Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.
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

System Binary Proxy Execution

ID

T1218

Description

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

Indicator

Name

6ea619f5c33c6852d6ed11c52b52589b16ed222046d7f847ea09812c4d51916d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6ea619f5c33c6852d6ed11c52b52589b16ed222046d7f847ea09812c4d51916d']

Name

010b72def59f45662150e08bb80227fe8df07681dcf1a8d6de8b068ee11e0076

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '010b72def59f45662150e08bb80227fe8df07681dcf1a8d6de8b068ee11e0076']

Name

wlynch.com

Pattern Type

stix

Pattern

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

Name

annetterawlings.com

Pattern Type

stix

Pattern

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

Name

9d9b38dffe43b038ce41f0c48def56e92dba3a693e3b572dbd13d5fbc9abc1e4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9d9b38dffe43b038ce41f0c48def56e92dba3a693e3b572dbd13d5fbc9abc1e4']

Intrusion-Set

Name
TA4557

Malware

Name
More_eggs
Description
[More_eggs](https://attack.mitre.org/software/S0284) is a JScript backdoor used by [Cobalt Group](https://attack.mitre.org/groups/G0080) and [FIN6](https://attack.mitre.org/groups/G0037). Its name was given based on the variable "More_eggs" being present in its code. There are at least two different versions of the backdoor being used, version 2.0 and version 4.4. (Citation: Talos Cobalt Group July 2018)(Citation: Security Intelligence More Eggs Aug 2019)

Domain-Name

Value
annetterawlings.com
wlynch.com

StixFile

Value
010b72def59f45662150e08bb80227fe8df07681dcf1a8d6de8b068ee11e0076
6ea619f5c33c6852d6ed11c52b52589b16ed222046d7f847ea09812c4d51916d
9d9b38dffe43b038ce41f0c48def56e92dba3a693e3b572dbd13d5fbc9abc1e4

External References

- https://otx.alienvault.com/pulse/6578960a6018330ac6e00f43
- https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta4557-targets-recruiters-directly-email