Mar 21 2024

NETMANAGEIT

Intelligence Report

Security Brief: TA450 Uses Embedded Links in PDF Attachments in Latest Campaign

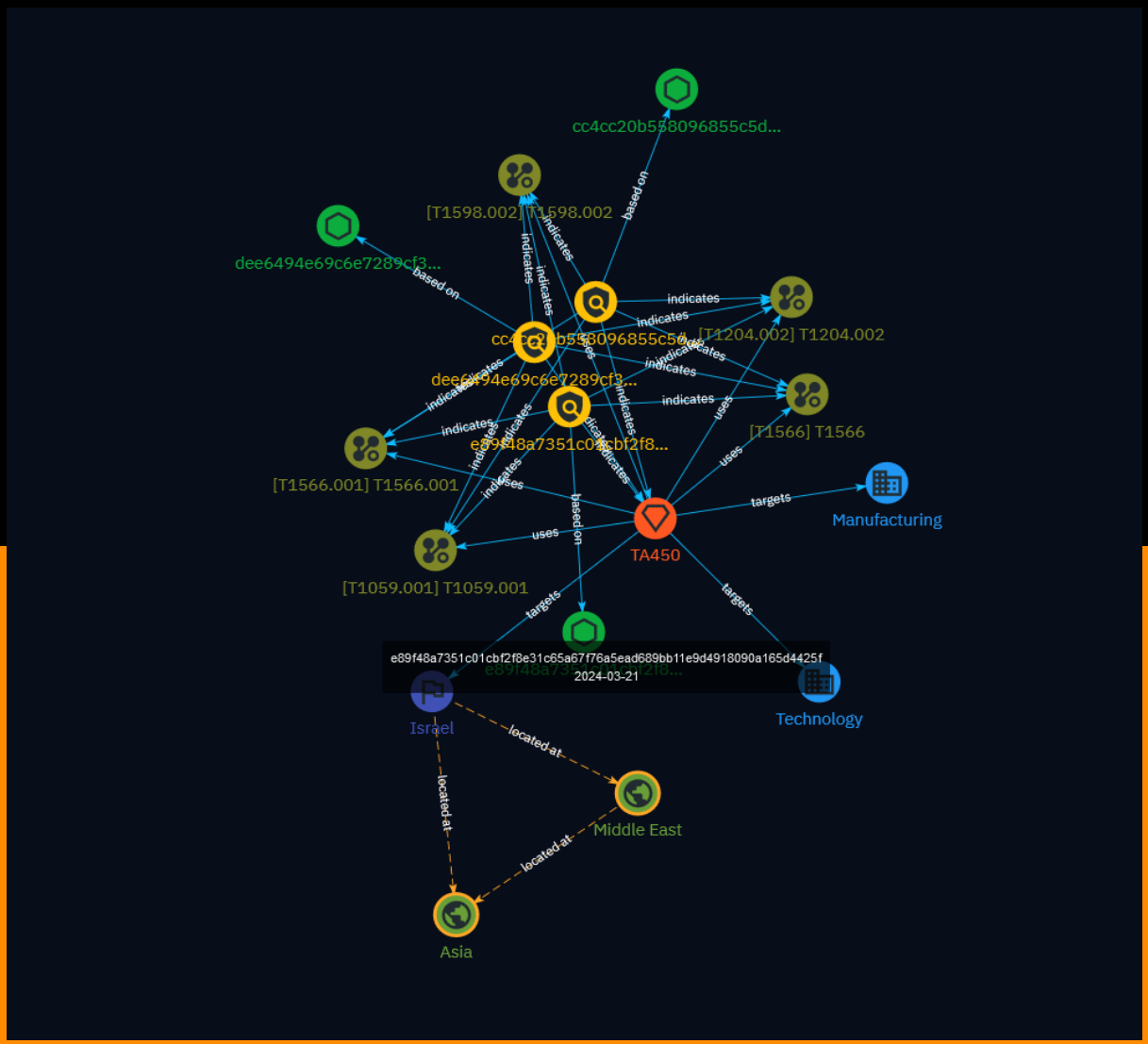

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Intrusion-Set 8
- Attack-Pattern 9
- Country 13
- Region 14
- Sector 15

Observables

- StixFile 16

External References

- External References 17

Overview

Description

Proofpoint researchers recently observed new activity by the Iran-aligned threat actor TA450, known for targeting Israeli entities, in which the group used a pay-related social engineering lure to target Israeli employees at large multinational organizations. In the phishing campaign, TA450 sent emails with PDF attachments containing malicious links leading to the download of remote administration software known to be abused by TA450. This activity continues TA450's trend of leveraging Hebrew language lures and compromised Israeli accounts to target individuals at companies with an Israeli footprint.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
dee6494e69c6e7289cf3f332e2867662958fa82f819615597e88c16c967a25a9
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'dee6494e69c6e7289cf3f332e2867662958fa82f819615597e88c16c967a25a9']
Name
e89f48a7351c01cbf2f8e31c65a67f76a5ead689bb11e9d4918090a165d4425f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e89f48a7351c01cbf2f8e31c65a67f76a5ead689bb11e9d4918090a165d4425f']
Name

cc4cc20b558096855c5d492f7a79b160a809355798be2b824525c98964450492

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cc4cc20b558096855c5d492f7a79b160a809355798be2b824525c98964450492']

Intrusion-Set

Name
TA450

Attack-Pattern

Name
T1059.001
ID
T1059.001
Description
Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)
Name

T1598.002

ID

T1598.002

Description

Adversaries may send spearphishing messages with a malicious attachment to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon the recipient populating information then returning the file.(Citation: Sophos Attachment)(Citation: GitHub Phishery) The text of the spearphishing email usually tries to give a plausible reason why the file should be filled-in, such as a request for information from a business associate. Adversaries may also use information from previous reconnaissance efforts (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)) to craft persuasive and believable lures.

Name

T1566

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

T1566.001

ID

T1566.001

Description

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](https://attack.mitre.org/techniques/T1204) to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted source. There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible

reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

Name

T1204.002

ID

T1204.002

Description

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

Country

Name
Israel

Region

Name
Middle East

Name
Asia

Sector

Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Technology
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

StixFile

Value
e89f48a7351c01cbf2f8e31c65a67f76a5ead689bb11e9d4918090a165d4425f
dee6494e69c6e7289cf3f332e2867662958fa82f819615597e88c16c967a25a9
cc4cc20b558096855c5d492f7a79b160a809355798be2b824525c98964450492

External References

- https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta450-uses-embedded-links-pdf-attachments-latest-campaign
- https://otx.alienvault.com/pulse/65fc927506c4feecdf1d0391