


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

 proofpoint.com/us/blog/threat-insight/security-brief-ta450-uses-embedded-links-pdf-attachments-latest-campaign

March 21, 2024



[Blog](#)

[Threat Insight](#)

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



Share with your network!

March 21, 2024 Joshua Miller and the Proofpoint Threat Research Team

What happened

Proofpoint researchers recently observed new activity by the Iran-aligned threat actor TA450 (also known as MuddyWater, Mango Sandstorm, and Static Kitten), in which the group used a pay-related social engineering lure to target Israeli employees at large multinational organizations. TA450 is known for targeting Israeli entities particularly since at least October 2023 with the start of the Israel-Hamas war and this continues that trend with a focus on global manufacturing, technology, and information security companies.

In the phishing campaign, which started 7 March and continued through the week of 11 March 2024, TA450 sent emails with PDF attachments that contained malicious links. While this method is not foreign to TA450, the threat actor has more recently relied on including malicious links directly in email message bodies instead of adding in this extra step. Proofpoint researchers observed the same targets receive multiple phishing emails with PDF attachments that had slightly different embedded links. The links were to a variety of file-sharing sites, including Egnyte, Onehub, Sync and TeraBox. The emails also used a likely compromised .IL sender account, which is consistent with this threat actor's recent activity.

As seen in Figures 1 and 2, if a target opened the attachment and clicked on the included link, it would lead to the download of a ZIP archive containing a compressed MSI that ultimately would install AteraAgent, remote administration software that is known to be abused by TA450.

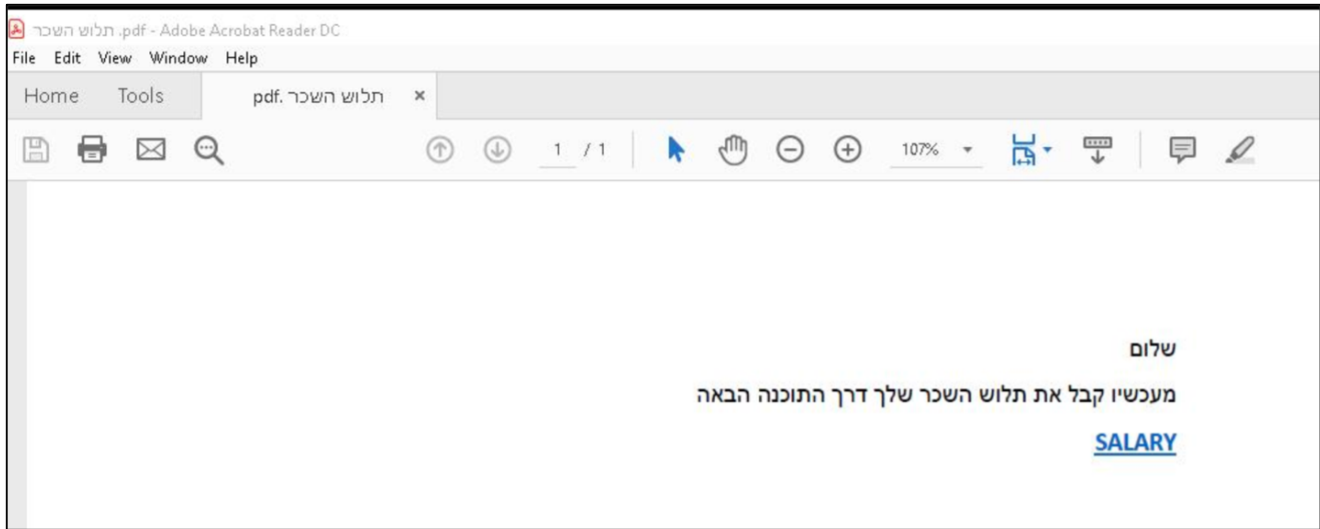


Figure 1. Opened PDF attachment with malicious link (Machine translation: Document title: Pay Slip; Body of PDF: Hello, From now on receive your pay slip through the following software).

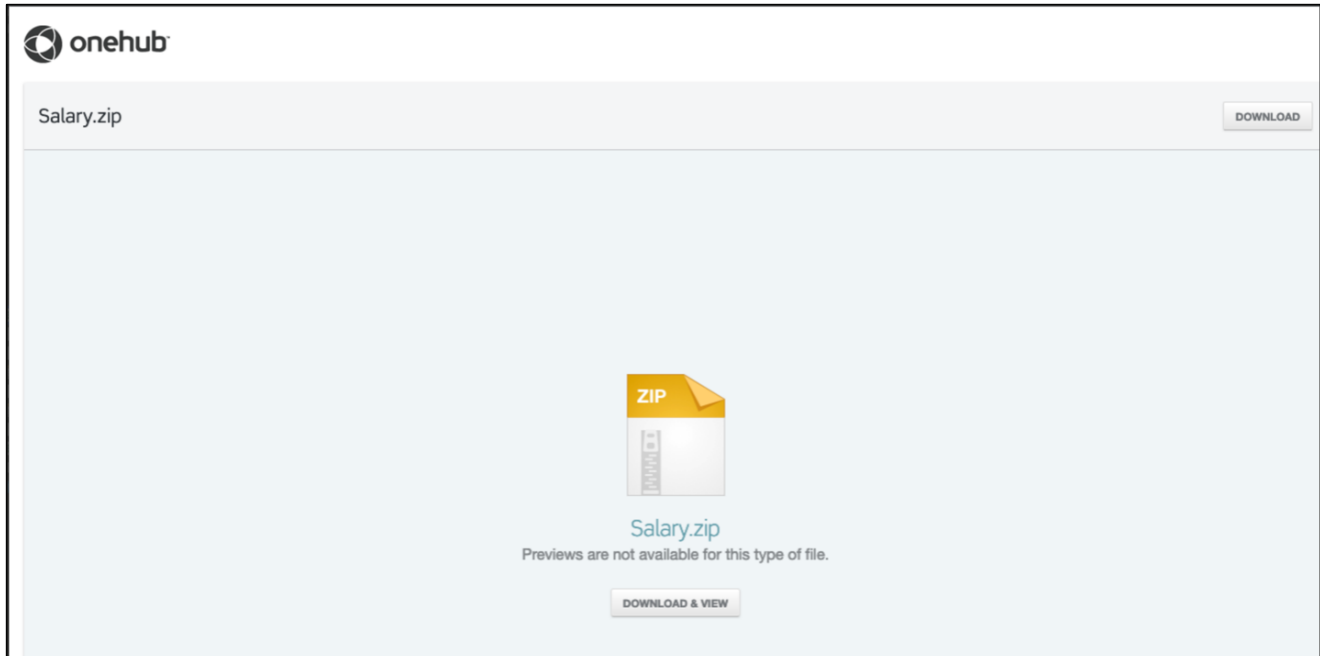


Figure 2. ZIP archive via Onehub that leads to the download of remote administration software.

Attribution

Proofpoint researchers attribute this campaign to TA450 based on known TA450 tactics, techniques, and procedures, campaign targeting, and malware analysis. In January 2022, the United States Cyber Command attributed this group to Iran's Ministry of Intelligence and Security.

Why it matters

This activity is notable for several reasons, including that it marks a turn in TA450's tactics. While this campaign is not the first observed instance of TA450 using attachments with malicious links as part of the threat actor's attack chain, it is the first time Proofpoint researchers have observed TA450 attempt to deliver a malicious URL in a PDF attachment rather than directly linking the file in an email. Additionally, this campaign is the first time Proofpoint has observed TA450 using a sender email account that matches the lure content. For example, this campaign used an email account of salary[<@>compromisedorg>.co[.jil, which is in alignment with the various pay-themed subject lines.

Finally, this activity continues TA450's trend of leveraging Hebrew language lures and compromised .IL accounts to target Israeli individuals belonging to large multinational companies, maintaining a heightened risk for organizations with this type of footprint.

Emerging Threat (ET) signatures

SID	Rule Name
2051743	ET OPEN DNS Query to File Sharing Domain (egnyte .com)
2051745	ET OPEN 2051745 - DNS Query to File Sharing Domain (sync .com)
2051749	ET OPEN DNS Query to File Sharing Domain (terabox .com)
2051750	ET OPEN Observed File Sharing Domain (terabox .com in TLS SNI)
2051746	ET OPEN Observed File Sharing Domain (egnyte .com in TLS SNI)
2051748	ET OPEN Observed File Sharing Domain (sync .com in TLS SNI)

Indicators of compromise (IOCs)

Indicator	Type
salary <salary[<@>compromisedorg>.co[.jil	Example of compromised email sender
תלושי השכר (Machine translation: Pay slip)	Email subject

02/2024 תלוש שכר לחודש (Machine translation: Pay slip for the month 02/2024)	Email subject
שכר לתלוש שכר (Machine translation: Pay slip password)	Email subject
תלוש השכר.pdf (Machine translation: Pay slip)	Document title
dee6494e69c6e7289cf3f332e2867662958fa82f819615597e88c16c967a25a9	SHA256 (PDF)
hxxp://ws.onehub[.]com/files/[alphanumericidentifier]	Example malicious URL
hxxps://salary.egnyte[.]com/[alphanumericidentifier]	Example malicious URL
hxxps://ln5.sync[.]com/[alphanumericidentifier]	Example malicious URL
hxxps://terabox[.]com/s/[alphanumericidentifier]	Example malicious URL
cc4cc20b558096855c5d492f7a79b160a809355798be2b824525c98964450492	SHA256 (salary.zip)
e89f48a7351c01cbf2f8e31c65a67f76a5ead689bb11e9d4918090a165d4425f	SHA256 (salary.msi)

Subscribe to the Proofpoint Blog