

Crossed wires: a case study of Iranian espionage and attribution

By Saher Naumaan and the Proofpoint Threat Research Team

Published: 2025-10-28 · Archived: 2026-10-14 02:02:23 UTC

Proofpoint would like to thank Josh Miller for his initial research on UNK_SmudgedSerpent and contribution to this report.

Key findings

- Between June and August 2025, Proofpoint began tracking a previously unidentified threat actor dubbed UNK_SmudgedSerpent targeting academics and foreign policy experts.
- UNK_SmudgedSerpent leveraged domestic political lures, including societal change in Iran and investigation into the militarization of the IRGC.
- UNK_SmudgedSerpent used benign conversation starters, health-themed infrastructure, OnlyOffice file hosting spoofs, and Remote Management & Monitoring (RMM) tools.
- Throughout the investigation, UNK_SmudgedSerpent demonstrated tactics resembling several Iranian actors: TA455 (C5 Agent, Smoke Sandstorm), TA453 (Charming Kitten, Mint Sandstorm), and TA450 (MuddyWater, Mango Sandstorm).
- Overlapping TTPs prevent high confidence attribution, but several hypotheses could explain the nature of the relationship between UNK_SmudgedSerpent and other Iranian groups.

Overview

In June, Proofpoint Threat Research began investigating a benign email discussing economic uncertainty and domestic political unrest in Iran. While coinciding with the escalations in the [Iran-Israel conflict](#), there was no indication that the observed activity was directly correlated with Israel's attacks on Iranian nuclear facilities or Iran's actions in response.

Initial analysis of the activity found tactics, techniques, and procedures (TTP) overlaps with multiple Iranian aligned groups, including TA455 (C5 Agent, Smoke Sandstorm), TA453 (Mint Sandstorm, Charming Kitten), and TA450 (MuddyWater, Mango Sandstorm). Given a lack of high confidence links to any one established threat group, we designated the activity as a temporary cluster called UNK_SmudgedSerpent.

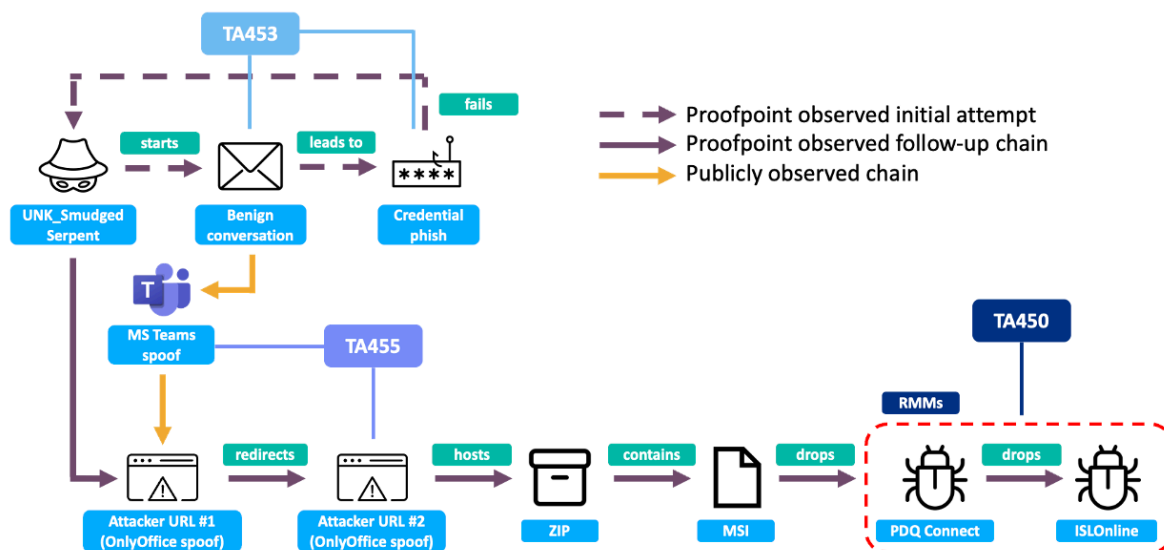


Figure 1. UNK_SmudgedSerpent infection chain with known actor overlaps.

The infection chain began with a benign conversation, followed by an email exchange and a credential harvesting attempt. After this initial credential harvesting attempt, UNK_SmudgedSerpent continued to conduct phishing activity within the same email thread with a specific target and subsequently delivered a URL that hosted an archive file with an MSI that loaded RMM payloads.

Iranian connections

Initial TA453 leads

UNK_SmudgedSerpent's first identified campaign within Proofpoint data spoofed a member of the Brookings Institute reaching out to over 20 members of a United States-based think tank in mid-June 2025. Targeting specific subject matter experts in Iran-related policy areas is often a characteristic of TA453 activity, particularly using a benign conversation starter. However, approaching a significant number of individuals at a single organization diverges from Proofpoint Threat Research's observations of typical TA453 techniques.

In another deviation from typical TA453 activity, members of the targeted organization focused across almost all areas of expertise including national defense, advanced technology, economic security, and global health, along with region-specific experts. TA453 primarily focuses on Middle Eastern policy topics, such as Iranian nuclear negotiations or Iran's foreign relations. Regardless of each recipient's expertise, UNK_SmudgedSerpent leveraged the same collaboration lure about impending Iranian societal reform.

The attackers' approach impersonated Suzanne Maloney – the vice president and director of the Foreign Policy program at the Brookings Institution and an expert on Iran – using a Gmail address and misspelled version of her name, "Suzzane Maloney."

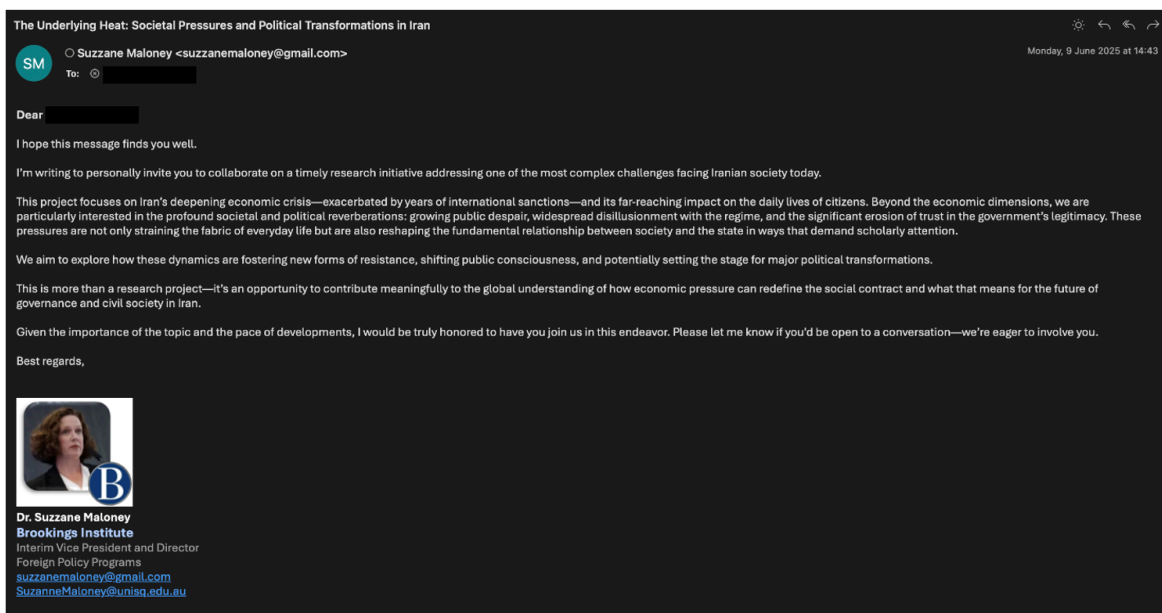


Figure 2. UNK_SmudgedSerpent initial approach.

Following a response, the Suzzane Maloney persona was more cautious than Proofpoint has observed in past interactions with TA453. The attacker insisted on verifying the identity of the target and authenticity of the email address before proceeding with any collaboration attempts.

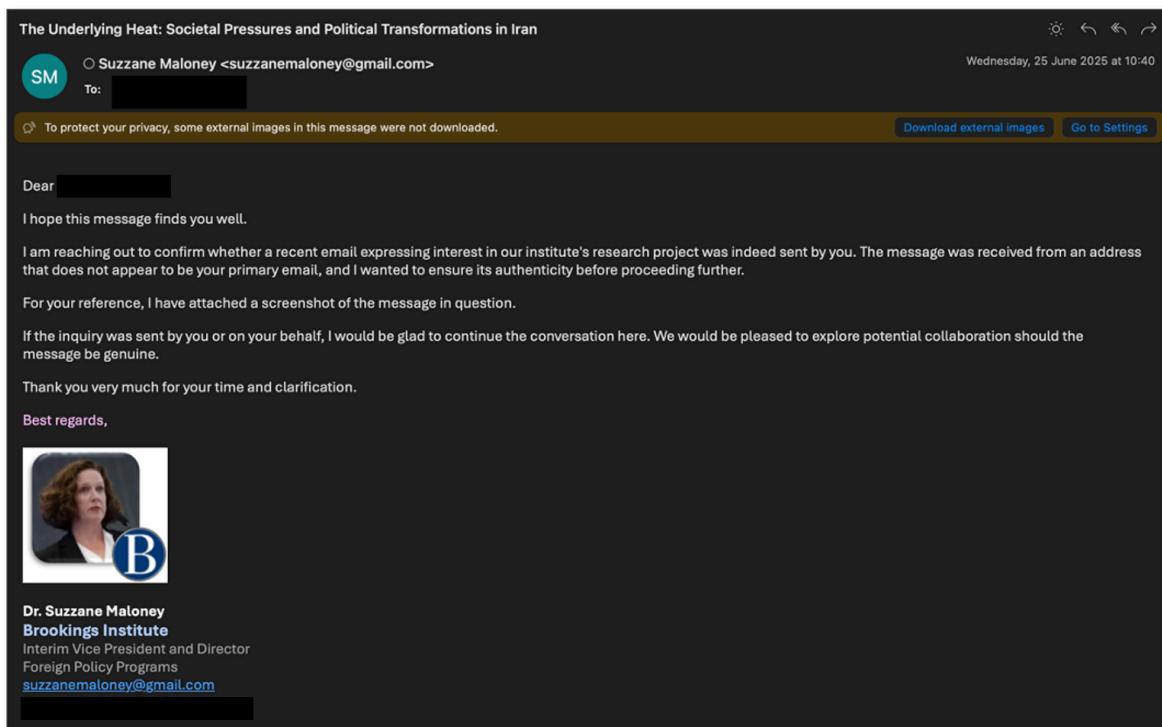


Figure 3. *UNK_SmudgedSerpent follow-up email.*

As the engagement continued, the persona sent an appointed time for a meeting, using Israel time as a point of reference though the target was based in the US. At the delivery stage, the actor began to deviate from TA453's typical TTPs and sent a link appearing to be an OnlyOffice URL belonging to "Suzzane Maloney" (again spelled incorrectly) with documents relevant to the upcoming meeting.

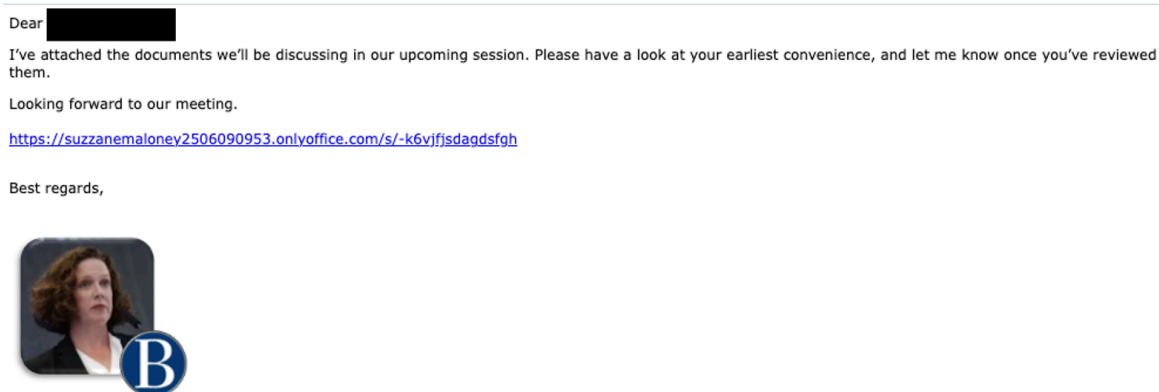


Figure 4. *UNK_SmudgedSerpent URL delivery.*

Transition to TA455

The URL was only masquerading as an OnlyOffice link in the email but instead hyperlinked to a health-themed attacker domain thebesthomehealth[.]com, which redirected to a second health-themed attacker domain mosaichealthsolutions[.]com that displayed a Microsoft 365 login page. The URL hosted a customized credential harvesting page with the user's information pre-loaded.

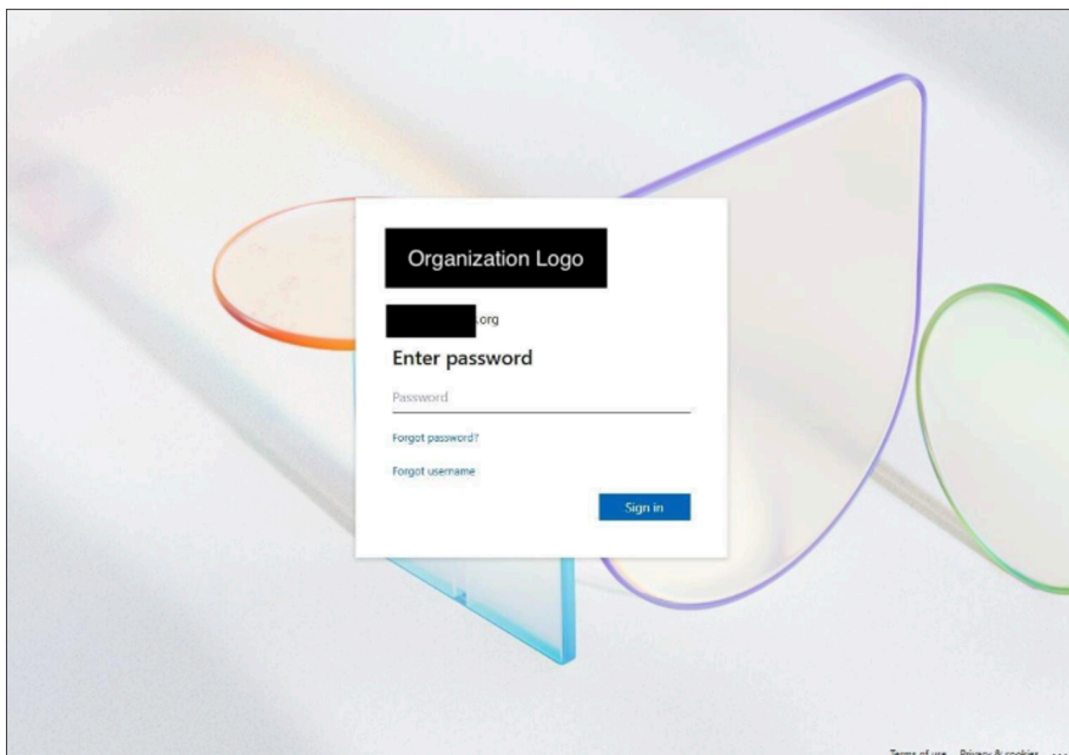


Figure 5. Customized Microsoft credential harvesting page.

Delivery variation

Another version of this infection chain can be found on VirusTotal, where both domains were similarly used in a Microsoft-related redirection chain. `hxxps://thebesthomehealth[.]com/[redacted15characterstring]` masqueraded as a Microsoft Teams login before redirecting to the `mosaichealthsolutions[.]com` domain.

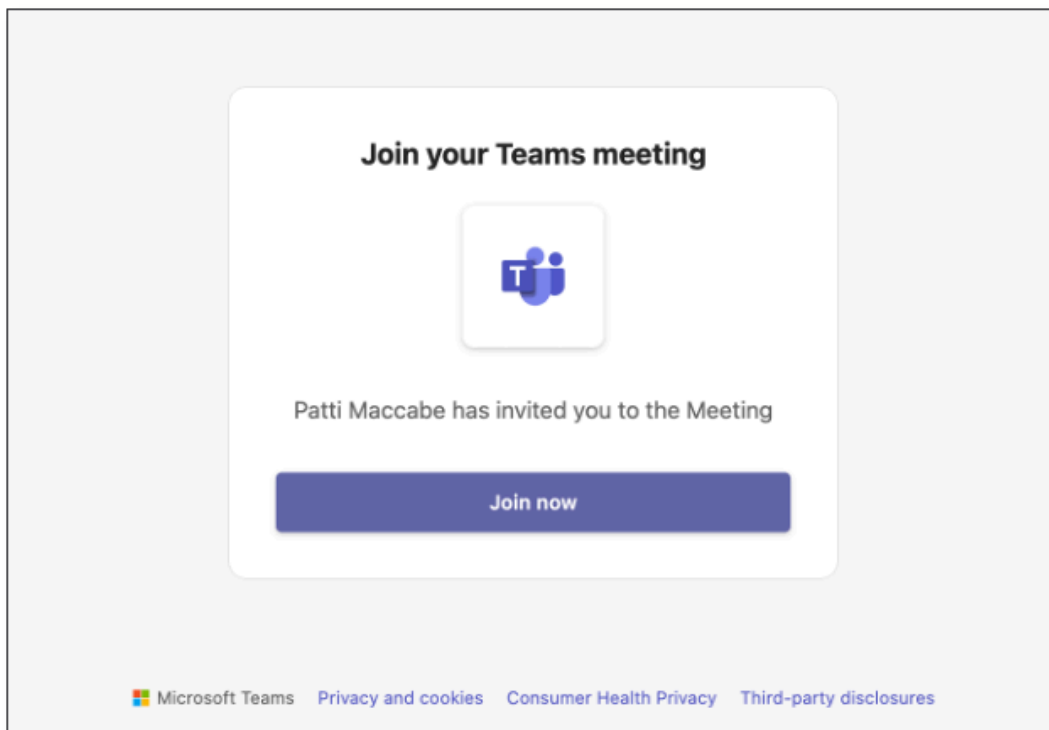


Figure 6. Microsoft Teams meeting spoof (VirusTotal).

However, the next stages following clicking the “Join Now” button are unclear at the time of writing.

TA455 continued

In Proofpoint’s investigation, after the target communicated suspicions about the credential harvesting page, UNK_SmudgedSerpent removed the password requirement on the initial thebesthomehealth[.]com URL. The link then proceeded to a spoofed OnlyOffice login page.

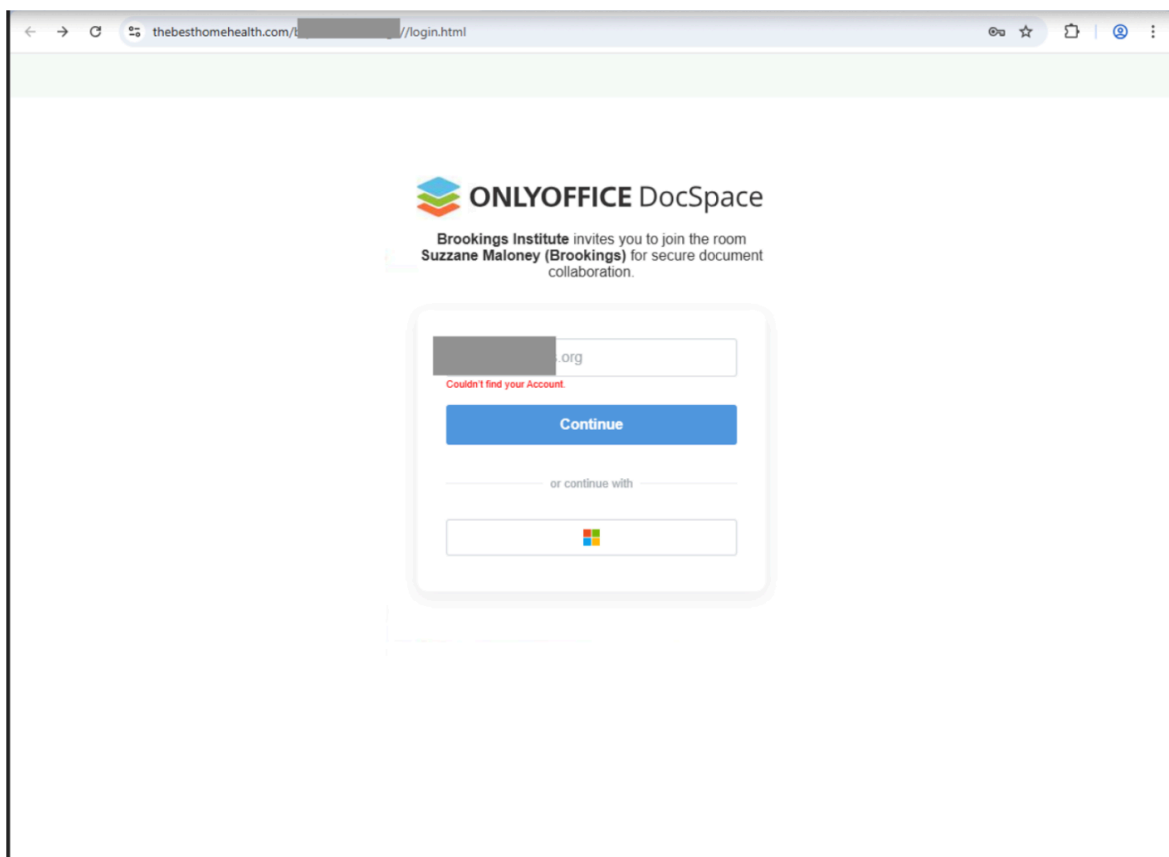


Figure 7. UNK_SmudgedSerpent OnlyOffice login spoof.

Clicking on “Continue” or login loads another page also hosted on thebesthomehealth[.]com, which continues to resemble OnlyOffice and hosted two PDFs, an Excel document, and a ZIP archive.

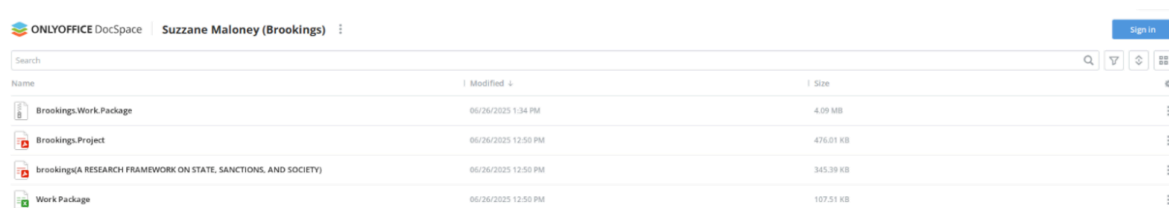


Figure 8. Files hosted on thebesthomehealth[.]com.

UNK_SmudgedSerpent’s reference to OnlyOffice URLs and health-themed domains is reminiscent of TA455 activity. TA455 began registering health-related domains at least since October 2024 following a consistent stream of domains with aerospace interest, with OnlyOffice becoming popular to host files more recently in June 2025, as shown by the timeline below.

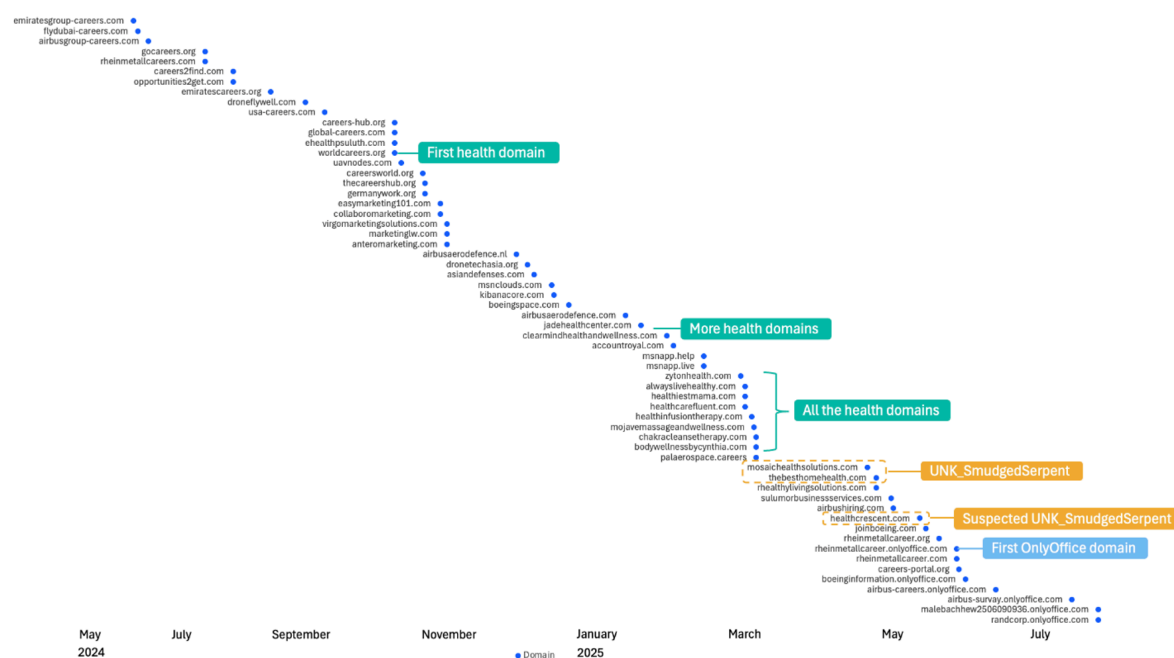


Figure 9. TA455 Domain Registration / First Seen Timeline (May 2024 – July 2025).

UNK_SmudgedSerpent domains began appearing in April 2025, several weeks before the first campaign was observed in June.

Completing the chain with TA450

Upon execution, UNK_SmudgedSerpent's ZIP archive loaded an MSI file, which launched the PDQConnect Remote Monitoring & Management (RMM) software. The rest of the documents appeared to be decoys.

During our research, Threat Research observed UNK_SmudgedSerpent engaging in suspected hands-on-keyboard activity where the attackers leveraged PDQConnect to install additional RMM software, ISL Online.

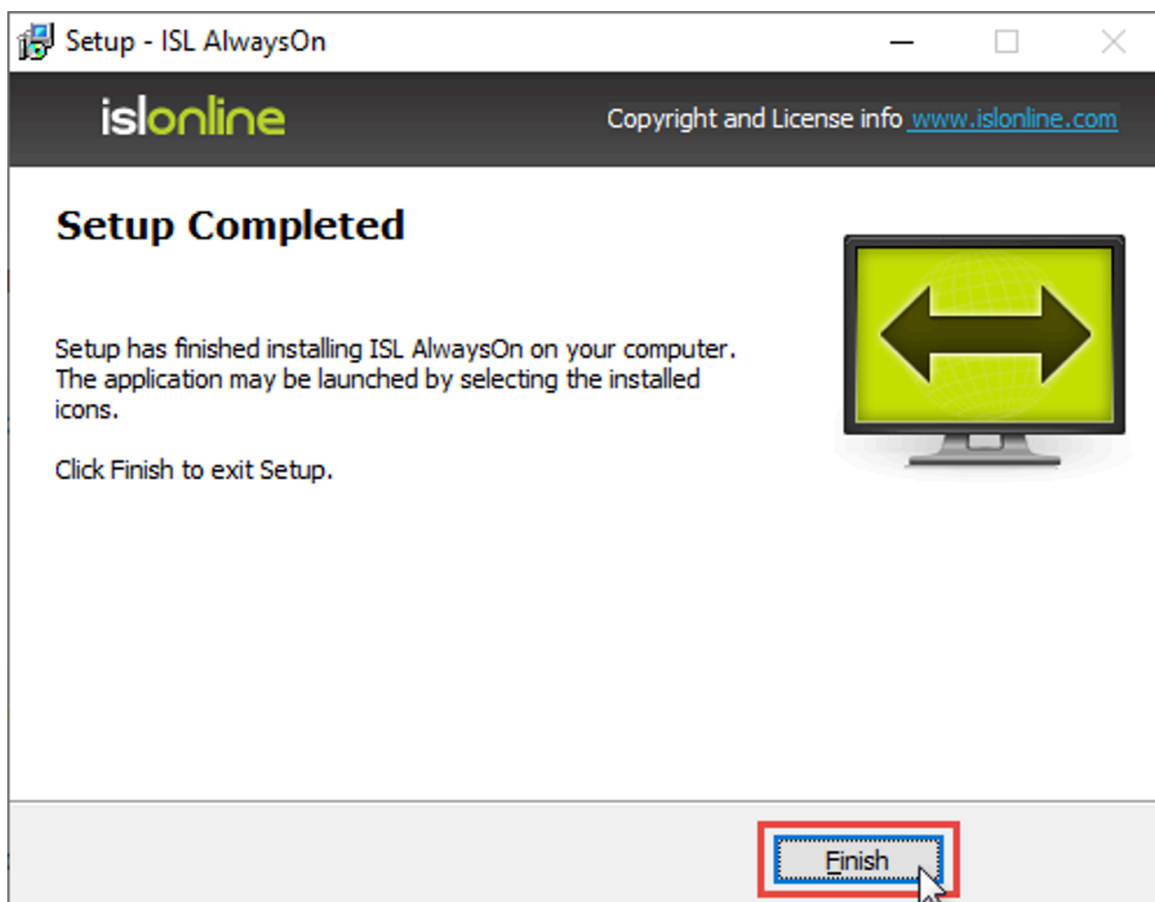


Figure 10. ISL Online RMM pop-up.

The reason for the attackers' sequential deployment of two distinct RMM tools remains unclear. It is possible UNK_SmudgedSerpent may have deployed RMM software as a throwaway option after the credential harvesting attempt didn't succeed, and the threat actor became suspicious of Proofpoint's investigation. However, neither hypothesis can be confirmed at the time of writing.

While the use of RMMs is a generic technique abusing common legitimate tools, it is rare to see them associated with state-sponsored actors and have been documented in use by only one Iranian actor, in [TA450 campaigns over the last several years](#).

Follow-on activity

Before the email exchange discussed ended on 26 June, Proofpoint identified an additional Gmail account on 23 June spoofing Dr. Maloney (with her name spelled correctly) – suzannemaloney68@gmail.com – targeting a US-based academic that appeared to be Israeli. In this lure, UNK_SmudgedSerpent asked for assistance investigating the IRGC.

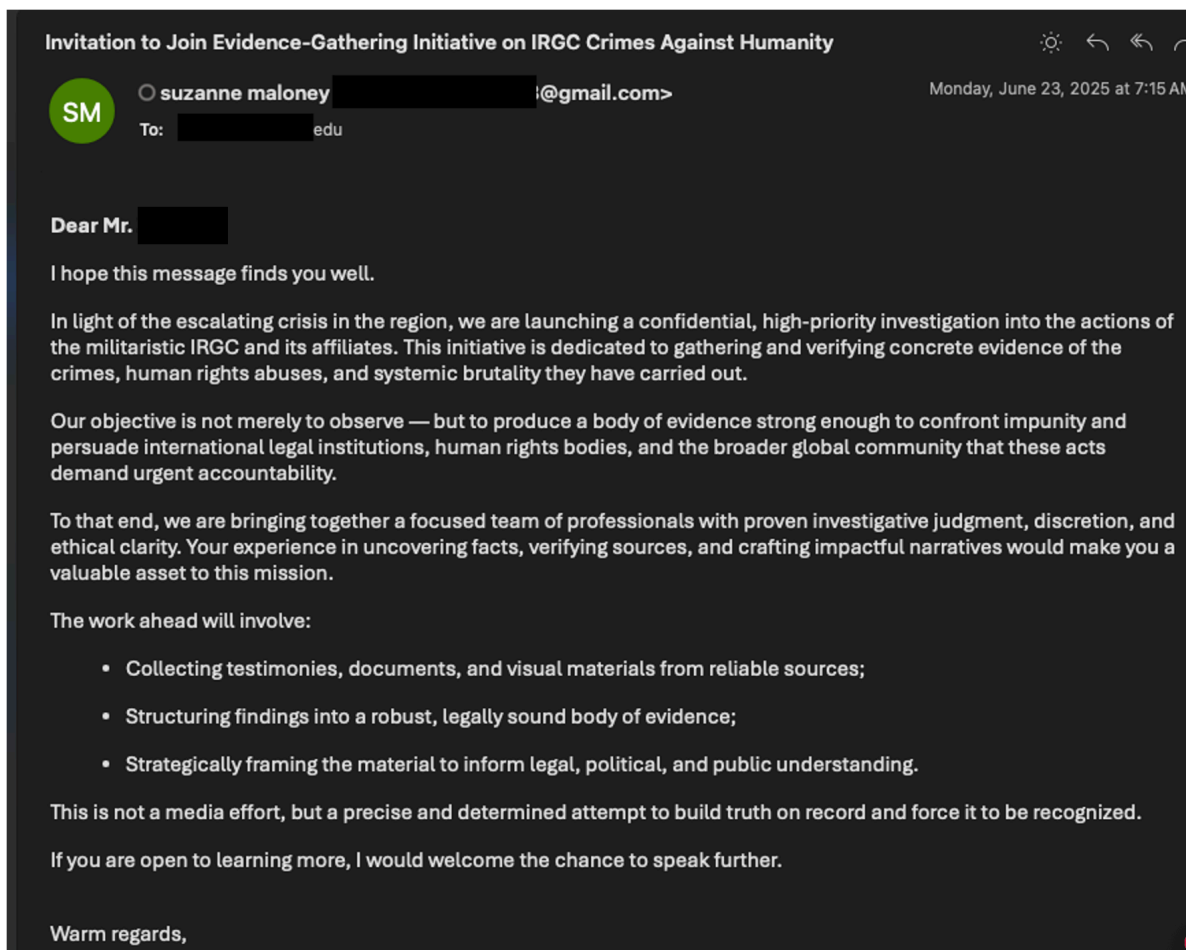


Figure 11. Second UNK_SmudgedSerpent phishing email.

A different persona, one spoofing Patrick Clawson – a Director at the Washington Institute – used the exact same content one week later to target the same academic using patrickclawson51@gmail[.]com.

In early August 2025, UNK_SmudgedSerpent surfaced again, this time soliciting information and collaboration on Iran's efforts in Latin America. The phishing email originated from another spoof of Patrick Clawson, this time using an Outlook email address: patrick.clawson51@outlook[.]com. However, the email in the signature did not match and included both potentially legitimate emails and patrickclawson51@gmail[.]com, which was the previously used spoofed email.

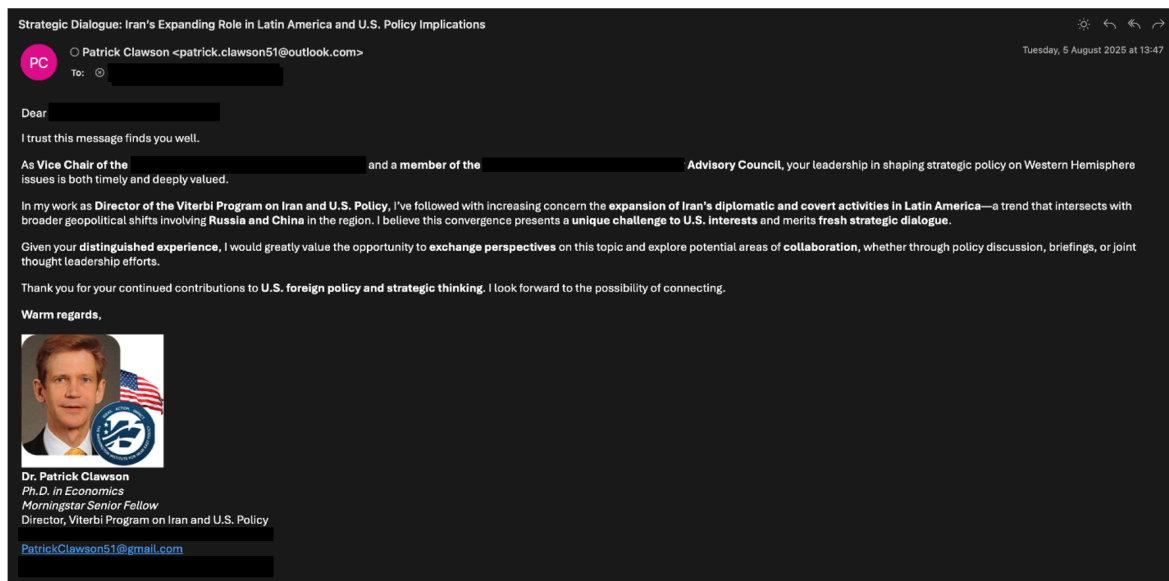


Figure 12. UNK_SmudgedSerpent Patrick Clawson Spoof #2.

The timeline below shows the campaigns and cadence of UNK_SmudgedSerpent activity, which appears to be topical and sporadic. After the initial approach that targeted over 20 individuals, Proofpoint data showed the actor focused only on solitary targets in further campaigns.

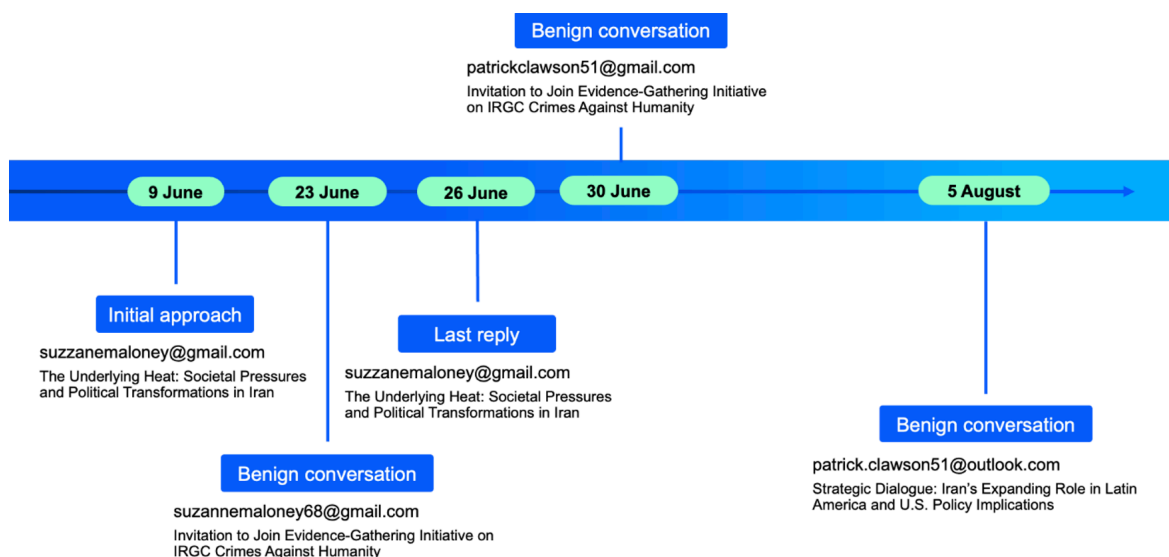


Figure 13. UNK_SmudgedSerpent phishing activity timeline.

Since early August, no further activity has been observed from this actor.

Infrastructure

Investigating suspected UNK_SmudgedSerpent infrastructure, such as healthcrescent[.]com, surfaced additional activity that further complicates UNK_SmudgedSerpent's relationship and overlaps with TA455.

healthcrescent[.]com shares server configuration similarities with a set of domains, including ebixcareers[.]com, that displays a fake Teams portal. The career-themed domain and Teams spoof are both reminiscent of previous TA455 activity.

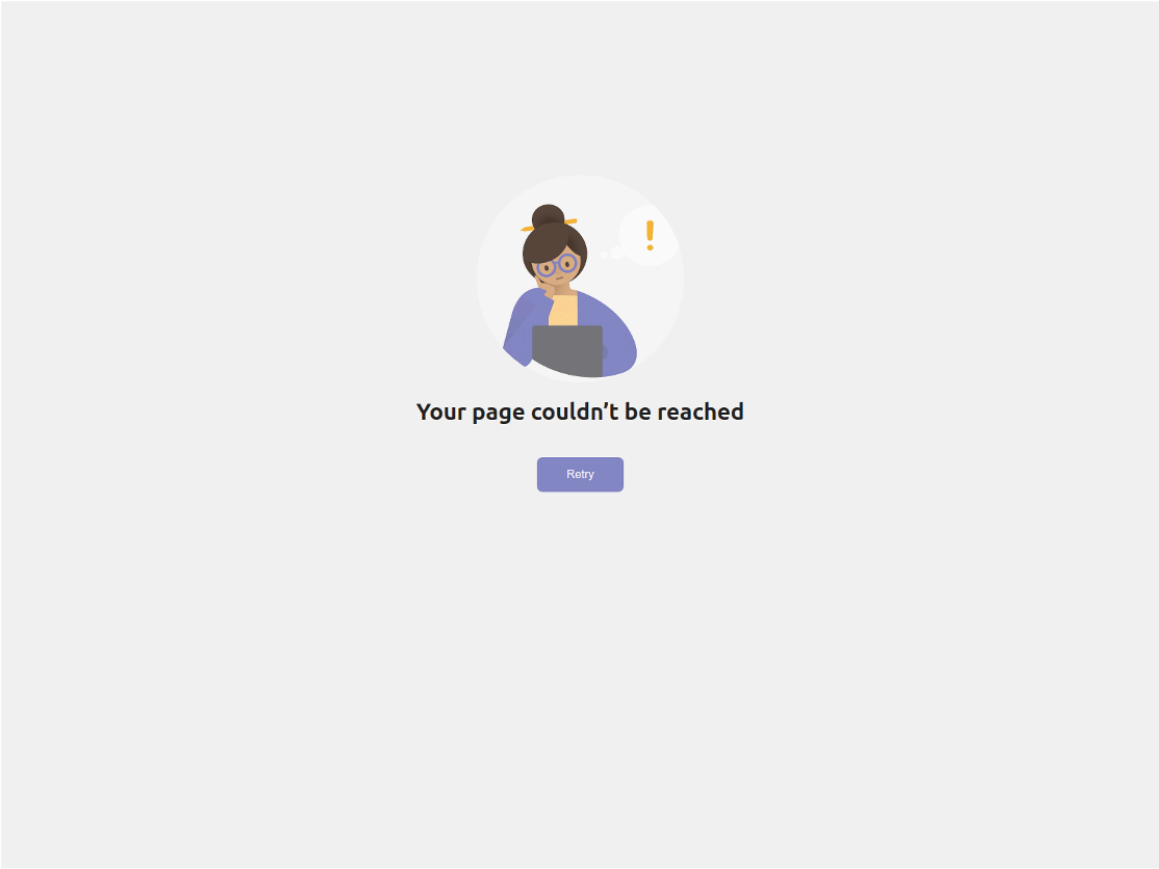


Figure 14. Fake Teams portal landing page.

Related URLs resembled previously seen activity from TA453, using [“meeting” themes](#).
hxxps://interview.ebixcareers[.]com/teams/join-online-room-homv-patm-elro/ fetched a payload from the following OnlyOffice URL:

hxxps://docspace-mpv1y2.onlyoffice[.]com/rooms/share?
key=ZXVSTehNKzM3NHBIeHg3R3M4cnBRcDFDUnk0b[...]0_Ijg4YzkzZTRhLWNmYzktNGJkMy1iYzYyLWY2NWY0OTczNT

ONLYOFFICE DocSpace

Boeing_Candidate46871

Sign in

Search

🔍

🏠

⬆️

🗃️

Name ↓	Modified ↓	Size	
 Interview time	09/17/2025 12:56 PM	4.88 MB	⋮
 Hiring Portal	09/17/2025 12:55 PM	3.7 MB	⋮
 Vibhav-Patil-Application form	09/17/2025 12:54 PM	128.55 KB	⋮
 Boeing_Germany_Recruitment_Process	09/17/2025 12:54 PM	139.05 KB	⋮
 Boeing HR Staff	09/17/2025 12:54 PM	168.45 KB	⋮

Figure 15. Files Hosted on OnlyOffice URL.

Files hosted on this page in mid-September included benign recruitment-related PDFs for Boeing, a traditional aspect of TA455’s operations involving both aerospace and career-themed interests.

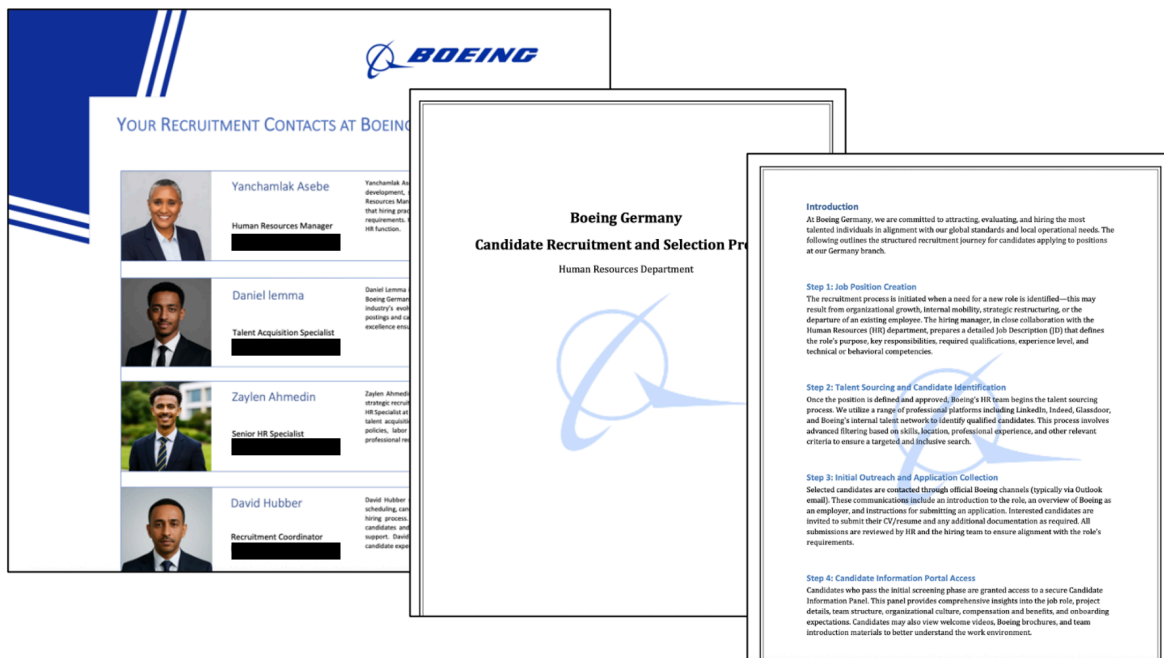


Figure 16. Benign PDFs.

Hiring Portal.zip contained two DLLs and an executable; the legitimate EXE sideloads userenv.dll and through another legitimate EXE, sideloads xmlite.exe. userenv.dll is a TA455 custom backdoor termed [MiniJunk](#) in public reporting, a version of previously reported malware called [MiniBike](#). While the infrastructure likely aligns with UNK_SmudgedSerpent, it remains unclear why it is simultaneously hosting TA455 custom malware.

The final file hosted on the OnlyOffice URL was Interview time.msi, a loader responsible for installing the RMM tool PDQConnect, seen deployed in both UNK_SmudgedSerpent and TA450 activity, though not previously seen associated with TA455.

The exploration of infrastructure and operations connected to UNK_SmudgedSerpent activity further blurs the lines of attribution and the nature of the relationship to TA455.

Attribution

Proofpoint Threat Research is currently tracking this activity separately as a new threat actor – UNK_SmudgedSerpent – and clustered distinctly from TA453, TA455, and TA450. While there are several overlaps with established threat actors in various stages of the infection chain, which are shown below, they remain tenuous in some cases without high confidence links.

TTP	UNK_SmudgedSerpent	TA453	TA455	TA450
Sender emails	Freemail (Outlook, Gmail)	Freemail (Outlook, Gmail, ProtonMail, Yahoo)	Attacker-owned domains	Compromised corporate accounts
Initial approach	Benign conversation	Benign conversation	Malicious recruitment applications	Malicious event invitations

Targeting	Policy experts, thinktanks	Policy experts, thinktanks	Aerospace and defense, transportation/logistics, technology	Government, telecommunications, transportation
Delivery	OnlyOffice spoof, Teams spoof	Teams spoof, Scalingo, OneDrive	OnlyOffice	Mega.nz, FliQR
Objective	Credential theft, malware delivery	Credential theft, malware delivery	Malware delivery	Malware delivery
Domain themes	Health and recruitment, organization spoofs	Organization, meeting, Google, Microsoft, and technology spoofs	Health, aerospace, and recruitment	Technology, other
Infrastructure	Cloudflare, Namecheap	Hetzner, OVH, RouterHosting, Namecheap	Cloudflare, Namecheap	NordVPN, Cloudflare Namecheap
Malware	RMM (PDQConnect)	PowerShell backdoors (occasional)	Custom backdoors (MiniJunk, MINIBIKE, MINIBUS)	RMMs, custom PowerShell and .NET backdoors (Phoenix)

Given the dynamic nature of the Iranian ecosystem and its heavy use of contracting companies, there are often instances where groups, activity, malware, and infrastructure intersect. We hypothesize there are several possibilities for the group's convergence of TTPs with varying degrees of likelihood, which include:

- Centralized procurement: a shared resource that registers and distributes infrastructure or a shared malware developer.
- Personnel mobility: one group dissolves, and another absorbs team members, or groups merge based on new requirements or shared remits.
- Interpersonal relationships: individual members of the same team have TTP preferences, and operators share their preferred techniques with one another.
- Parallel contractor deployment: the parent/sponsoring agency tasks more than one contracting company to a particular threat group or campaign.
- Institutional collaboration: cross-agency exchanges between IRGC and MOIS at an organizational level due to the groups' affiliations with differing agencies.

Conclusion

UNK_SmudgedSerpent's first observed campaign was in June 2025, after which the group was seen a few times targeting policy experts in the US using lures about internal political developments in Iran. The subsequent investigation revealed

multiple overlaps in TTPs with TA453, TA450, and TA455. However, the abundance of links prevents high confidence attribution to any one of these groups.

While UNK_SmudgedSerpent has not been observed in email campaigns since August 2025, related activity likely remains ongoing. The appearance of a new actor with borrowed techniques suggests there may be personnel mobility or exchange between teams, but with a consistent remit; however, there is no confirmed attribution for UNK_SmudgedSerpent at the time of writing. The TTPs and infrastructure are an extension of previously observed behavior from Iranian threat groups, and the targeting of Iran foreign policy experts continues to reflect the Iranian government's intelligence collection priorities.

ET rules

[2054935 - ET INFO PDQ Remote Management HTTP Header Observed \(x-pdq-key-ids\)](#)

[2054936 - ET INFO PDQ Remote Management User-Agent Observed \(PDQ rover\)](#)

[2054937 - ET INFO PDQ Remote Management Agent HTTP Activity](#)

[2054938 - ET INFO PDQ Remote Management Agent Checkin](#)

[2062767 - ET INFO Observed DNS Query to Online Document Sharing Service \(onlyoffice .com\)](#)

[2062768 - ET INFO Observed Online Document Sharing Service Domain \(onlyoffice .com in TLS SNI\)](#)

[2065399 - ET PHISHING Observed UNK_SmudgedSerpent Style URI](#)

[2065427 - ET MALWARE Observed DNS Query to TA455 Domain \(msnapp .help\)](#)

[2065434 - ET MALWARE Observed DNS Query to TA455 Domain \(accountroyal .com\)](#)

[2065439 - ET MALWARE Observed DNS Query to TA455 Domain \(palaerospace .careers\)](#)

[2065444 - ET MALWARE Observed DNS Query to TA455 Domain \(msnapp .live\)](#)

[2065448 - ET MALWARE Observed DNS Query to TA455 Domain \(healthiestmama .com\)](#)

[2065449 - ET MALWARE Observed DNS Query to TA455 Domain \(mojavemassageandwellness .com\)](#)

[2065450 - ET MALWARE Observed DNS Query to TA455 Domain \(alwayslivehealthy .com\)](#)

[2065451 - ET MALWARE Observed DNS Query to TA455 Domain \(rhealthylivingsolutions .com\)](#)

[2065452 - ET MALWARE Observed DNS Query to TA455 Domain \(rheinmetallcareer .org\)](#)

[2065453 - ET MALWARE Observed DNS Query to TA455 Domain \(chakracleansetherapy .com\)](#)

[2065454 - ET MALWARE Observed DNS Query to TA455 Domain \(clearmindhealthandwellness .com\)](#)

[2065455 - ET MALWARE Observed DNS Query to TA455 Domain \(joinboeing .com\)](#)

[2065456 - ET MALWARE Observed DNS Query to TA455 Domain \(healthcarefluent .com\)](#)

[2065459 - ET MALWARE Observed DNS Query to TA455 Domain \(rheinmetallcareer .com\)](#)

[2065464 - ET MALWARE Observed DNS Query to TA455 Domain \(zytonhealth .com\)](#)

[2065470 - ET MALWARE Observed DNS Query to TA455 Domain \(sulumorbusinessservices .com\)](#)

[2065475 - ET MALWARE Observed DNS Query to TA455 Domain \(airbushiring .com\)](#)

[2065481 - ET MALWARE Observed DNS Query to TA455 Domain \(healthinfusiontherapy .com\)](#)

[2065484 - ET MALWARE Observed DNS Query to TA455 Domain \(bodywellnessbycynthia .com\)](#)

[2065486 - ET MALWARE Observed DNS Query to TA455 Domain \(careers-portal .org\)](#)

[2065487 - ET MALWARE Observed TA455 Domain \(msnapp .help in TLS SNI\)](#)

[2065488 - ET MALWARE Observed TA455 Domain \(accountroyal .com in TLS SNI\)](#)

[2065489 - ET MALWARE Observed TA455 Domain \(palaerospace .careers in TLS SNI\)](#)

[2065490 - ET MALWARE Observed TA455 Domain \(msnapp .live in TLS SNI\)](#)

[2065491 - ET MALWARE Observed TA455 Domain \(healthiestmama .com in TLS SNI\)](#)

[2065493 - ET MALWARE Observed TA455 Domain \(mojavemassageandwellness .com in TLS SNI\)](#)

[2065495 - ET MALWARE Observed TA455 Domain \(alwayslivehealthy .com in TLS SNI\)](#)

[2065498 - ET MALWARE Observed TA455 Domain \(rhealthylivingsolutions .com in TLS SNI\)](#)

[2065501 - ET MALWARE Observed TA455 Domain \(rheinmetallcareer .org in TLS SNI\)](#)

[2065502 - ET MALWARE Observed TA455 Domain \(chakracleansetherapy .com in TLS SNI\)](#)

[2065503 - ET MALWARE Observed TA455 Domain \(clearmindhealthandwellness .com in TLS SNI\)](#)

[2065504 - ET MALWARE Observed TA455 Domain \(joinboeing .com in TLS SNI\)](#)

[2065505 - ET MALWARE Observed TA455 Domain \(healthcarefluent .com in TLS SNI\)](#)

[2065506 - ET MALWARE Observed TA455 Domain \(rheinmetallcareer .com in TLS SNI\)](#)

[2065507 - ET MALWARE Observed TA455 Domain \(zytonhealth .com in TLS SNI\)](#)

[2065508 - ET MALWARE Observed TA455 Domain \(sulumorbusinessservices .com in TLS SNI\)](#)

[2065509 - ET MALWARE Observed TA455 Domain \(airbushiring .com in TLS SNI\)](#)

[2065510 - ET MALWARE Observed TA455 Domain \(healthinfusiontherapy .com in TLS SNI\)](#)

[2065511 - ET MALWARE Observed TA455 Domain \(bodywellnessbycynthia .com in TLS SNI\)](#)

[2065512 - ET MALWARE Observed TA455 Domain \(careers-portal .org in TLS SNI\)](#)

[2065513 - ET PHISHING Observed DNS Query to UNK SmudgedSerpent Domain \(mosaichealthsolutions .com\)](#)

[2065514 - ET PHISHING Observed DNS Query to UNK SmudgedSerpent Domain \(ebixcareers .com\)](#)

[2065515 - ET PHISHING Observed DNS Query to UNK SmudgedSerpent Domain \(healthcrescent .com\)](#)

[2065516 - ET PHISHING Observed DNS Query to UNK SmudgedSerpent Domain \(thebesthomehealth .com\)](#)

[2065517 - ET PHISHING Observed UNK SmudgedSerpent Domain \(mosaichealthsolutions .com in TLS SNI\)](#)

[2065518 - ET PHISHING Observed UNK SmudgedSerpent Domain \(ebixcareers .com in TLS SNI\)](#)

[2065519 - ET PHISHING Observed UNK SmudgedSerpent Domain \(healthcrescent .com in TLS SNI\)](#)

[2065520 - ET PHISHING Observed UNK SmudgedSerpent Domain \(thebesthomehealth .com in TLS SNI\)](#)

Indicators

UNK_SmudgedSerpent			
Indicator	Type	Description	First Seen
suzzanemaloney@gmail[.]com	Email address	Phishing	June 2025
suzannemaloney68@gmail[.]com	Email address	Phishing	June 2025
patrickclawson51@gmail[.]com	Email address	Phishing	June 2025
patrick.clawson51@outlook[.]com	Email address	Phishing	August 2025
hxtps://suzzanemaloney2506090953.onlyoffice[.]com/s.-k6vjflsdagdsfgh	URL	Delivery	June 2025
thebesthomehealth[.]com	Domain	Delivery	April 2025
mosaichealthsolutions[.]com	Domain	Delivery	April 2025
healthcrescent[.]com	Domain	Delivery	May 2025
ebixcareers[.]com	Domain	Delivery	July 2025
6eb7df21d6f1e3546c252a112504eefbb19205167db89038f2861118bbc8871c	SHA256	Benign PDF	September 2025

0bdb64fc1d5533f7b3ffaf821e89f286ad2d7400a914f21abdcbb7bb8a39e63	SHA256	Benign PDF	September 2025
cac018dcccdf6ce4bef19ab71e3e737724aed104bc824332a5213c878b065ff50	SHA256	EXE	September 2025
7b5fb8202bff90398ab007579713f66430778249e43b46f35df6c3ded628f129	SHA256	DLL	September 2025
129a40e38ef075c7d33d8517b268eb023093c765a32e406b58f39fab6cc6a040	SHA256	DLL	September 2025
85858880ee7659cc1152b6a126bc20b9b4fb1b46dddea5af2d65d48d58cd0589	SHA256	MSI	September 2025
0fcdaa2f4db94e0589617830d3d80430627815ef0e4b0c7b7ff5c1ebb82a4136	SHA256	Benign PDF	September 2025
1e9c31ce0eba2100d416f5bc3b97dfe2da0d3d9aee96de59ec774365fe3fe89	SHA256	ZIP	September 2025

TA455

Indicator	Type	Description	First Seen
emiratesgroup-careers[.]com	Domain	Related infrastructure	May 2024
flydubai-careers[.]com	Domain	Related infrastructure	May 2024
airbusgroup-careers[.]com	Domain	Related infrastructure	May 2024
gocareers[.]org	Domain	Related infrastructure Related infrastructure	June 2024
rheinmetallcareers[.]com	Domain	Related infrastructure	June 2024
careers2find[.]com	Domain	Related infrastructure	June 2024

opportunities2get[.]com	Domain	Related infrastructure	June 2024
emiratescareers[.]org	Domain	Related infrastructure	July 2024
droneflywell[.]com	Domain	Related infrastructure	July 2024
usa-careers[.]com	Domain	Related infrastructure	August 2024
careers-hub[.]org	Domain	Related infrastructure	September 2024
global-careers[.]com	Domain	Related infrastructure	September 2024
ehealthpsuluth[.]com	Domain	Related infrastructure	September 2024
worldcareers[.]org	Domain	Related infrastructure	September 2024
uavnodes[.]com	Domain	Related infrastructure	September 2024
careersworld[.]org	Domain	Related infrastructure	September 2024
thecareershub[.]org	Domain	Related infrastructure	September 2024
germanywork[.]org	Domain	Related infrastructure	September 2024
easymarketing101[.]com	Domain	Related infrastructure	September 2024
collaboromarketing[.]com	Domain	Related infrastructure	September 2024

virgomarketingsolutions[.]com	Domain	Related infrastructure	September 2024
marketinglw[.]com	Domain	Related infrastructure	September 2024
anteromarketing[.]com	Domain	Related infrastructure	September 2024
airbusaerodefence[.]nl	Domain	Related infrastructure	November 2024
dronetechasia[.]org	Domain	Related infrastructure	November 2024
asiandefenses[.]com	Domain	Related infrastructure	November 2024
msnclouds[.]com	Domain	Related infrastructure	November 2024
kibanacore[.]com	Domain	Related infrastructure	November 2024
boeingspace[.]com	Domain	Related infrastructure	November 2024
airbusaerodefence[.]com	Domain	Related infrastructure	December 2024
jadehealthcenter[.]com	Domain	Related infrastructure	December 2024
clearmindhealthandwellness[.]com	Domain	Related infrastructure	January 2025
accountroyal[.]com	Domain	Related infrastructure	January 2025
msnapp[.]help	Domain	Related infrastructure	January 2025

msnapp[.]live	Domain	Related infrastructure	January 2025
zytonhealth[.]com	Domain	Related infrastructure	February 2025
alwayslivehealthy[.]com	Domain	Related infrastructure	February 2025
healthiestmama[.]com	Domain	Related infrastructure	February 2025
healthcarefluent[.]com	Domain	Related infrastructure	February 2025
healthinfusiontherapy[.]com	Domain	Related infrastructure	February 2025
mojavemassageandwellness[.]com	Domain	Related infrastructure	February 2025
chakracleansetherapy[.]com	Domain	Related infrastructure	February 2025
bodywellnessbycynthia[.]com	Domain	Related infrastructure	February 2025
palaerospace[.]careers	Domain	Related infrastructure	February 2025
rhealthylivingsolutions[.]com	Domain	Related infrastructure	April 2025
sulumorbusinessservices[.]com	Domain	Related infrastructure	April 2025
airbushiring[.]com	Domain	Related infrastructure	April 2025
joinboeing[.]com	Domain	Related infrastructure	May 2025
rheinmetallcareer[.]org	Domain	Related infrastructure	May 2025
rheinmetallcareer[.]onlyoffice[.]com	Domain	Related infrastructure	May 2025
rheinmetallcareer[.]com	Domain	Related infrastructure	May 2025

careers-portal[.]org	Domain	Related infrastructure	May 2025
boeinginformation[.]onlyoffice[.]com	Domain	Related infrastructure	May 2025
airbus-careers[.]onlyoffice[.]com	Domain	Related infrastructure	June 2025
airbus-survay[.]onlyoffice[.]com	Domain	Related infrastructure	July 2025
malebachhew2506090936.onlyoffice[.]com	Domain	Related infrastructure	July 2025
randcorp.onlyoffice[.]com	Domain	Related infrastructure	July 2025

Source: <https://www.proofpoint.com/us/blog/threat-insight/crossed-wires-case-study-iranian-espionage-and-attribution>