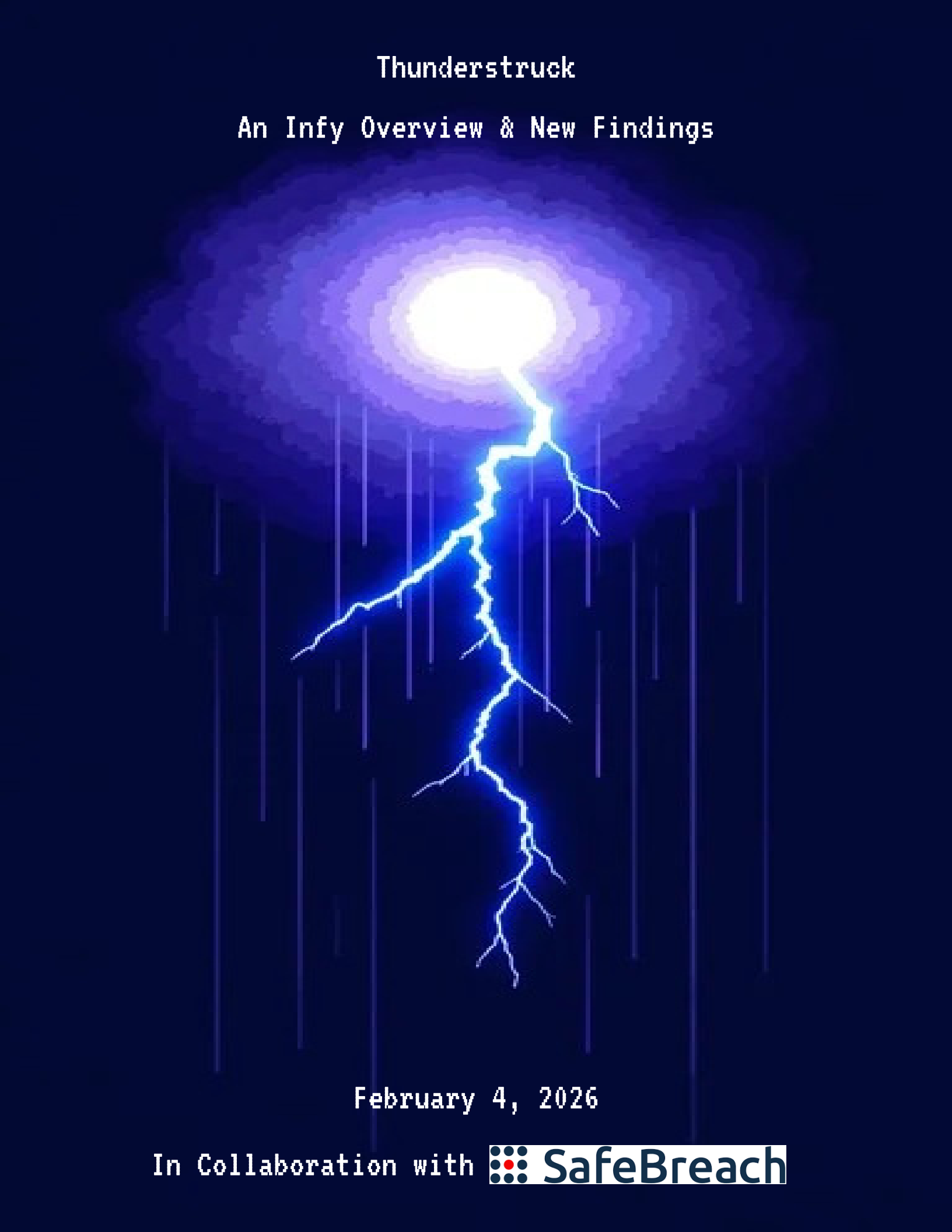
Thunderstruck

An Infy Overview & New Findings



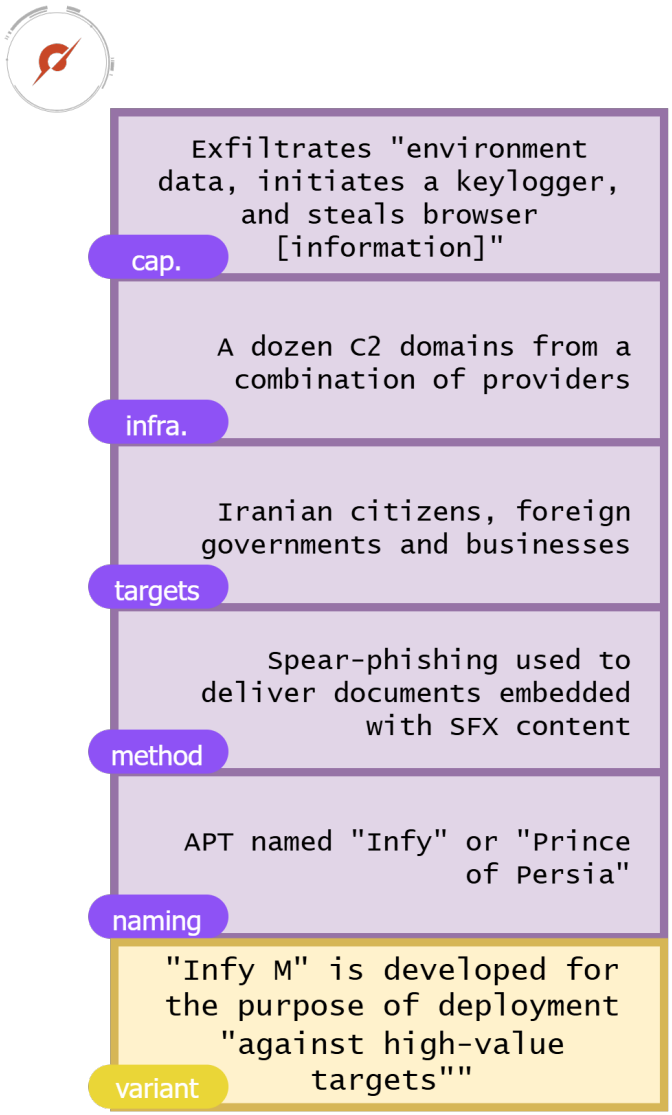
February 4, 2026

In Collaboration with SafeBreach

Threat hunters at SafeBreach Inc. recently identified increased activity of the Infy Advanced Persistent Threat (APT) group. After a report published by SafeBreach in December of 2025, Monitoring Circuit investigated the threat group's activity on Telegram; API credentials described in the report as used to exfiltrate data and communicate with the malware's C2 server(s) were leveraged to extract new findings. This report includes a review of Infy's activity to date, as well as an update on the group's new abilities.

>___ Timeline

The Infy APT is believed to have begun operating as early as 2007 per research conducted by Palo Alto's cyber threat intelligence division ("Unit 42"). In 2016, Unit 42 released one of the first major reports on Infy's then decade-long campaign, noting its preference for targeting Iranian citizens and relying on multi-layer Self-Extracting Executable Archive (SFX) content embedded in Microsoft Word and PowerPoint documents to infect its victims.



"We refer to the malware as "Infy" because the actor used this string in multiple locations, including filenames ("infy74f1.exe" - Infy version 7.4 F1), C2 strings ("subject=INFY M 7.8"), and C2 folder names."[3]

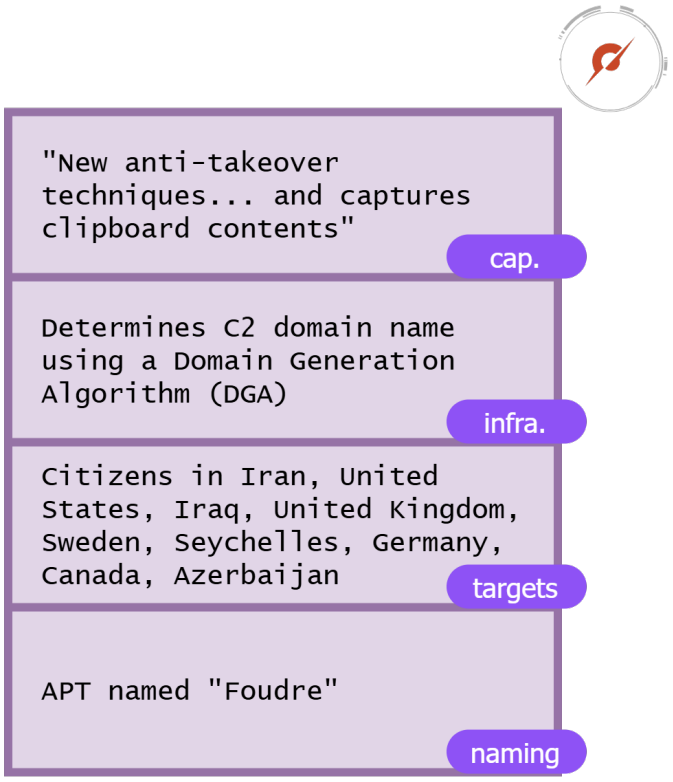
Infy was soon identified as a targeted espionage operation based out of Iran, aimed at Iranian citizens and an international assortment of both governments and businesses – Unit 42's appraisal remains accurate at the time of this report. A variant of Infy dubbed "Infy M" was developed at the same time as the original strain "for the purpose of deployment against "high-value targets"."[3]

Soon after Unit 42's initial report, Qi-Anxin's Threat Intelligence Center investigated similar patterns of threat actor activity and dubbed the APT "Operation Mermaid."[4]

Text in the Rain

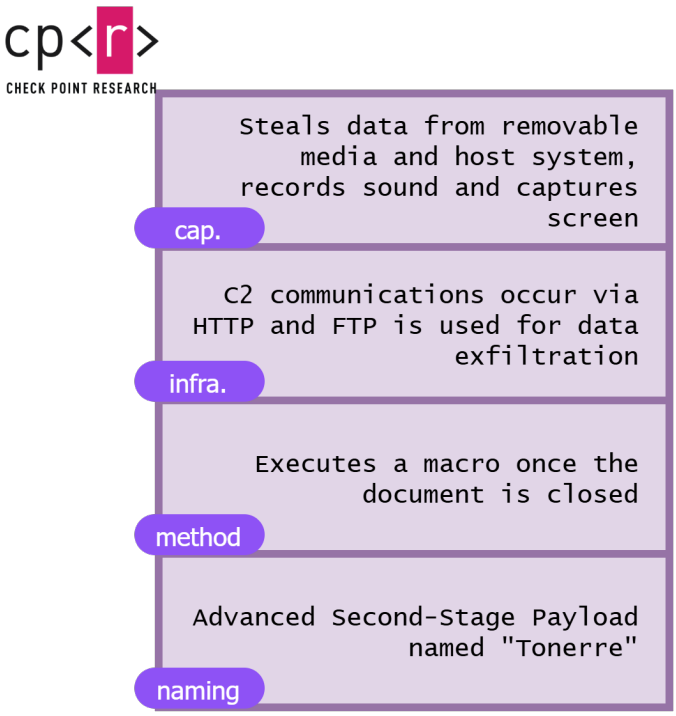
A common attribute across every Infy iteration has been an inclusion of "embedded strings from news articles"[10], frequently from around when the executable was created. Examples range from a 2020 BBC update on a Turkish maritime research vessel embroiled in disputed Mediterranean energy rights claims, the Süddeutsche Zeitung's detailing of a German right-wing extremist and neo-Nazi terrorist's trial, and a French publication on the US president's defense of hydroxychloroquine's effectiveness during the Covid-19 pandemic (2020). As of this report's publication, no definitive answer has been given as to why these excerpts are embedded in the malware.

Unit 42 released a follow-up to their research in 2017. Infy's newer variant was dubbed "Foudre" ("lightning", in French) after the string appeared repeatedly in its code. Foudre remained an information stealer, now "[incorporating] new anti-takeover techniques in an attempt to avoid their C2 domains being sinkholed,"[2] Foudre used a Domain Generation Algorithm (DGA) to determine its C2 domain name and an "RSA signature verifying algorithm to check the veracity of [the] C2 domain."[2] This was the first instance of Infy dramatically advancing its capabilities in relative secrecy, a habit that would become expected of the group.



"In July 2016, at Blackhat U.S., Claudio Guarnieri [and] Collin Anderson presented evidence that a subset of the C2 domains redirecting to our sinkhole were blocked by DNS tampering and HTTP filtering by the Telecommunication Company of Iran (AS12880), preventing Iran-domestic access to our sinkhole."[2]

After lying dormant for several years, an advanced variant of Foudre was identified by cyber threat intelligence researchers at Check Point Research. The updated malware ran a macro once the victim closed a document delivered primarily via phishing, as opposed to manipulating the victim into clicking a link. C2 communications occurred via HTTP and FTP was used for data exfiltration. This new variant of Foudre was dubbed Tonnerre ("thunder", in French)



"Tonnerre is used to expand the functionality of Foudre; possibly its functionality was put into a separate component to make sure it is deployed only when needed, and meets fewer prying eyes."[9]

Tonnere used its C2 to store metadata about the victim, steal files that match a set predefined extensions, download updates and retrieve information on an additional C2 (which in turn is used to store the stolen data and provide a list of commands) – per Check Point, "communication to the first C2 uses HTTP, whereas the second C2 communicates using FTP. The FTP password is hardcoded in the malware, but the username is the name of the victim's computer, which was previously sent to the HTTP C2."[9]

Shortly after, Bitdefender reported that Tonnerre was likely a variant of Infy M, though with a slew of new C2 communication abilities. Coupled with new Top Level Domains (TLDs) for Tonnerre's C2 infrastructure, Infy's resurgence lasted only a short while before once more receding into the background hum of the electron and the switch.

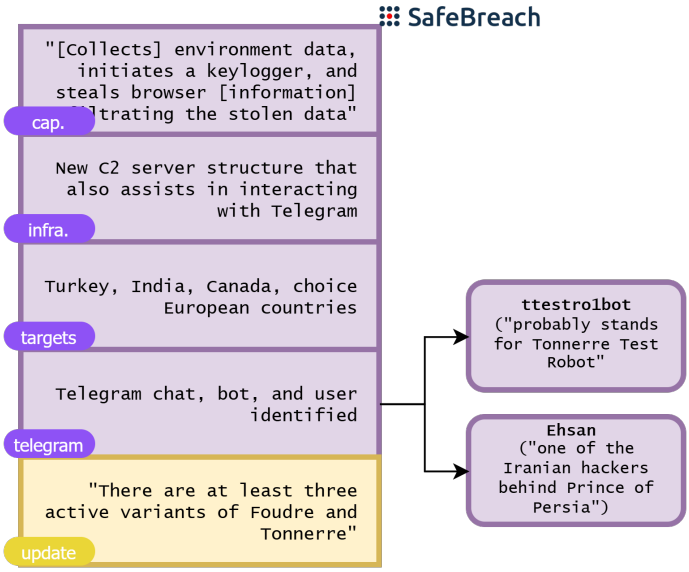
Victim Demographic

Since its inception, the **Infy campaign has predominantly targeted Iranian citizens**, though a secondary focus is given to targets in the United States and Iraq. With respect to its high-value targets, Infy has historically chosen them and the corresponding packaging of its malware with precision and care. Chiefly an espionage campaign, Infy's choice of targets speaks to the intelligence priorities of those who direct it.

A 2017 Foudre variant analyzed by SafeBreach likely used "on high valued victims" [10] was masquerading as Amaq News Finder, a fake digital offshoot of the Amaq News Agency. In 2019, Amaq News Agency was designated a "part of [ISIS]'s propaganda apparatus" [6] by the Department of Homeland Security. Iran has held strained relations with ISIS, and this variant of Foudre was likely intended to compromise targets who could gfrant Iranian intelligence services access to potentially actionable information on ISIS activity.

A 2018 Foudre variant analyzed by Intezer levied a video depicting "protesters in Iran who [were] protesting the mandatory use of the hijab for women" [7] as a means of distracting the victim while the malware executes, suggesting a particular subset of dissidents were targeted.

After a four year period of decreased activity, cyber threat intelligence researchers at SafeBreach Inc. published a report detailing the apparent expansion and advancements that the Infy campaign had quietly undergone in its absence.



"The scale of Prince of Persia's activity is more significant than we originally anticipated. Our research identified multiple campaigns that used a large number of malware variants and C2 servers."[10]

The new Tonnerre variant is redirected by its C2 server to a Telegram group that is then used to send commands and exfiltrate stolen data. SafeBreach was able to identify a Telegram user, `Ehsan` ("one of the Iranian hackers behind Prince of Persia"[10] who is "responsible for commanding the victim's machines over Telegram"[10]) as well as the Telegram bot `ttestro1bot` ("probably stands for Tonnerre Test Robot"[10]) that is used to exfiltrate data – both the user and bot remain active as of this report's publication.

Game Over

Following Unit 42's initial report, a coordinated attempt was conducteed to sinkhole then-active Infy domains to learn more about the campaign. They were able to determine that:

- One-third of victims (at that time) are identified to be Iranian citizens.
- Considerably more care and effort is put towards maintaining persistence when Infy M is deployed.

Try Again

After SafeBreach's newest findings were released, `Ehsan`'s Telegram username was changed from `ehsan8999100` to `Ehsan66442`. Infy operators have been known to remove or alter known strings such as "foudre" or "tonnerre" in the malware's code to impede signature-based detection models.

Updated Indicators of Compromise (IOC) can be found in most of the articles included on the references page.

Most troubling was the apparent action taken on behalf of the Iranian state to impede mitigation efforts. Per Unit 42: "Regarding the actions by the Telecommunication Company of Iran to prevent the C2s from resolving to our sinkhole, Guarnieri & Anderson note "The filtering policy indicates that Iranian authorities had specifically intervened to block access to the command and control domains of a state aligned intrusion campaign at a country level"." [2]

>___ New Findings

Safebreach's report on Infy's resurgence contained information detailing the Telegram chat ID and bot token (shown below, respectively) used by the threat actor for C2 communication and data exfiltration:

874675833
7900216285:AAEVjLjt4csUKGanerJuuiDhdsmlUv0yooM

In collaboration with SafeBreach, we were able to leverage a Telegram chat message enumeration tool to retrieve messages from chats whose message IDs were in the range of 0-1000. This range proved most fruitful for finding messages, though higher ranges may hold more data – the IDs of bot-sent Telegram messages are determined incrementally, relative to how many messages the bot has sent thus far. As such, the message ID may increase past what was previously known if the bot has been interacted with by Infy or external users to send or enumerate messages.

Messages were exfiltrated from the following chat, according to data returned by the /getUpdates query on the Telegram bot's token:

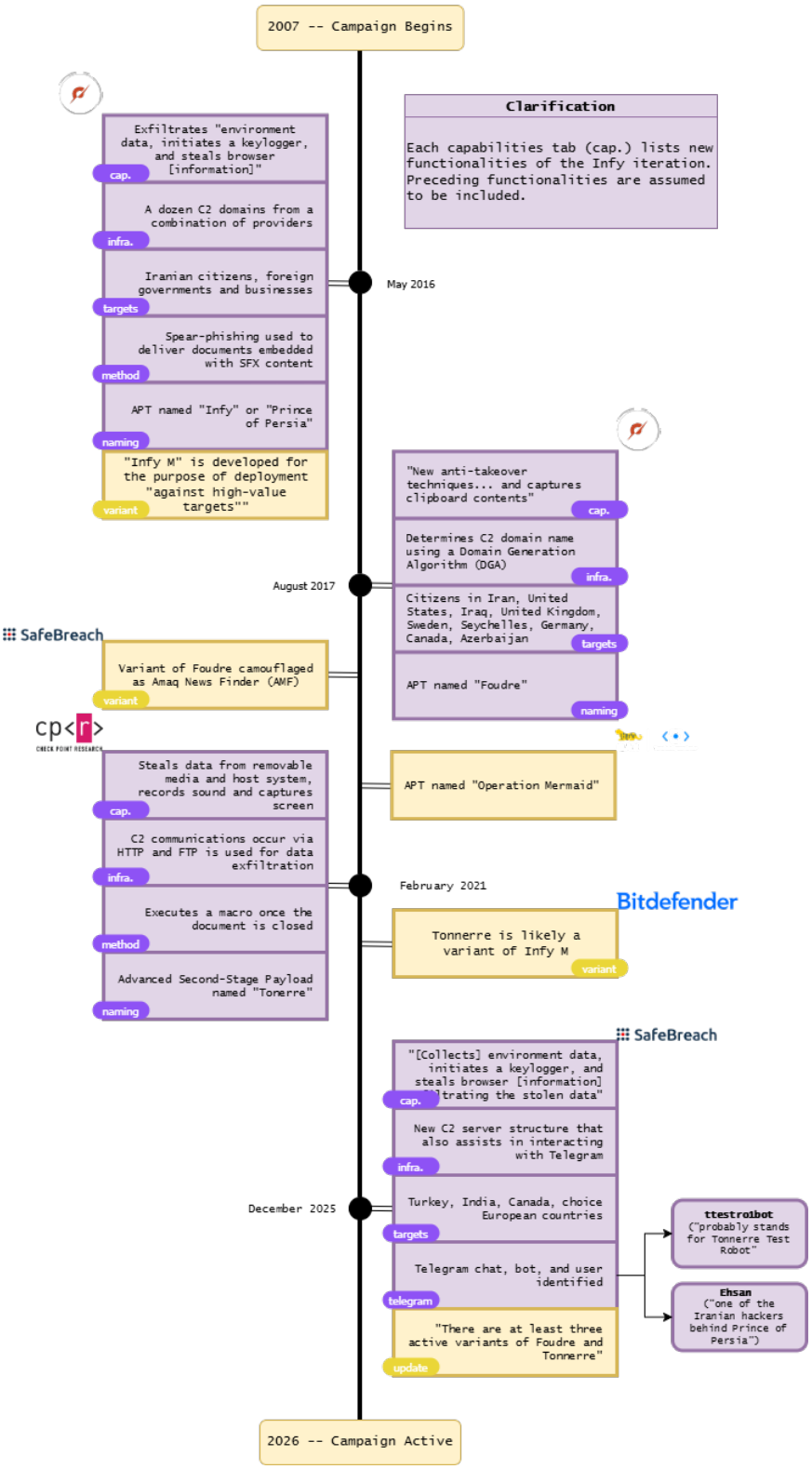

```
{
  "ok": true,
  "result": {
    "id": 874675833,
    "first_name": "سرافراز",
    "username": "Ehsan66442",
    "type": "private",
    "can_send_gift": true,
    "active_usernames": [
      "Ehsan66442"
    ],
    "has_private_forwards": true,
    "accepted_gift_types": {
      "unlimited_gifts": true,
      "limited_gifts": true,
      "unique_gifts": true,
      "premium_subscription": true,
      "gifts_from_channels": true
    },
    "max_reaction_count": 11,
    "accent_color_id": 3
  }
}
```


The chat under the username "Ehsan66442" held the highest number of files, and may therefore be one of the primary avenues through which the current Infy operators sought to ferry data from compromised systems – enumeration of all chats gleaned substantial insight into the current state of the campaign:

- Foudre-exfiltrated files
- Tonnerre-exfiltrated files (from two different machines)
- An Foudre v50 HTTP POST request to exfiltrate files from a third machine
- The URL of an inactive executable stored in a known C2 server
- Text messages beginning in March 2025

Note: The nature of Telegram's bot API allows any user with a bot's token and appropriate chat ID to manipulate it – any new users and/or groups that have interacted with ttestro1bot may very well be researchers, hobbyists, or other benign third-party entities. While Ehsan66442 has been confirmed to be an operator of the Infy campaign, we strongly caution against associating newly sighted users of the bot to Infy without having concrete evidence of malintent.

>___ Timeline Graphic



A downloadable and regularly updated copy of this graphic is linked in the section header above

References

[1] Unit 42. “Prince of Persia – Game Over”. In: (June 28, 2016). URL: https://unit42.paloaltonetworks.com/unit42-prince-of-persia-game-over/.

[2] Unit 42. “Prince of Persia – Ride the Lightning: Infy returns as “Foudre””. In: (Aug. 1, 2017). URL: https://unit42.paloaltonetworks.com/unit42-prince-persia-ride-lightning-infy-returns-foudre/.

[3] Unit 42. “Prince of Persia: Infy Malware Active In Decade of Targeted Attacks”. In: (May 2, 2016). URL: https://unit42.paloaltonetworks.com/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/.

[4] Qi-Anxin. “OPERATION MERMAID —6-Year Targeted Attacks Against Government”. In: (Mar. 24, 2020). URL: https://en.qianxin.com/threat/reportdetail?report_id=207.

[5] Bitdefender. “Iranian APT Makes a Comeback with “Thunder and Lightning” Backdoor and Espionage Combo”. In: (Feb. 18, 2021). URL: https://download.bitdefender.com/resources/files/News/CaseStudies/study/393/Bitdefender-Whitepaper-Iranian-APT-Makes-a-Comeback-with-Thunder-and-Lightning-Backdoor-and-Espionage-Combo.pdf.

[6] Department of Homeland Security. In: (Mar. 21, 2019). URL: https://2017-2021.state.gov/amendments-to-the-terrorist-designations-of-the-islamic-state-of-iraq-and-syria/.

[7] Intezer. “Prince of Persia: The Sands of Foudre”. In: (Aug. 17, 2018). URL: https://intezer.com/blog/prince-of-persia-the-sands-of-foudre/.

[8] Malpedia. “Infy”. In: (Jan. 7, 2026). URL: https://malpedia.caad.fkie.fraunhofer.de/actor/infy.

[9] Check Point. “After Lightning Comes Thunder”. In: (Feb. 8, 2021). URL: https://research.checkpoint.com/2021/after-lightning-comes-thunder/.

[10] SafeBreach. “Prince of Persia: A Decade of Iranian Nation-State APT Campaign Activity under the Microscope”. In: (Dec. 18, 2025). URL: https://www.safebreach.com/blog/prince-of-persia-a-decade-of-an-iranian-nation-state-apt-campaign-activity/.

[11] Stockcake. In: (Jan. 6, 2026). URL: https://stockcake.com/i/electric-storm-pixel_2097850_1349155.

[12] Diana Johanna Velasquez. In: (Jan. 7, 2026). URL: https://www.vecteezy.com/free-vector/cloud.