Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

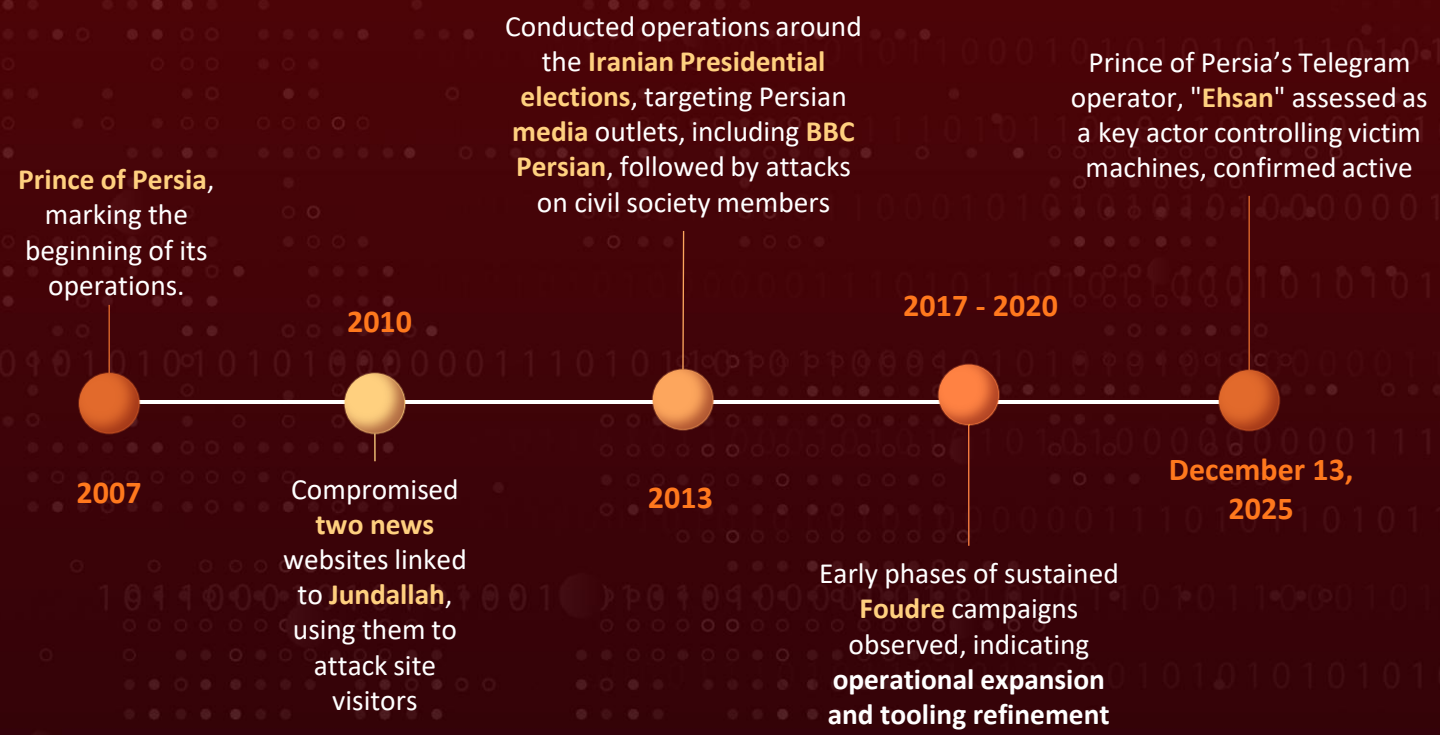
Prince of Persia APT Campaigns Across Iran, Europe, and Beyond

Date of Publication	Admiralty code	TA Number
December 23, 2025	A1	TA2025387

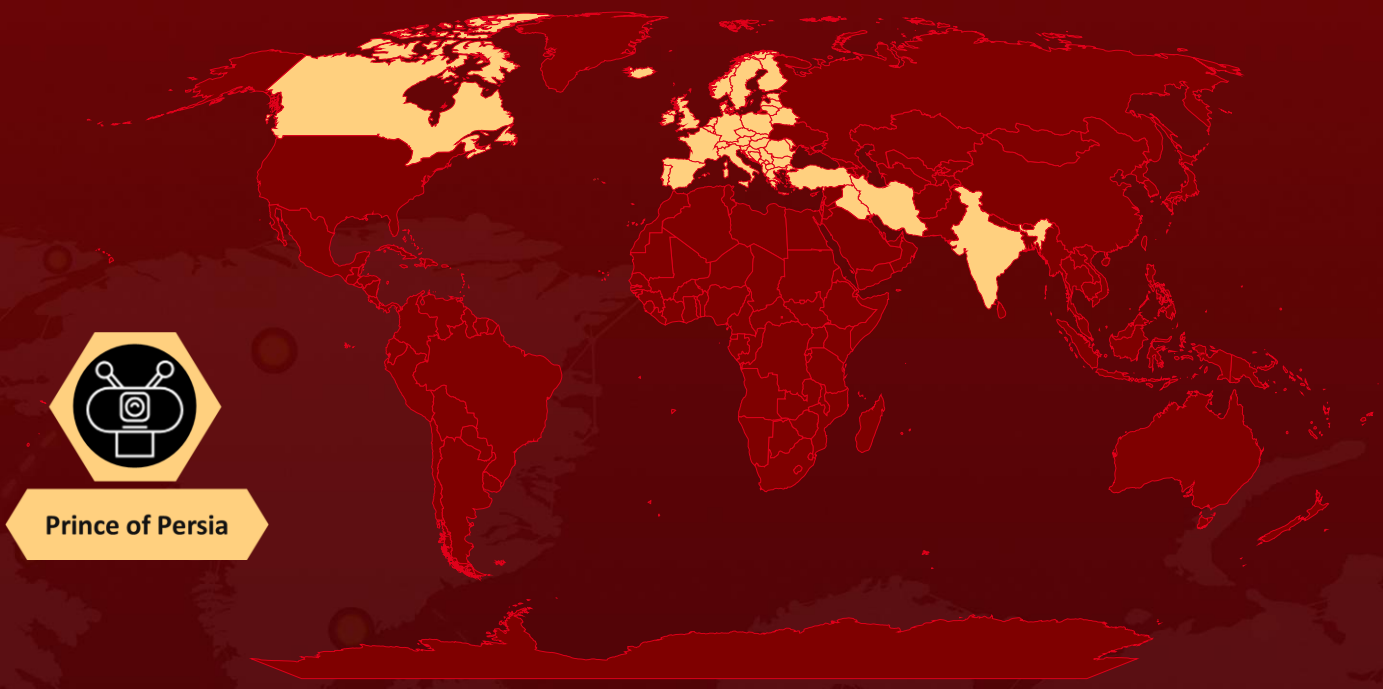
Summary

First Seen: 2007
Threat Actor: Prince of Persia (alias Infy, Operation Mermaid, APT-C-07)
Malware: Foudre, Tonnerre
Targeted Countries: Iran, Iraq, Turkey, India, Canada, Albania, Andorra, Austria, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Kosovo, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom, Vatican City
Targeted Industries: Critical Infrastructure, Telecommunication, Government, Private Sector, Media

Attack Timeline



Actor Map



Actor Details

#1 Prince of Persia, also known as Infy, is among the longest-running Iranian advanced persistent threat groups, with operations traced back to 2007. Multiple assessments attribute the group with high confidence to state sponsorship, acting in alignment with Iranian government interests.

#2 The group's early activity targeted victims in Iran and parts of Europe, establishing a foundation for long-term cyber-espionage. After several quiet years, Prince of Persia resurfaced in 2017 with a new malware family called Foudre, marking a renewed and more refined operational phase.

#3 Its campaigns rely on a two-stage malware architecture. Initial access is typically achieved through phishing emails that deliver Foudre, a downloader and system profiler. Foudre then deploys a secondary implant, Tonnerre, designed to extract sensitive data from selected high-value systems.

#4

Multiple active variants of both tools operate simultaneously, each using distinct domain generation algorithms to maintain a resilient command-and-control infrastructure across several servers. Recent iterations show further evolution. Tonnerre version 50 redirects communications through a Telegram group controlled by a bot, likely leveraging the Telegram API to issue commands and receive exfiltrated data.

#5

This shift reflects a move toward blending malicious traffic with legitimate platforms to reduce detection. Prince of Persia has a history of politically motivated operations. As early as 2010, the group compromised news websites linked to Jundallah, exploiting ActiveX vulnerabilities to infect site visitors. Activity intensified around the 2013 Iranian presidential elections, with a focus on Persian media outlets.

#6

In its most recent campaigns, the group has conducted covert operations across Iran, Iraq, Turkey, India, Canada, and several European countries. These attacks used updated versions of Foudre and Tonnerre, with the latest Tonnerre variant detected in September 2025. Delivery techniques have also shifted, replacing macro-based Excel documents with files embedding executables to install Foudre, reinforcing the group's continued adaptation and persistence.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
Prince of Persia (alias Infy, Operation Mermaid, APT-C-07)	Iran	Iran, Iraq, Turkey, India, Canada, Albania, Andorra, Austria, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Kosovo, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom, Vatican City	Critical Infrastructure, Telecommunication, Government, Private Sectors, Media
	MOTIVE		
	Information theft and espionage		

Recommendations

Harden Email and Document-Based Entry Points: Prince of Persia primarily gains initial access through phishing emails and weaponized Office documents. Enforce strict email filtering, block embedded executables, restrict document execution, and use attachment sandboxing. These controls directly reduce the success of Foudre-based delivery and initial compromise.

Implement Network Segmentation and Robust Access Controls: Isolate critical infrastructure and sensitive data from general user networks using network segmentation. Enforce strict access control lists (ACLs) to regulate traffic flow between segments, minimizing the potential for lateral movement during a security breach.

Detect and Disrupt Command-and-Control Infrastructure: Monitor for DGA-based DNS activity, anomalous outbound traffic, and suspicious use of messaging platforms such as Telegram. Focus on identifying abnormal DNS patterns, unexpected API usage, and unauthorized external connections to disrupt C2 communication and limit persistence and data exfiltration.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery
TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
T1598 Phishing for Information	T1583 Acquire Infrastructure	T1583.001 Domains	T1587 Develop Capabilities

T1587.001 Malware	T1588 Obtain Capabilities	T1566 Phishing	T1204 User Execution
T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.005 Visual Basic	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1543 Create or Modify System Process	T1543.003 Windows Service	T1027 Obfuscated Files or Information
T1027.002 Software Packing	T1140 Deobfuscate/Decode Files or Information	T1036 Masquerading	T1036.005 Match Legitimate Resource Name or Location
T1574 Hijack Execution Flow	T1574.001 DLL	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers
T1082 System Information Discovery	T1057 Process Discovery	T1518 Software Discovery	T1518.001 Security Software Discovery
T1056 Input Capture	T1005 Data from Local System	T1560 Archive Collected Data	T1071 Application Layer Protocol
T1568 Dynamic Resolution	T1568.002 Domain Generation Algorithms	T1102 Web Service	T1573 Encrypted Channel
T1105 Ingress Tool Transfer	T1041 Exfiltration Over C2 Channel	T1048 Exfiltration Over Alternative Protocol	T1485 Data Destruction

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	cb6ed0dd5dbc2e34ae36dd22b9522f7eec94bbfda2dcda7425736656279f8cdf, 30c20ada243b7e476e006dec94876bdeece4f8aca12a4cb6cf962c80f1a6ee3c, d9dfc8a8e3e259a517a91e2e91e3a1d6ef1d5b0886e6729bf897d6ef1b2de722, 43ccc2620229d88d5a6ca2b064da0554ec3c3cc29a097e7a2d97283257cfae69, 0bfc11c6ba57fdaa8b865555d80d8f7d7b1d0f41a23a277885198b3113c945d9, cf64bf78ce570f8085110defc8ec32ff4f01c7359723510b9d1923fd93d12240, fbb2ac0d07b84068aa35376cc994039f9fc1d2341643bc2bf268d65ab11ecbe3, 2c46406fb9111e0e4d982de54f335ae2900cdc39490d58f765cd5014153b3e12, 52abb57bf6f9db815b3ddf6241e21d4096f36eb998bb51e728bbe68c0f8e8e15, fa95a09e538b8c186a3239e3ff80ec9054b50aab80c624e75563ace4e60e31da, f54cfe296186644d0fed271c469af1ef9b6156affe9e030e7b83b8de097eb1e7, 6f976a685ae838a7062fb4f152c6c77c42168b78b9aadd4278ec1c19f9bc1055, 12847dc6dfd86603e8f0085ae561b4b2e3089e5414e49628f7c411483c7b5ce8, d3d8b79f86f152338aabeadfaf35ba2e43f82aa4bfa29ff70b59702b455fa6a6, 15dd41ec1bdaabb741e8cc6481e0a98831798ac4e93c2513cdbd00c51241ffb7, 52e3a856548825ec0a3d6630e881ff4f79d2a11bc3420a73d42e161fabed53d9, c8583fddf668808e31f993ff6bcfc6f8ba8b4c2c0c4ea51d4ccc6f5d311b6c90, 34692cabe9e9ba584ec2b8947a7aad4f787d10a3da56886e52d05d0675fe7b01, 5ad83f9fad87273593f9df73761de211a704e6e10984fde113a6435cc83c1e58,

TYPE	VALUE
SHA256	04844b5e15750467224c29b6fe5806e4093cd1d0ee4904dccf96831947574c85, b9741ad9ac084fb43804618acabe637f6b097bf72264b3335514678b2d0da785, a107635083212c662dbb3b69951e0de7b3d3894d8bcd7cfff545d119f81aeb1f, 23761caf7f4c6d7b3b4608c59729eb807c961deaa23aac94db5289b9b9739864, 09a2f03b5d54b48ba5f0df9ea57a6c20ba6fa90ad0f334132ea1da9320fbfbfd, a8565b678857129158904760ffe468e3ea6e4cf8a63a6c16b97e5717b1e8a384, de94830b9b4df6867b7d2888acca9f3d0c103933b01721c04e6bd6492bde9e58, 55d60bcf83c81fff25ca413dc2f720a671f522d79cc13b6d618f7f25094acd62, B1a16dd0500c570fb44cd13b68737fcd18710072559f810f3b3691ca93787cff
URL	hxxps[:]//api[.]telegram[.]org/bot7900216285[:]AAEVjLjt4csUKGanerJuuiDhdsmlUv0yooM/getChatMember?user_id=874675833&chat_id=874675833
IPv4	178[.]33[.]49[.]126, 45[.]80[.]148[.]35, 45[.]80[.]151[.]166, 45[.]80[.]151[.]24, 45[.]80[.]151[.]179, 45[.]80[.]148[.]128, 179[.]43[.]190[.]13, 45[.]80[.]151[.]71, 45[.]80[.]148[.]195, 45[.]80[.]148[.]124, 45[.]80[.]149[.]100, 198[.]252[.]108[.]158, 83[.]122[.]48[.]123, 37[.]156[.]153[.]108, 5[.]125[.]60[.]37, 37[.]156[.]155[.]168, 113[.]203[.]19[.]147
Domains	hkdhhwsafvnef[.]hbmc[.]net, zjnomxhcrkfc[.]site, Whpgwzunsijn[.]site, Gwmkgkfyovzy[.]site, Vitevjtlawkl[.]site,

TYPE	VALUE
Domains	Dmxqdlcuiryu[.]site, Rbhfrmezhmlz[.]site, Plfwpybxjysx[.]site, Oszzoalgfarg[.]site, 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, tegfxbnk[.]site, iiunewhmlz[.]site, zbddztherkfc[.]ix[.]tc, ffhbnqtsmv[.]site, auuxshqodj[.]ix[.]tc, ejjnhkucbw[.]ix[.]tc

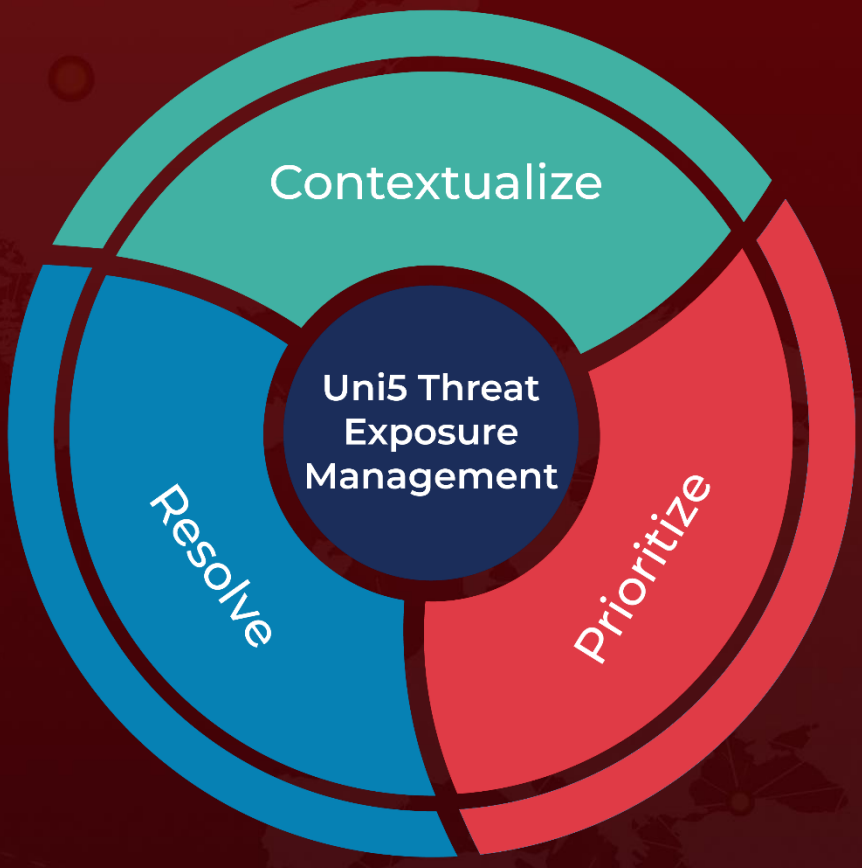
References

https://www.safebreach.com/blog/prince-of-persia-a-decade-of-an-iranian-nation-state-apt-campaign-activity

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 23, 2025 • 7:00 AM

© 2025 All Rights are Reserved by HivePro

More at www.hivepro.com