



LESSONS LEARNED FROM IRAN'S CYBER WARFARE IN 2020

TABLE OF CONTENTS

- 3** EXECUTIVE SUMMARY
- 4** IRANIAN CYBERWARFARE
- 5** 2020 INCIDENTS ON A GEOPOLITICAL TIMELINE
- 7** CONNECTING THE DOTS ON THE TIMELINE
- 8** A DEEPER LOOK INTO THE PAY2KEY CAMPAIGN
- 10** WHAT DID SENTINELONE DISCOVER?
- 12** LESSONS LEARNED: THE IRANIAN CASE IN A GLOBAL CONTEXT
- 13** ABOUT SENTINELLABS



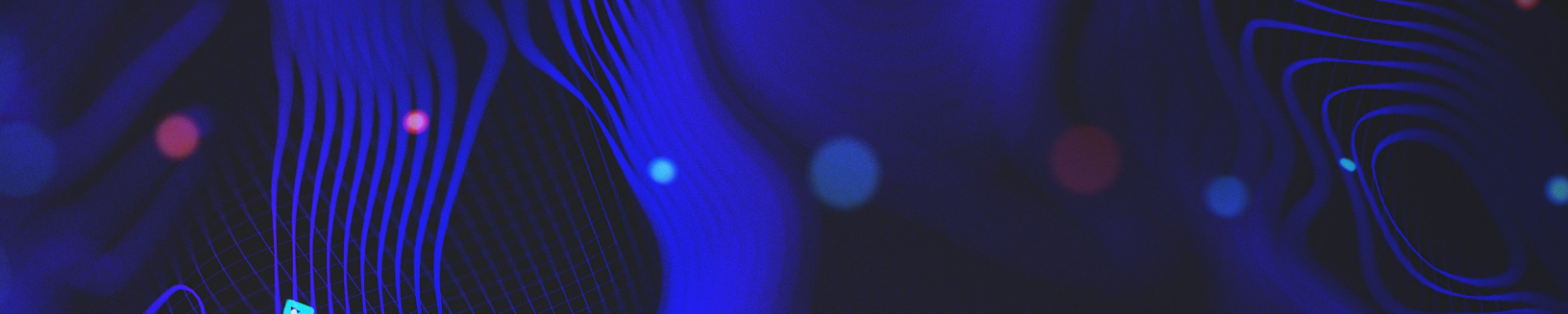
EXECUTIVE SUMMARY

Cyber warfare is commonly regarded as the “fifth domain” in which opponent forces fight, but of course cyber wars do not occur in isolation. Rather, they are part of a continuum of actions that encompass “classical” warfare in the physical dimension, nation state political processes and agendas, and state-backed cyber attacks such as those attributed to Iran during 2020.

Our research into Iranian cyber activities reveals the strong correlation between physical aggression and cyber retaliation. We also notice that Iran has adopted a more versatile and deniable style, using TTPs borrowed from cybercrime actors and exploiting “low hanging fruit” to deliver political messages to its regional rivals.

We demonstrate this thesis through the peculiar case of the “pay2key” campaign. On the surface, pay2key looks like any other ransomware attack, but its abnormalities indicate that it was something more than just a campaign aimed at extorting companies for financial gain.

SentinelLabs Team



IRANIAN CYBERWARFARE

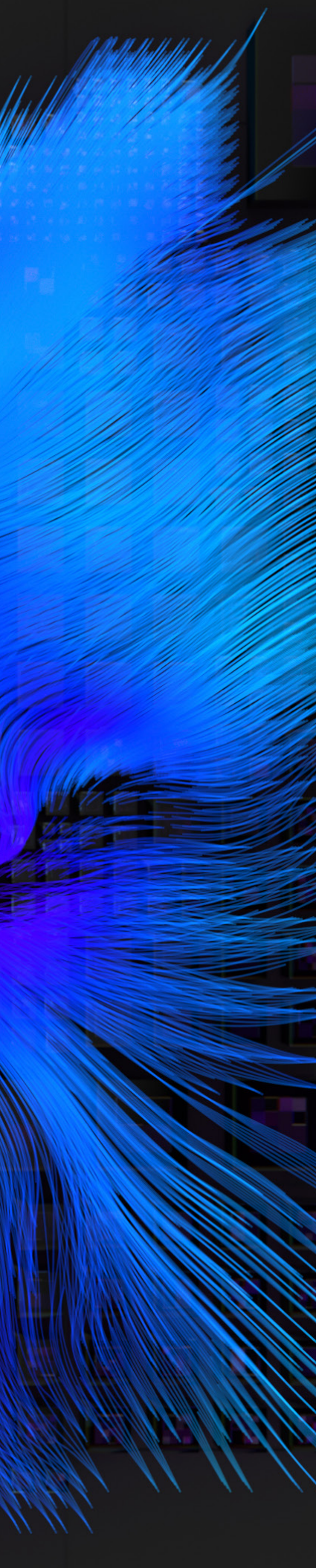
Long years of embargoes, financial and economic sanctions, and tensions with its regional opponents pushed Iran towards developing cyber warfare capabilities and use them widely, instead of or in addition to more traditional sorts of warfare. Supreme Leader Ayatollah Sayed Ali Khamenei is personally involved in making Iran's cyberspace more protected and resilient, while building its competence to hit opponents in the fifth domain.

Iran is home to numerous state-sponsored, state-affiliated, state-run and independent attack groups that operate to fulfil the interests of intelligence, government and military forces and agencies. While other nation-state related groups often use proprietary tools, zero-day vulnerabilities and persistent backdoors, the history of Iranian groups shows that they prefer a blend of off-the-shelf tools, "street style hacking", and exploiting strategic 1-days.

In addition, many of their operations are not made to last; on the contrary, they are made to be exposed to create a psychological effect. Iranian groups share with each other some features and targets, making attribution a tricky task, yet we can distinguish several well-established threat actors that continue to adapt as they challenge Iran's political opponents¹.

- OilRig (AKA APT34/Helix Kitten)
- MagicHound (AKA APT35/Newscaster/Cobalt Gypsy)
- APT33 (AKA Refined Kitten/Elfin)
- DarkHydrus
- Shamoon
- MuddyWater (AKA Static Kitten)

¹<https://unit42.paloaltonetworks.com/threat-brief-iranian-linked-cyber-operations/>



2020 INCIDENTS ON A GEOPOLITICAL TIMELINE

An eventful year

2020 was an intensive year in Iran's long history of cyberwarfare, influenced by geopolitical factors such as the U.S. elections, the economic pressure caused by COVID-19, and the tightening of cooperation between Israel and some of Iran's neighbours from the Gulf Cooperation Council (GCC). Although the Iranian regime did not confirm all the cyber attacks attributed to it, the timing and the symbolism of those attacks lead us and other researchers to believe that they stood behind them, as we will soon demonstrate.

In order to make sense of the scattered cyber attacks that are attributed to Iran, we should first mention a few impactful incidents that took place on the physical battlefield:

- On the night of January 3rd 2020, a United States drone struck near Baghdad International Airport, killing the Iranian Major General Qasem Solemani, the commander of Quds Force, the long arm of Iran's Islamic Revolutionary Guard Corps (IRGC). Solemani, who led Iran's operations outside the country and promoted the Iranian agenda with its affiliates like the Syrian regime, Hezbollah in Lebanon and the Houthi rebels of Yemen, was a powerful person who had been a member of the very intimate group of policy makers with the Iranian supreme leader, Khamenei. The absence of the dominant and charismatic leader was well observed in the ability of Iran to carry out operations and shape the regional balance of power.
- Between June 25th and July 19th 2020, a series of "mysterious explosions" hit numerous facilities around Iran, all related to nuclear research and weapons production, oil and gas middle/downstream infrastructure, and energy supply. One of the explosions happened in a facility which the International Atomic Energy Agency (IAEA) confirmed was a factory for advanced centrifuges. Iranian officials attributed the incidents to "Israel and its agents", and in some cases claimed that the explosion was caused by a cyber attack; however, they haven't provided any evidence to support those assertions.

- 
- In late November, Brigadier General Mohsen Fakhrizadeh was assassinated as he was traveling from Tehran to Damavand. Fakhrizadeh, a physics professor, had been leading IRGC's projects of nuclear weapon development for nearly three decades and was considered by many as "the brain" behind Iran's nuclear R&D.

Revenge is a dish better served cold (and far away)

Iran usually responds to such incidents twice: immediately, and after a while. The immediate responses - attempts to hunt down the attackers, publishing evidence from the case or sharing theories on what happened - are necessary for the regime to make a clear statement of unacceptance and intolerance. The postponed response, often weeks or months later, is always symbolic yet sometimes in a different context than that of the original incident, and serves to restore the balance of power but not to set a bigger fire. Therefore, trying to tag cyber attacks as revenge actions, we should expect a delay between the two.

A commonality between all the incidents mentioned here is that they took place inside Iran or in locations Iran considers its "backyard", such as Iraq. The reprisal action, however, seeks to rearrange the strategic set up and move the combat as far from Iran's borders as possible, according to its defensive doctrine dubbed "forward defense".² The original purpose of this doctrine was to avoid conflicts between the revolutionary base and the reformist one and push away controversial actions from the national grounds. In this regard, the cyber dimension is the ultimate battlefield: it is "distant" (in a sense), free, full of opportunities, and the adversaries can keep their actions discrete and deniable.

CONNECTING THE DOTS ON THE TIMELINE

Red - physical

Blue - cyber

- J-03 - Soleimani assassination.²
- Jan-04 - “Down with America”: ~50 websites defaced by Iranian and Palestinian hackers.²
- Apr-23 - Attack on Israeli water infrastructures (the campaign targeted controllers that were exposed to the internet, and was detected before causing harm).
- May-09 - Disruptive cyber attack on Iran’s Shahid Rajee port, causing operational shut down.²
- Jun-25 to Jul-19 - Explosions in weapons production and energy sector facilities in Iran.³
- September - Muddywater campaign against Israeli organizations, aiming to deploy a commodity ransomware.⁴
- October - Iranian hackers attempt to breach emails of Trump campaign team members⁵
- November-Mid December - pay2key campaign, attributed to unknown threat actors in Iran, hits several Israeli companies.⁶
- Nov-03 - US presidential elections.
- Nov-25 - Fakhriadeh assassination.⁷
- Dec-01 - Attackers release a video showing a breach into a virtual HMI (human-machine interface) of a water reservoir in Israel. In reality the attack failed.⁸
- Dec-01 - Shirbit, an Israeli insurer, attacked by a previously unknown ransomware, refuses to pay \$1M ransom claim.⁹

The sequence of actions and attacks shows a possible correlation between physical attacks against Iran, and cyber attacks Iran initiated in response. However, Iran never admitted that any of its official forces actually stood behind the attacks, allowing its opponents to “contain” the attacks without undesired escalation.

While some attacks, like the Muddywater campaign of September 2020, were easily attributed to Iran by the TTPs they used, other attacks that leveraged off-the-shelf commercial attack tools and disposable infrastructures were harder to attribute, yet it became possible thanks to OpSec flaws that exposed some of the attackers’ deep infrastructures and due to the list of victims which consisted only of Israeli companies and organizations. The case of the pay2key campaign, which reached its peak in December 2020, is an interesting example of that.

¹<https://www.cybersecurity-insiders.com/cyber-attack-on-israel-water-system/>

²https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

³https://en.wikipedia.org/wiki/2020_Iran_explosions

⁴<https://www.clearskysec.com/operation-quicksand/>

⁵<https://www.bbc.com/news/world-us-canada-49940657>

⁶<https://www.bankinfosecurity.com/pay2key-ransomware-campaign-targets-israeli-firms-a-15631>

A DEEPER LOOK INTO THE PAY2KEY CAMPAIGN

What is it? What happened?

Pay2key is an offensive campaign that hit mostly Israeli companies from late October to mid December 2020. The victims of the campaign belong to several business verticals, not necessarily related to each other. For example, Israel Aerospace Industries (IAI) was attacked, as well as Habana Labs (a chip maker, acquired recently by Intel) and Portnox (a provider of IT services).

For a few days, the campaign made the headlines across the nation, and pushed many to ask themselves whether they would be the next victims.



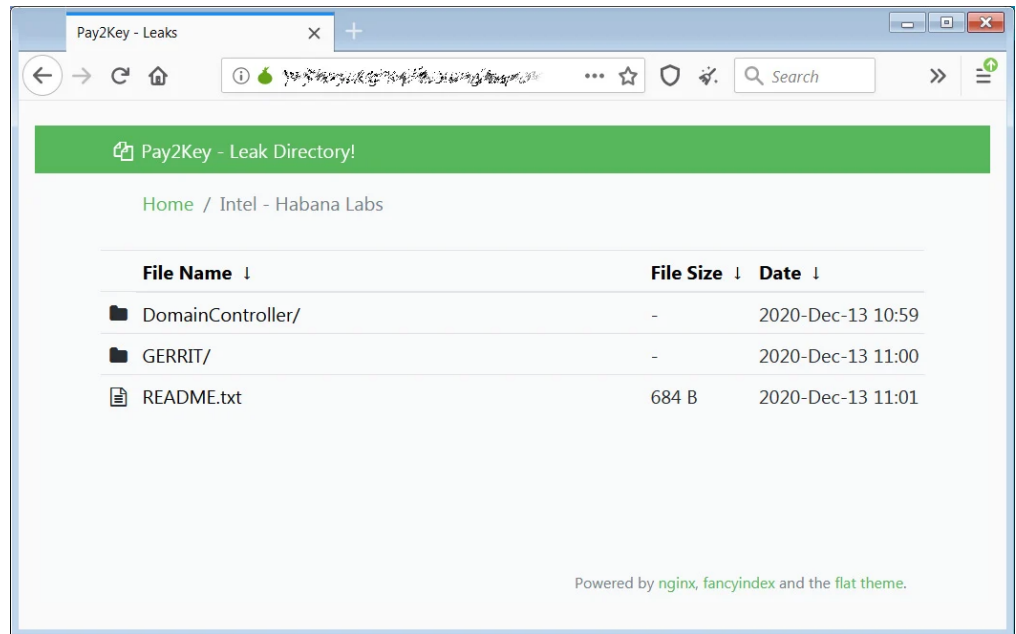
Pay2key leak directory. Source: Geektime

⁷<https://www.inss.org.il/publication/fakhrizadeh/>

⁸<https://www.trustnet.co.il/blog/cyber-attack-on-israeli-water-reservoir/>

⁹<https://www.timesofisrael.com/israels-supply-chain-targeted-in-massive-cyberattack/>

The attackers used RDP connections to establish initial access, then stole large volumes of data from the infected networks and deployed an advanced encryption, leaving a “ransom note” that demanding a ransom payment in Bitcoin. To amplify the pressure on victims, the attackers threatened to leak data if not paid fully and on time. In some cases, these threats were carried out.



Inside Pay2key’s leak site, showing files stolen from Habana Labs. Source: Bleeping Computer

At first sight, it seems like a common ransomware campaign, perhaps of a new strain. However, the fact that the campaign targeted only Israeli companies led researchers to look deeper into it. Through tracking the bitcoin wallet, researchers were able to link the campaign to Iran and assess with high certainty that the attackers started preparing the campaign’s infrastructure in late June¹⁰.

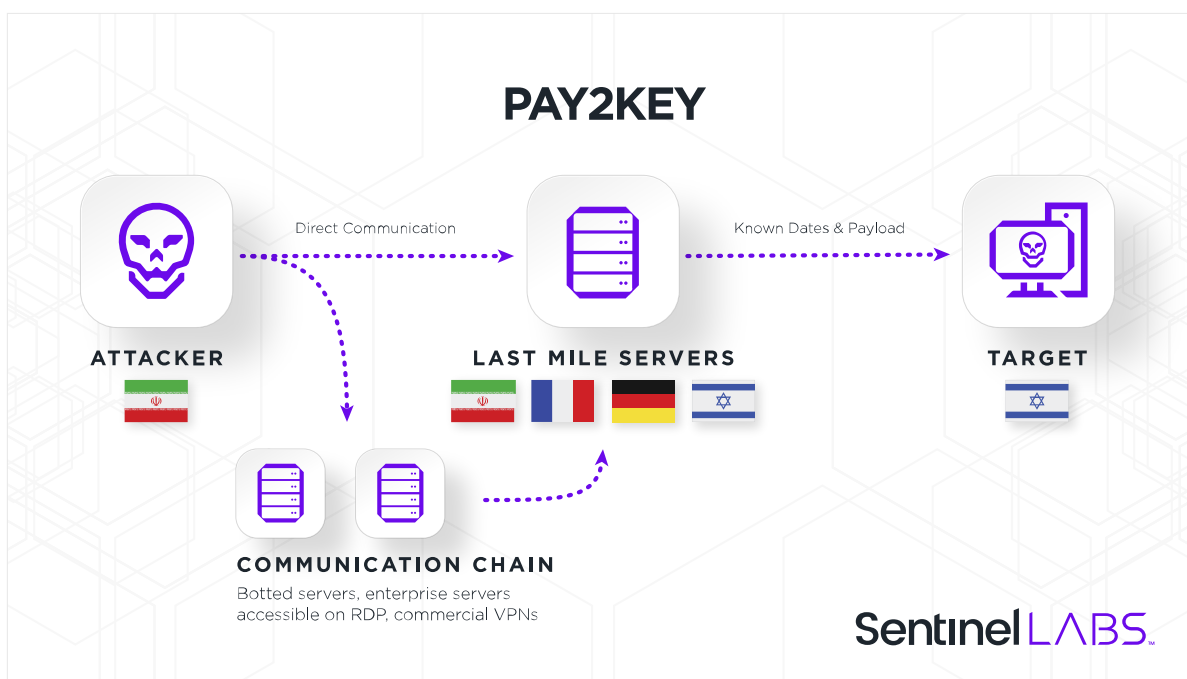
¹⁰<https://research.checkpoint.com/2020/ransomware-alert-pay2key/>

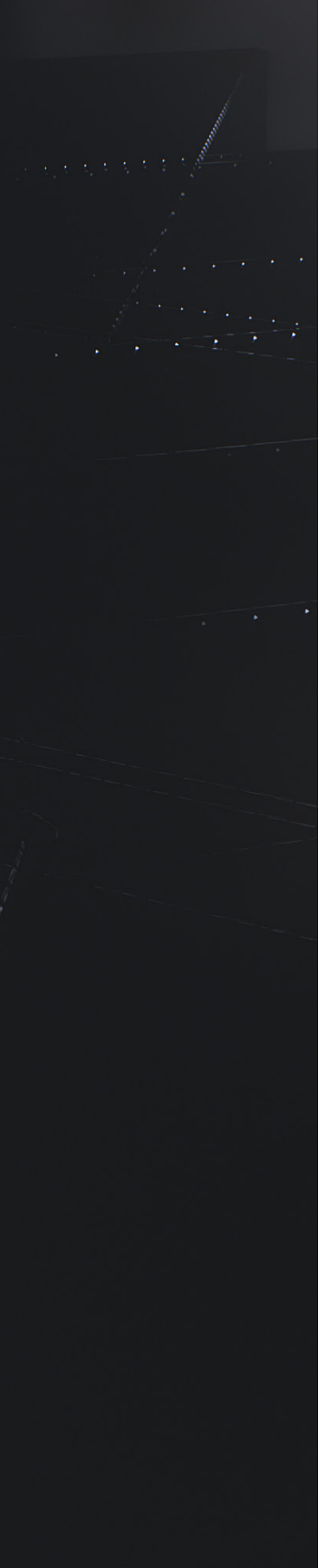
WHAT DID SENTINELONE DISCOVER?

SentinelOne investigated the campaign's C2 infrastructure, which consisted of several servers that were active from (at least) October and until December 20, 2020, when most were publicly exposed and reported. Examining the communication patterns, activity times and targets helped us assess with high certainty that the campaign originated from Iran.

Core Findings:

- Investigating the communication patterns of the C2s involved in the attack, SentinelOne found that they were approached over RDP port (3389) by chains of publicly exposed servers. In addition, the suspected C2s involved in the attack were also used by other users not related to the campaign. Both findings demonstrate how the pay2key campaign used disposable infrastructures in order to evade detection and blocking.



- 
- The attackers used the same C2 infrastructure to attack many targets, and did not ditch a server after a “successful” attack on a specific target.
 - SentinelOne confirms that the campaign only targeted Israeli organizations, strengthening our assumption that pay2key was supported or initiated by an opponent nation-state actor.
 - SentinelOne found that pay2key kept its C2s alive until the end of December 2020, although most of them had been reported two weeks earlier.

Of particular significance was the campaign’s list of targets:

- Six large shipping companies, some of which are representatives for global giants;
- Five IT companies that provide cloud services, IT management, Microsoft 365 licenses, and ERP systems. Closer investigation on those companies revealed that most are contractors of defence organizations or providers of some critical infrastructure and services;
- Three engineering companies that provide turnkey project management and other solutions to defence organizations and military industries;
- A provider of medical labs equipment, involved in performing COVID-19 tests;
- The targets were all commercial (no governmental entities at all)

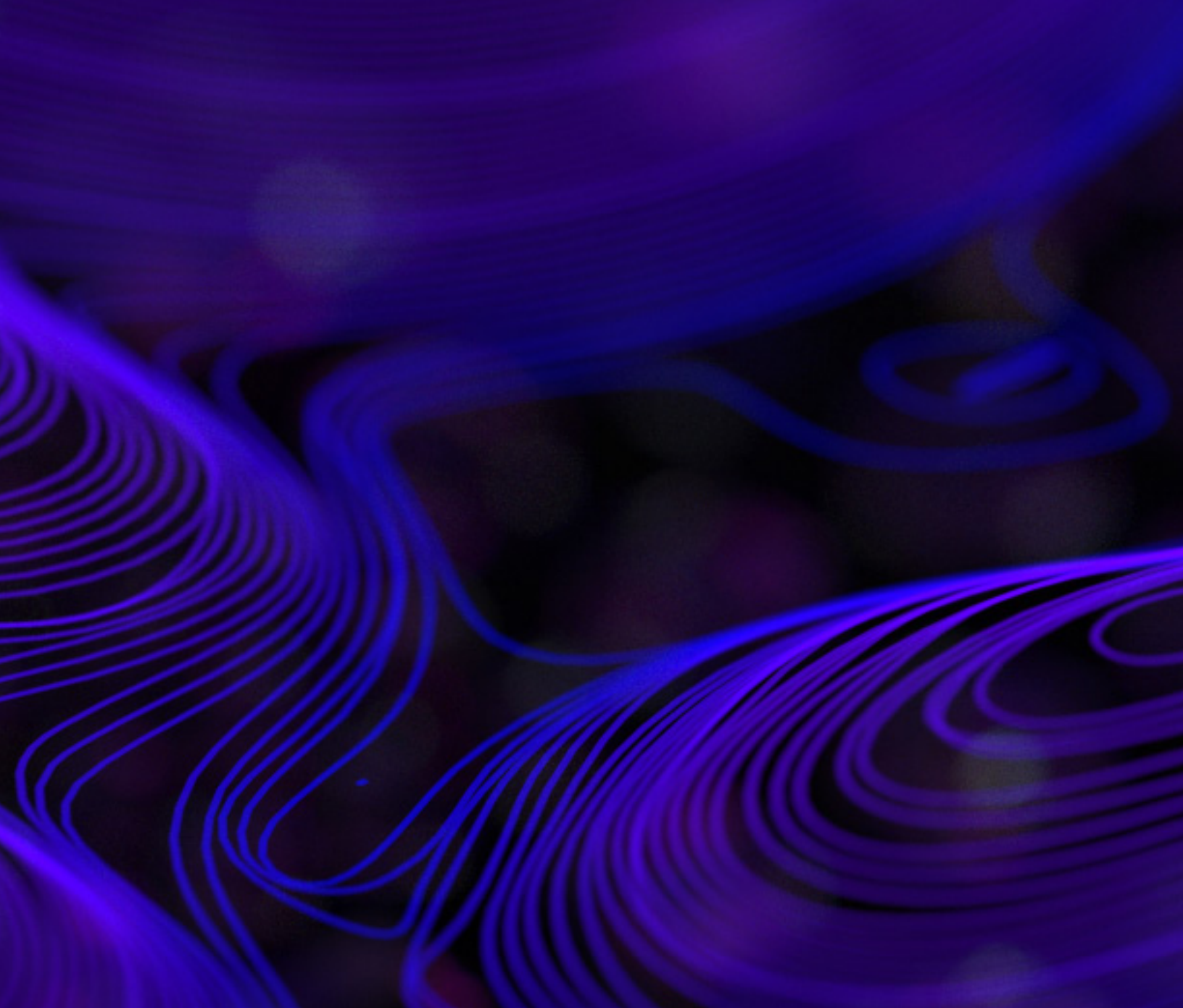
While the use of TTPs that regularly belong to financially-motivated cybercrime activities makes it harder to attribute and easier for accused entities to deny, by adding our findings to what we already know about pay2key, we can now assess with high certainty that the campaign originated from Iran with the objective of causing havoc and confusion.

LESSONS LEARNED: THE IRANIAN CASE IN A GLOBAL CONTEXT

The chronicle of the Israeli-Iranian conflict in the past year demonstrates how much the cyber dimension has become an undetachable part of the modern battlefield, where a sabotage action against a military asset, or an assassination, is responded to with a cyber attack against a critical infrastructure or sensitive data.

While on a traditional battlefield, civilians are supposed to be kept out of the fire zone, the opposite happens when the war shifts into the fifth domain. Contractors, suppliers, partners or just companies that are essential for the normal functioning of a nation become legitimate targets, and their preparedness and resilience isn't always appropriate, to say the least.

Learning from the specific case of pay2key, we foresee that more threat actors will choose to carry out similar attacks that masquerade as ransomware campaigns or other “miscellaneous cybercrime”. It is especially beneficial for TA's that lack powerful tools like 0-day vulnerabilities and highly clandestine RATs, or for those who prefer to avoid using their proprietary tool arsenal for such purposes. Moreover, as such “commercial-like” attacks require a lower level of knowledge and sophistication, we should expect more nation-state actors to join the game and realize their geopolitical goals in the digital dimension.



ABOUT SENTINELLABS

The missing link in infosec today is not about alerts - it's about the context of those alerts. What, When, Where, Why, How and most importantly - Who. SentinelLabs came to life to solve the gap security practitioners have between autonomously protecting their enterprise assets and understanding the significance and story of alerts. Unlike other threat intelligence solutions, SentinelLabs does not focus on sharing what is already public knowledge. We focus on new findings that can assist enterprises in staying protected from adversaries. We cover both cybercrime and APT (nation-state) while having a voice in the larger community of threat hunters who are passionate about a world that is safer for all. In addition to Microsoft operating systems, we also provide coverage and guidance on the evolving landscape that lives on Apple and macOS devices. <https://labs.sentinelone.com/>