The Curious Case of Predatory Sparrow

Reconstructing the Attack from a 4th party collector's point of view

Hamid Kashfi

[Update: December 18th, 2023]: On 18th December, Predator Sparrows launched a second attack against the fuel distribution system in Iran, similar to their previous operation in 2021. Since 2021, Iranian officials or third-party security vendors have not published any analysis or technical details about the original attack, which is not unusual. Their screenshots from the latest attacks provide some clues that only confirm our previous work, indicating connections to the "Yaas Arghavani" company, a VSAT and POS service provider for the fuel distribution system. The following is an old draft from December 2021, which I wrote for peer eyes rather than public view. The original draft focused on the first attack against the fuel distribution system. Still, some remarks remain valid and relevant to the recent attack on 18 Dec 2023, as little has changed regarding how the system works. The same infrastructure, same suppliers, and same 3rd party vendors, so we are likely just talking about a different attack vector and entry point from the previous case. I will probably draft a new note about the recent attack from scratch soon and when more details are gathered rather than updating the old speculative work.

The new attack itself is not an unexpected incident. Following the recent situation in Israel and Gaza, which led to various cyber operations by multiple proxy actors, Some of the Iranian proxy actors launched attacks against Israelis and, more recently, American infrastructure. As the following draft explains, attacks against critical infrastructure often have consequences. The Predatory Sparrow's initial attack in 2021 against the fuel distribution system was a warning to Iranians in response to some of their operations back then, which were crossing lines and unwritten rules of engagement. Iran has crossed the same lines again, which triggered the same actor's response now!

I have carried on with work on the subject since the original draft in December 2021 and updates in January 2022, that are not reflected there. Moreover, we have been observing many interesting (and relevant) incidents since then that have been discussed publicly by myself or other individuals interested in them. The most recent publication worth noting has been Juan's presentation at LABSCon 2021 and our discussions about the subject during a GlassHouse OpenCall back in 2022.

The original works were a group effort by myself, Juan Andrés, and Silas Cutler, and a number of individuals who prefer to remain anonymous but deserve credit for their help through the process, and I would like to thank them again.

[The original draft, December 2021]:

On October 26th, 2021, Iranians woke up to the news about yet another cyber attack against the country. Unlike all previous cases, which ranged from dismantling spinning centrifuges to wiping computers of Ports & Maritime Organization, the latest hit broke some norms and unwritten codes of conduct, directly targeting so-called critical infrastructures of a country, interrupting the daily lives of millions by putting every single gas pump and station in the country out of service. Ukraine has already tasted the effects of similar attacks, but even there, we have witnessed the second-order impacts of (an intentionally broken) ransomware attack spreading worldwide. This attack was specifically tailored to interrupt the daily lives of civilians nationwide by cutting the fuel distribution, hard enough to potentially cause domestic conflicts and riots against the government, but not too hard to cause irreversible and long-term technical damage and also carefully planned to not directly cause casualties as the result of cutting emergency services off of their fuel supply by giving them an early warning.

The early warning attempt is an interesting aspect of the attack to explore and was rarely seen before. It indicates significant intelligence operation, mature planning (controlled damage), and knowledge about a notable number of (ranked) individuals managing and operating emergency services such as ambulances or fire bridges. The Attacker hand-picked these individuals, based on their daily jobs and organizational hierarchy, to deliver a warning message about an imminent fuel outage and instruct them to refuel before the outage. While the identity of some of these individuals could not be confirmed (through previous Iranian civilians' personal information leaks), the fact that the attackers have gone through this is an essential operational detail. Such early warning minimizes the risk of potentially fatal side effects. It is unclear if any of the receivers of the warning acted up on it.

Another important operational aspect of the attack is that, despite having complete access and capability of delivery, the Sparrows chose to cause minimal yet effective damage to the system. Predatory Sparrows only wiped middle-level management servers and temporarily disabled POS terminals at gas stations by reconfiguring them into an unusable state, demanding the physical presence of operators at the stations to restore. They were in position and capable of doing the following damage to the system but planned not to:

- Erase and damage POS terminals by exploiting vulnerabilities that would allow them to corrupt the devices into a state that system operators could not recover, even with physical presence and access to terminals.
- Wipe central management servers and other systems in the compromised data center
- Wipe customer data and records or backup data of the fuel system
- Push corrupted data, wipe or deactivate the smart cards issued to customers
- Tamper with customer’s quota, for example, lifting quota limits for all customers
- Publicly release customer or other sensitive data related to the fuel system, such as sensitive smart-card details that could have forced nationwide reissue of cards to customers.

Such attacks against critical infrastructure (Fuel supply system being one) are usually considered off-limits by many nation-state actors as they can escalate into more severe forms of conflict and response. In this case, the attackers stepped on that line, showing their capability, but did not cross it far. Despite the scale of the attacks, Iranian officials could also revive the system in a reasonable time. One of the reasons this attack did not turn into chaos was that soon after the incident, stations were already back to business but were selling gas at regular prices and not subsidized. This is a crucial observation and point about their operation, **aimed at delivering a bold message rather than simply causing chaos.** A similar effort by Sparrows can also be observed in their attempt to deliver targeted messages that would be visible only to forensics teams. During their attack against the Ports & Marine organization (No public proof or confirmation), some internal systems were also wiped, but instead of random bytes or encrypting disk contents, disks were wiped with specific classified information.

As of today and the release of this draft, while Iranian officials have confirmed the attack and partially admitted its significance publicly, technical details have yet to be released to the public by government organizations in charge or by private threat-analysis companies in Iran. Very few details and even a speculative so-called forensics report from a 3rd party company (Modaberan Group) have been circulating, none pointing to facts or confirming technical aspects of the incident.

As interesting as the attack might be, and we will uncover some details about it, the main focus of this post is not the attack itself. As part of gathering information and details about the attack, we discovered something uncommon and strange. The Iranian government has always been highly restrictive and vague when it comes to sharing technical information about major cyber attacks against them. If foreign threat intelligence companies do not publish a technical analysis of a case, we rarely see an official statement backed up by technical facts. Even less so, we see Iranian threat analysis and CERT-like organizations voluntarily releasing full technical details of an attack. Yet, in this case, we got a rare opportunity to shoulder surf the individuals responsible for forensics of the attack live, as they handed over hundreds of megabytes of memory dumps from attacked systems and uploaded them to public websites, hoping to find shreds of trails from attackers. We are still determining what exactly they managed to find out, but instead, we observed these reckless attempts that put us in the position of a 4th-party collector. **We also cannot rule out the possibility that even these “mistakes" were part of the same operation.**

The Smart Fuel System in Iran:

Before discussing the attack and its significance, we need to understand how the gas distribution system in Iran operates and is managed. Gas prices in Iran used to be heavily subsidized for decades, keeping it reasonable and in balance with an average wage in the country. Over the years, the low price of gas contributed to issues such as mismanagement of consumption and trafficking of gas to neighboring countries. As part of a plan to reduce the trafficking issue, a new smart quota and distribution system was introduced and enforced nationwide in 2007. In this new system, every registered vehicle received a fixed quota, which the owner could use at subsidized prices. Owners of the cars receive a smart card tied to the vehicle's license plate and protected by a PIN code, used as an authentication mechanism at gas stations. Every pump at the gas station is equipped with a POS machine, which shows the remaining quota for the card. The station staff then handles Payment for the fueling separately via cash or regular payment cards.

Once you use your quota (currently about 60 liters per month for regular vehicles), you can refill your refuel at gas stations, but it will cost you triple the price!

Increase in gas prices & protests:

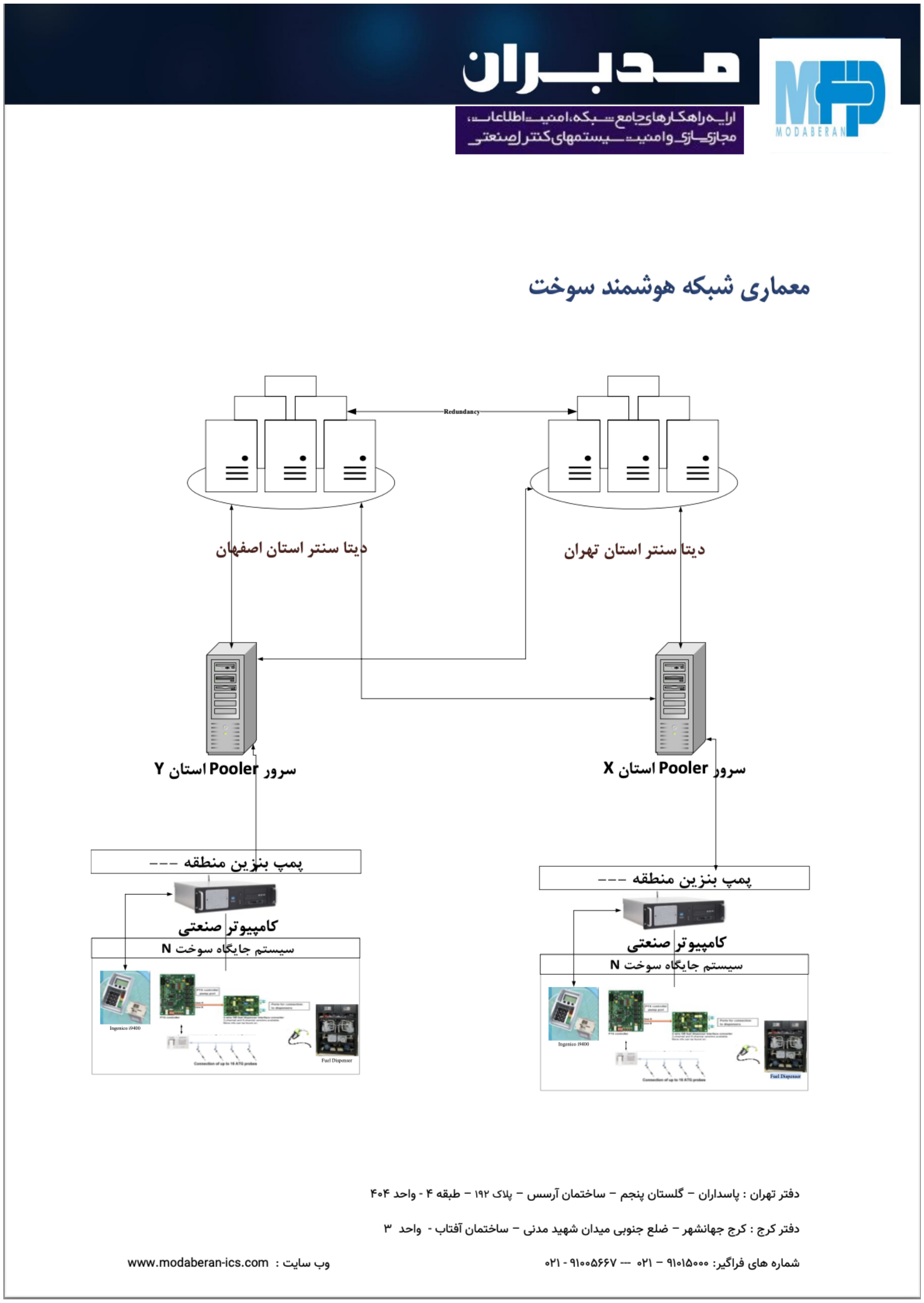
Over the years, people became accustomed to these new regulations, and fuel consumption was notably reduced across the country. Later, the government increased the prices annually for subsidized and unsubsidized distribution. Annual increases, despite complaints, were gradually accepted by the people. However, The Iranian government occasionally and irrationally increases the prices to the point of causing sudden and significant inflation in prices for pretty much any item used by people daily. The most recent spike in prices happened on 15th November 2019. Overnight, the subsidized gas price increased by 50%, and the non-subsidized price was up by 200%. The spike was so drastic and unexpected that it caused riots and protests across the country, which continued for multiple weeks and led to a brutal crackdown on civilians. Hundreds of civilians were killed and thousands injured in the streets by official and undercover anti-riot forces across the country.

The recent attack against the gas distribution system in Iran happened on the 2nd anniversary of these protests, which one can admit could have the potential to revive tensions and remind people of the brutal crackdowns by the government. That did not happen; however, the reasons and how the Iranian government handled the incident are beyond this draft.

The Smart Fuel System Architecture:

Contrary to the claims of the officials in Iran about the unique architecture of the smart fueling system and taking pride in implementing the system using home-grown products and solutions, many of the software and hardware components, especially the key components responsible for handling the smart card, transactions, managing POS systems, and the underlying framework that interconnects gas stations with central management systems are based on (now obsolete) commercial products. Specifically, the core of the system and hardware are based on products of Ingenico, a French company. Idea-Negr, the Iranian company in charge of the original design and implementation of parts of the system, both hardware and software components, has built a management system on top of and based on Ingenico products and platforms tailored for the needs of the smart fuel system in Iran. They are also open about this and mention inheriting the designs from Ingenico. Regardless, the smart fuel system is a complex and multi-layer architecture with many components and connections, each of which can be subject to attacks. As significant and effective as the design is, it has been a hardly homemade product the Iranian government claims it to be.

The system's architecture and implementation are pretty elaborate but can be summarized as the following diagram, obtained from an analysis report by Modaberan company.



مدبران

MODABERAN

ارایه راهکارهای جامع شبکه، امنیت اطلاعات، مجازی سازی و امنیت سیستمهای کنترل صنعتی

معماری شبکه هوشمند سوخت

دفتر تهران : پاسداران – گلستان پنجم – ساختمان آرسس – پلاک ۱۹۲ – طبقه ۴ - واحد ۴۰۴

دفتر کرج : کرج جهانشهر – ضلع جنوبی میدان شهید مدنی – ساختمان آفتاب - واحد ۳

شماره های فراگیر: ۹۱۰۱۵۰۰۰ – ۰۲۱ --- ۹۱۰۰۵۶۶۷ - ۰۲۱

وب سایت : www.modaberan-ics.com

[The fuel system diagram, Modaberan report, page 5]

POS & Fuel Dispenser:

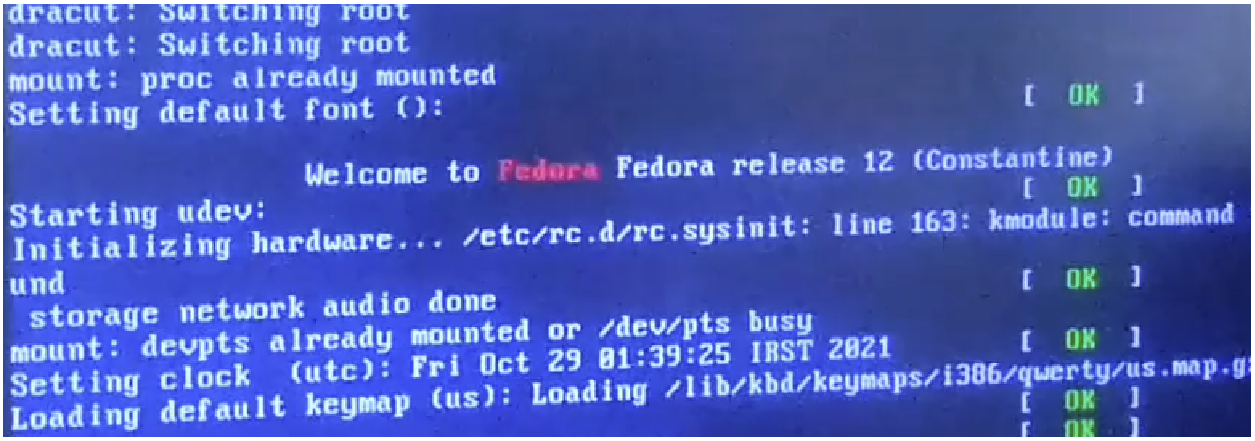
Every fuel dispenser and pump at the gas station has two main controller parts that handle the operations. A microcontroller board manages the fueling operation, such as commanding pump activation or measurement of dispensed fuel. The second part contains the POS smartcard reader interface, a pin-pad, and an integrated controller. The microcontroller board handling fueling operation is connected to the station management server (IPC) using serial data connections. The POS package, however, runs the proprietary firmware of Ingenico, is implemented, and operates based on common security standards for payment systems.

POS terminals and controller boards of fuel dispensers are connected via ethernet and serial connections to a customized computer at every gas station, known as an IPC server.

IPC Servers:

The IPC server operates and monitors gas pumps, handles telemetry data of the station, and is also used to manage and update the firmware and data on POS terminals if necessary. The same system is also responsible for pulling and pushing the latest customer data, such as fuel quotas, to the smart cards.

Each IPC server acts as a remote agent for the central management system. The IPC runs a customized version of Linux based on the Fedora 12 distribution (likely not receiving upstream security updates).



```
dracut: Switching root
dracut: Switching root
mount: proc already mounted
                                                          [  OK  ]
Setting default font ():

              Welcome to Fedora Fedora release 12 (Constantine)
                                                          [  OK  ]
Starting udev:
Initializing hardware... /etc/rc.d/rc.sysinit: line 163: kmodule: command
und                                                       [  OK  ]
 storage network audio done
mount: devpts already mounted or /dev/pts busy
                                                          [  OK  ]
Setting clock  (utc): Fri Oct 29 01:39:25 IRST 2021
Setting clock  (utc): Fri Oct 29 01:39:25 IRST 2021
Loading default keymap (us): Loading /lib/kbd/keymaps/i386/qwerty/us.map.g
                                                          [  OK  ]
                                                          [  OK  ]
```

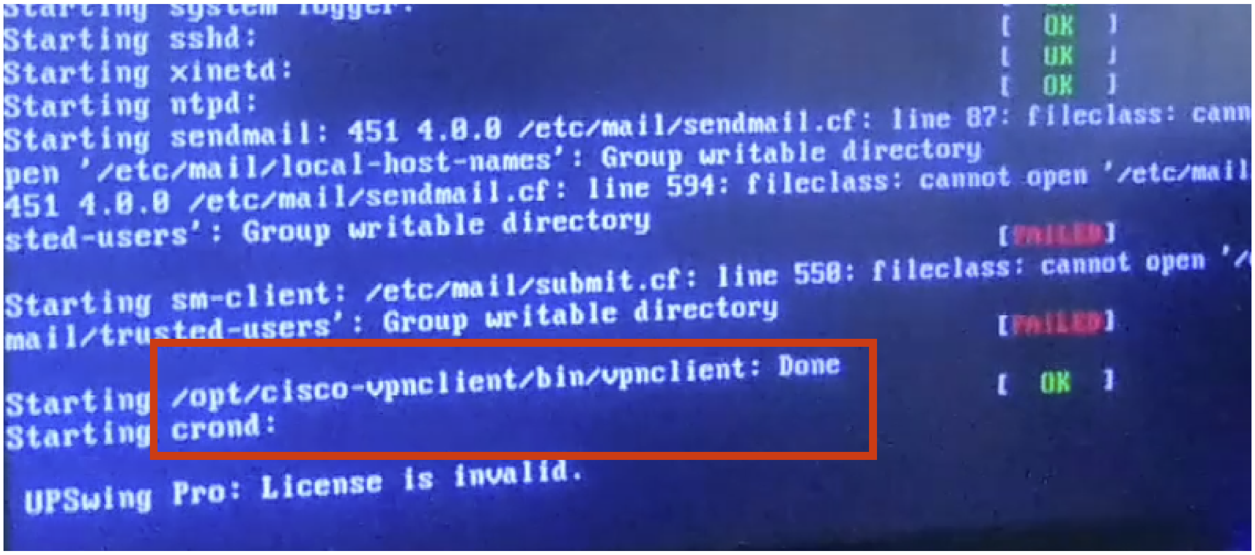
[The Gas station platform server boot log, running Fedora 12]

Pooler Servers:

IPC servers and their data are aggregated and managed remotely in larger regional groups via Pooler servers. Based on the information from the Modaberan company analysis report, which we will address later, there are eight aggregation points or Pooler servers geographically distributed across the country. Pooler servers connect to the data center using VSAT terminals.

Connections between Pooler servers, IPC servers, and gas stations are mentioned in this report to be based on E1 dialup connections, APN, or intranet. We have independently observed that many gas stations also use VSAT terminals or LTE modems for connectivity.

IPC servers use pre-configured VPN connections (Cisco VPN implementations) to secure access.



```
Starting system logger:
Starting sshd:                                                     [  OK  ]
Starting xinetd:                                                   [  OK  ]
Starting ntpd:                                                     [  OK  ]
Starting sendmail: 451 4.0.0 /etc/mail/sendmail.cf: line 87: fileclass: cann
pen '/etc/mail/local-host-names': Group writable directory
451 4.0.0 /etc/mail/sendmail.cf: line 594: fileclass: cannot open '/etc/mail
sted-users': Group writable directory
                                                                   [FAILED]
Starting sm-client: /etc/mail/submit.cf: line 550: fileclass: cannot open '/
mail/trusted-users': Group writable directory
                                                                   [FAILED]
Starting /opt/cisco-vpnclient/bin/vpnclient: Done                  [  OK  ]
Starting crond:
 UPSwing Pro: License is invalid.
```

[The gas station platform server boot log shows Cisco VPN client initialization.]

The datalink between the datacenter and IPC servers is supposedly over an MPLS network and not exposed over the internet, so everything operates as part of a giant intranet network nationwide. In reality, however, different gas stations use other methods to call back home. Most remotely located stations use VSAT terminals, piggybacking an existing VSAT network operated by Bank-Mellat. Over the years, many stations have switched to local infrastructure provided by DCI (Data Communication Company of Iran). We also observed many stations using LTE connections to connect to the Internet using SIM cards provided by the MCI (Mobile Telecom Company of Iran). As one might have guessed, VSAT terminal modems and LTE CPEs already break the promised “isolation” of this system's sensitive management network. More on this later. Whether an isolated APN and specially issued SIM cards for gas stations are used or whether they share the infrastructure with regular MCI customers is unclear to us.

Data-Centers:

At the system's core, management servers operate at two data centers in Tehran and Isfahan, pulling data from the pooler servers and all IPC servers, POS, VSAT, and other connectivity terminals across the country. The central monitoring interface of the system, developed by Idea-Negr, is a combination of web applications implemented in PHP and partly Java and an eye-opening series of shell scripts. More on these systems later.

Anyone with privileged access to these management systems could remotely control, upgrade, or nuke IPC or even POS terminals nationwide. That is precisely what went down during the incident. Still, the process is slightly more complicated than compromising a broken PHP web application and injecting OS commands all over the network to IPC servers and POS systems. Software updates for POS terminals and IPC servers are distributed as RPM packages over the network. In addition and by design, POS firmware is usually cryptographically signed. Even with access to the infrastructure, pushing rogue firmware and configurations to POS devices, as observed, would require attackers to obtain digital certificates and cryptographic keys. The security features mentioned here are not unique to the smart fueling system and are common among manufacturers producing payment solutions.

The core management systems in the data center must communicate with several external systems. For instance, registration details of each vehicle, information about the individual customers, and information about stolen and lost smart-card reports must be obtained from third-party entities. NIOC (National Iranian Oil Company), the higher-up organization in the chain and charge of the system, naturally provides some of these details via dedicated APIs to the smart fuel system and its operators.

Tech-Support Portal:

Besides the operational and management systems, a secondary technical support portal lives alongside the system on the same infrastructure and data center. This portal aims to receive support inquiries from gas station operators regarding issues and maintenance of IPC servers on-site.

Potential Attack Vectors:

Based on the architecture of the system and various technical artifacts obtained through the investigation, we can speculate more likely and potential ways that the system could have been compromised, in no particular order:

- **VSAT Communications:** Many of the gas stations and supposedly Pooler servers are connected to the data-center via VSAT terminal. We have also found various artifacts confirming this. While the Modaberan report states only Pooler servers are using VSAT, we have artifacts mentioning and operating VSAT terminals related to gas stations. VSAT comms, by nature, are insecure and can be compared to an open Wi-Fi hotspot, except an entire continent can snoop on your data. That’s why VPNs at layer 2/3 of the network are usually part of VSAT connections. In the case of this system, we uncovered artifacts that confirmed automatic VPN connection during the boot process of the IPC server based on the IKE protocol. So the chance of intercepting and decrypting data, unless VPN credentials and encryption keys are compromised by other means, is unlikely. However, we cannot eliminate this possibility as attackers with insider access could have obtained VPN credentials from any IPC server. We should also consider the

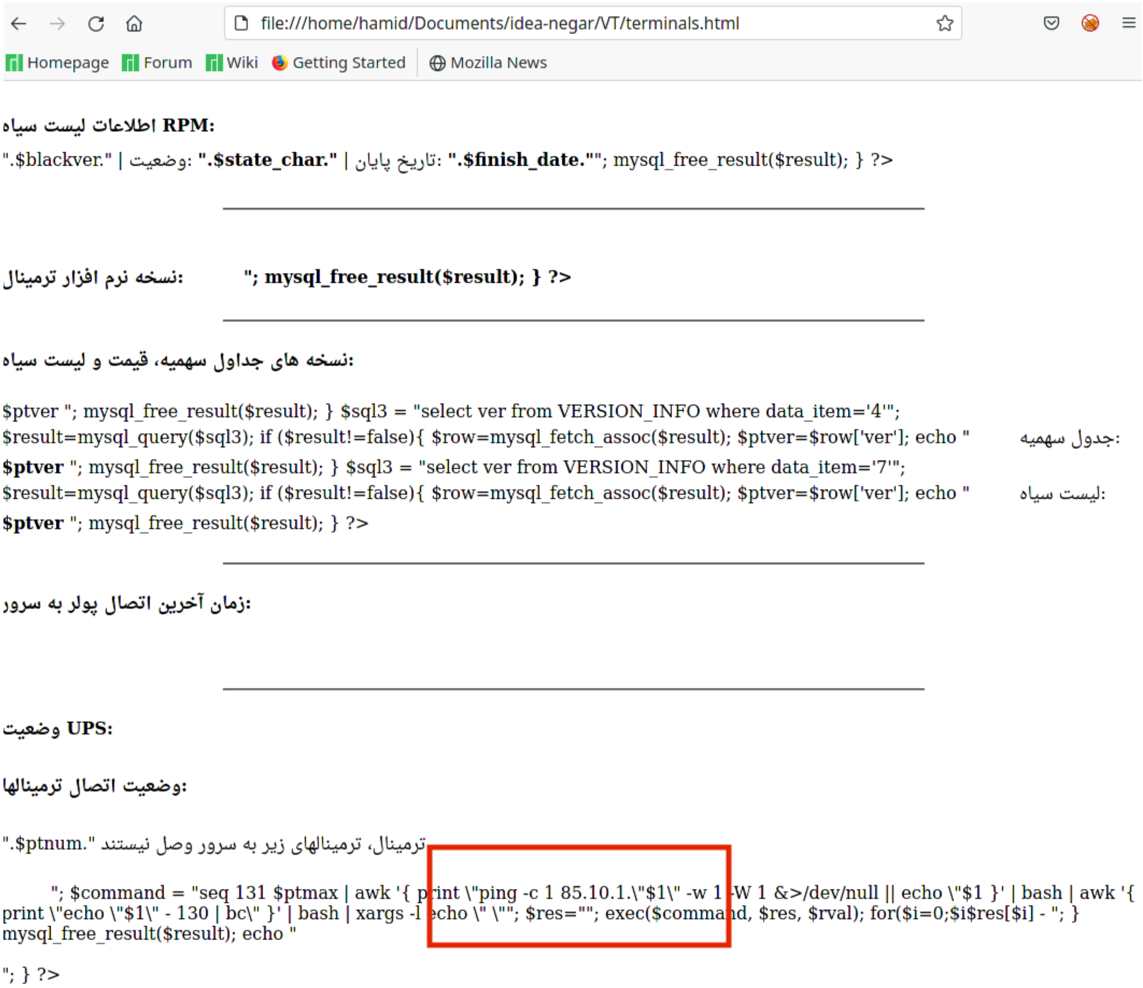
SIGINT capabilities of nation-states, as we have previously observed the possibility of backdooring encryption implementations. It is doubtful and far-fetched to assume such effort was used in this case. Even if we assume the VPN connection is not compromised, VSAT comms are still exposed to other attacks. An attacker with moderate experience and off-the-shelf equipment can still hijack and spoof VSAT terminals, effectively placing themselves “inside” the network perimeter. Such attacks require a few basic dependencies but are well within the capabilities of any moderately skilled threat actor or intelligence agency.

- **VSAT Terminals:** VSAT terminals work very similarly to any router supplied or sold to home users by internet providers. The same type of vulnerabilities also affect them, which are relatively easy to find and exploit. Not all VSAT terminals and their management (Web, SSH) interfaces are exposed over the Internet. Larger customers often use internal IP addresses not routable on the internet. However, this was not exactly the case with the smart fuel system. Bank-Mellat, the supplier in charge of providing and maintaining VSAT terminals (through a 3rd party private company named Yaas Arghavani), uses foreign satellite-based internet service providers and leases IPv4 blocks of addresses to be used by terminals. Since such VSAT customers constantly change and move and are not bound to specific countries or even regions, whois records of such IPv4 addresses are often anonymous and vague, only using specific code words to identify and mark them as VSAT clients. This makes it very challenging for an average user to connect the dots and identify the current owner of an IPv4 dedicated to a VSAT terminal. This is not a hard cloak to unmask for a determined threat actor or anyone with OSINT experience. Once IPv4 of a VSAT terminal is identified, attackers are one remote exploit away from gaining access to the network behind the terminal, in this case the smart fuel system and gas station systems. We were also able to identify artifacts revealing the usage of such terminals, identify a few internet-exposed router management interfaces, and confirm, with moderate confidence, several live router devices within the identified IPv4 blocks.

  While we could not go further than that passively for confirmation, chances of our findings being wrong are quite low when we have:

  - Found forensic artifacts (memory dump) directly related to the incident
  - Which contained source-code of management systems developed by Idea-negar
  - That is clearly labeled to monitor and accessibility of VSAT terminals
  - And the hardcoded IPv4 block in the code is also internet routable*
  - And a satellite internet provider company also owns the IPv4 block
  - And there are matching live IPs responding to ICMP in the block
  - And they happen to expose certain manufacturer modems web interfaces

  ***** We cannot eliminate the possibility that observer IPv4 addresses belong to an internal network and what we have observed is a striking match and similarity but not necessarily correct observation.



اطلاعات لیست سیاه RPM:

".$blackver." | وضعیت: **".$state_char."** | تاریخ پایان: **".$finish_date.""**; mysql_free_result($result); } ?>

نسخه نرم افزار ترمینال: **"; mysql_free_result($result); } ?>**

نسخه های جداول سهمیه، قیمت و لیست سیاه:

$ptver "; mysql_free_result($result); } $sql3 = "select ver from VERSION_INFO where data_item='4'"; $result=mysql_query($sql3); if ($result!=false){ $row=mysql_fetch_assoc($result); $ptver=$row['ver']; echo " جدول سهمیه: **$ptver** "; mysql_free_result($result); } $sql3 = "select ver from VERSION_INFO where data_item='7'"; $result=mysql_query($sql3); if ($result!=false){ $row=mysql_fetch_assoc($result); $ptver=$row['ver']; echo " لیست سیاه: **$ptver** "; mysql_free_result($result); } ?>

زمان آخرین اتصال پولر به سرور:

وضعیت UPS:

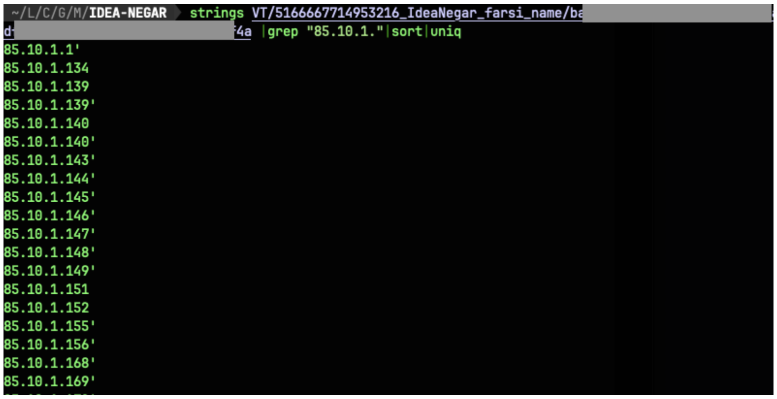
وضعیت اتصال ترمینالها:

".$ptnum." ترمینال، ترمینالهای زیر به سرور وصل نیستند

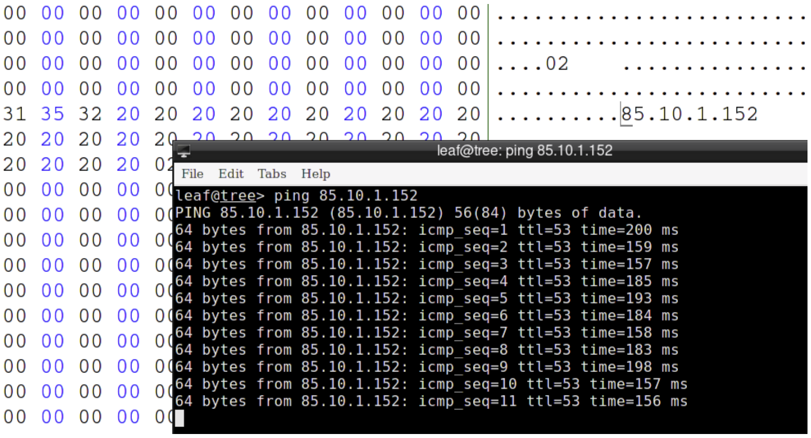
"; $command = "seq 131 $ptmax | awk '{ print \"ping -c 1 85.10.1.\"$1\" -w 1 -W 1 &>/dev/null || echo \"$1 }' | bash | awk '{ print \"echo \"$1\" - 130 | bc\" }' | bash | xargs -I echo \" \""; $res=""; exec($command, $res, $rval); for($i=0;$i$res[$i] - "; } mysql_free_result($result); echo "

"; } ?>

[Searching uploaded samples for VSAT connection artifacts]



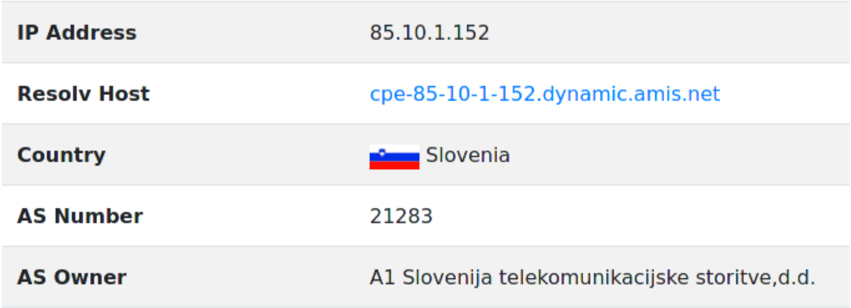
```
~/L/C/G/M/IDEA-NEGAR  strings VT/5166667714953216_IdeaNegar_farsi_name/ba[redacted]
d[redacted]f4a |grep "85.10.1."|sort|uniq
85.10.1.1'
85.10.1.134
85.10.1.139
85.10.1.139'
85.10.1.140
85.10.1.140'
85.10.1.143'
85.10.1.144'
85.10.1.145'
85.10.1.146'
85.10.1.147'
85.10.1.148'
85.10.1.149'
85.10.1.151
85.10.1.152
85.10.1.155'
85.10.1.156'
85.10.1.168'
85.10.1.169'
```



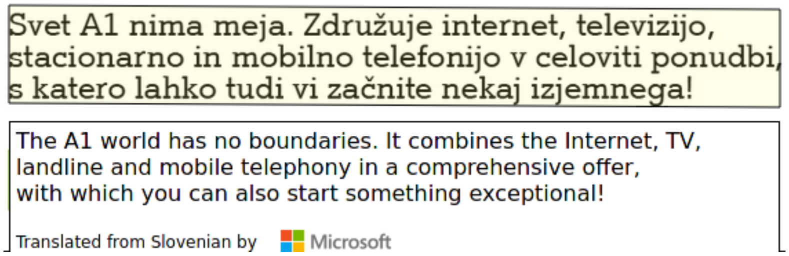
```
00 00 00 00 00 00 00 00 00 00 00 00 00 ........................
00 00 00 00 00 00 00 00 00 00 00 00 00 ........................
00 00 00 00 00 00 00 00 00 00 00 00 00 ....02    ...............
00 00 00 00 00 00 00 00 00 00 00 00 00 ........................
31 35 32 20 20 20 20 20 20 20 20 20 20 ..........85.10.1.152
20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 02
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
```

```
leaf@tree> ping 85.10.1.152
PING 85.10.1.152 (85.10.1.152) 56(84) bytes of data.
64 bytes from 85.10.1.152: icmp_seq=1 ttl=53 time=200 ms
64 bytes from 85.10.1.152: icmp_seq=2 ttl=53 time=159 ms
64 bytes from 85.10.1.152: icmp_seq=3 ttl=53 time=157 ms
64 bytes from 85.10.1.152: icmp_seq=4 ttl=53 time=185 ms
64 bytes from 85.10.1.152: icmp_seq=5 ttl=53 time=193 ms
64 bytes from 85.10.1.152: icmp_seq=6 ttl=53 time=184 ms
64 bytes from 85.10.1.152: icmp_seq=7 ttl=53 time=158 ms
64 bytes from 85.10.1.152: icmp_seq=8 ttl=53 time=183 ms
64 bytes from 85.10.1.152: icmp_seq=9 ttl=53 time=198 ms
64 bytes from 85.10.1.152: icmp_seq=10 ttl=53 time=157 ms
64 bytes from 85.10.1.152: icmp_seq=11 ttl=53 time=156 ms
```

[Live (VSAT) IP addresses recovered from uploaded artifacts]



IP Address	85.10.1.152
Resolv Host	cpe-85-10-1-152.dynamic.amis.net
Country	🇸🇮 Slovenia
AS Number	21283
AS Owner	A1 Slovenija telekomunikacijske storitve,d.d.



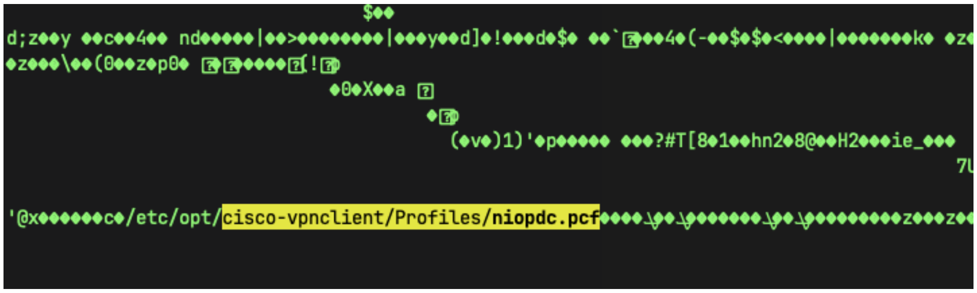
Svet A1 nima meja. Združuje internet, televizijo, stacionarno in mobilno telefonijo v celoviti ponudbi, s katero lahko tudi vi začnite nekaj izjemnega!

The A1 world has no boundaries. It combines the Internet, TV, landline and mobile telephony in a comprehensive offer, with which you can also start something exceptional!

[The A1 region is noted by the ISP to be allocated to customers with no fixed location (VSAT)]

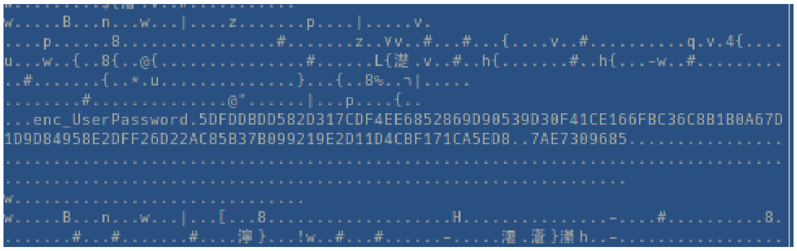
- **LTE Terminals:** We learned from multiple anonymous sources about using LTE modems and MCI-supplied SIM cards to provide internet access to gas stations and the IPC server to connect (via VPN) to data-center VPN servers. LTE/GPRS modems and CPEs, similar to any other consumer modem/routers, are prone to remotely exploitable vulnerabilities when their management interfaces and protocols are exposed over the internet. In the case of LTE CPEs, this is even more common due to how CPEs are remotely configured by service providers. We will not go through common attacks against various management protocols here, but the chances of identifying and exploiting a CPE used by a gas station cannot be underestimated. However, we could not identify any forensic artifacts in obtained dumps and data that would indicate remote management or monitoring of CPE terminals via the management interfaces in the smart fuel system web application.

- **Data Center VPN Servers:** We have previously explored the (very likely and nearly confirmed) possibilities of gas stations calling back home to the management data center through VPN. Naturally, this VPN server must also be exposed over the internet. We have seen enough remotely exploitable vulnerabilities in commercial VPN appliances in recent years that would spare us from explaining how this attack scenario could have continued. We have uncovered Cisco VPN configuration profiles and even managed to recover some connection credentials' clear-text passwords. An insider attacker with temporary access to any IPC server could have obtained the same information, too.



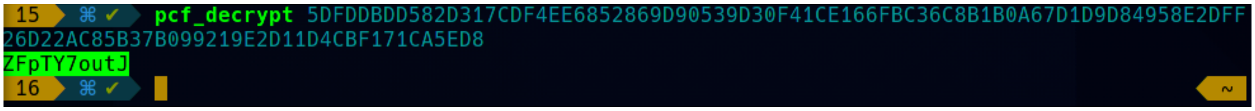
```
                                $◆◆
d;z◆◆y ◆◆c◆◆4◆◆ nd◆◆◆◆◆|◆◆>◆◆◆◆◆◆◆◆|◆◆◆y◆◆d]◆!◆◆◆d◆$◆ ◆◆`⍰◆◆4◆(-◆◆$◆$◆<◆◆◆◆|◆◆◆◆◆◆◆k◆ ◆z◆
◆z◆◆◆\◆◆(0◆◆z◆p0◆ ⍰⍰◆◆◆◆⍰(!⍰
                              ◆0◆X◆◆a ⍰
                                         ◆⍰
                                           (◆v◆)1)'◆p◆◆◆◆◆ ◆◆◆?#T[8◆1◆◆hn2◆8@◆◆H2◆◆◆ie_◆◆◆
                                                                                        7U

'@x◆◆◆◆◆◆c◆/etc/opt/cisco-vpnclient/Profiles/niopdc.pcf◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆z◆◆◆z◆◆
```

Cisco VPN client artifacts found in uploaded samples



```
w.....B...n...w...|....z.......p....|.....v.
....p......8................#........z..Yv..#...#...{....v..#..........q.v.4{....
u...w..{..8{..@{................#.......L{澁.v..#..h{.......#..h{...-w..#.........
..#.......{..*.u...............}...{..8%..¬|.....
.........#..............@".......|...p....{..
...enc_UserPassword.5DFDDBDD582D317CDF4EE6852869D90539D30F41CE166FBC36C8B1B0A67D
1D9D84958E2DFF26D22AC85B37B099219E2D11D4CBF171CA5ED8..7AE7309685................
................................................................................
................................................................
w..............................
w.....B...n...w...|...[...8....................H..............-....#..........8.
.......#...#.......#....瀰}...!w..#...#......-.....瀝.瀟}瀟h..-.................
```

[Cisco VPN credentials recovered from uploaded samples]



```
15 ⌘ ✓ pcf_decrypt 5DFDDBDD582D317CDF4EE6852869D90539D30F41CE166FBC36C8B1B0A67D1D9D84958E2DFF
26D22AC85B37B099219E2D11D4CBF171CA5ED8
ZFpTY7outJ
16 ⌘ ✓                                                                                  ~
```

[Decryption of obtained Cisco credentials]

- **Physical Access to IPC Servers:** An attacker with physical access, even temporary and short term, to a single IPC server in any gas station across the country could have easily dumped various sensitive information (such as VPN credentials) from the server or install a software/hardware implant for persistence access to the IPC server and the smart fuel system network as the result of that. Gas stations, especially at remote locations, are not a difficult target to physically compromise and are lightly guarded (if at all).
- **Physical Access to station network:** IPC servers at gas stations, as mentioned before, are connecting to the data center using VPN connections established on the IPC server, But this server is still exposed and accessible within the internal network of the gas station, or at least to the VSAT/LTE/Other modems that are connecting it to the internet or the MPLS network of the fuel system. Considering the operating system version used

for the IPC server, Fedora 12, which has been EoL (End of Life) since December 2010, we can assume it would not be a hard target to compromise over the network.

- **Insider Attack:** Insider attacks are the most speculated and also favorite of some nation states when it comes to such attacks. While domestic sources in Iran speculate about the involvement of technical insider attackers responsible for this incident, we believe that, in reality, an insider attack could have been as basic as bribing or convincing a gas station operator into giving temporary access to the server or network, long enough for attackers to gain persistence on one of the systems. While the design and management of the system might look complex, it is not something that any determined and experienced attacker cannot figure out independently by reviewing the manufacturer's technical documents and user manuals (Ingenico). The involvement of high-level technical operators of the system would not have been necessary by any means. We do not believe Insider Attacks have been the source of the incident here.
- **The Government-Network (Shabake-Dolat):** Almost all government organizations and national entities in Iran are interconnected using a domestic and dedicated network infrastructure, which operates independently from the infrastructure used to deliver internet connections nationwide. Government entities use this network to exchange information, interact with exposed APIs by each entity, and have a secure medium to interconnect them overall. A few elements of the smart fuel system are also exposed over this network, as confirmed by two independent sources.

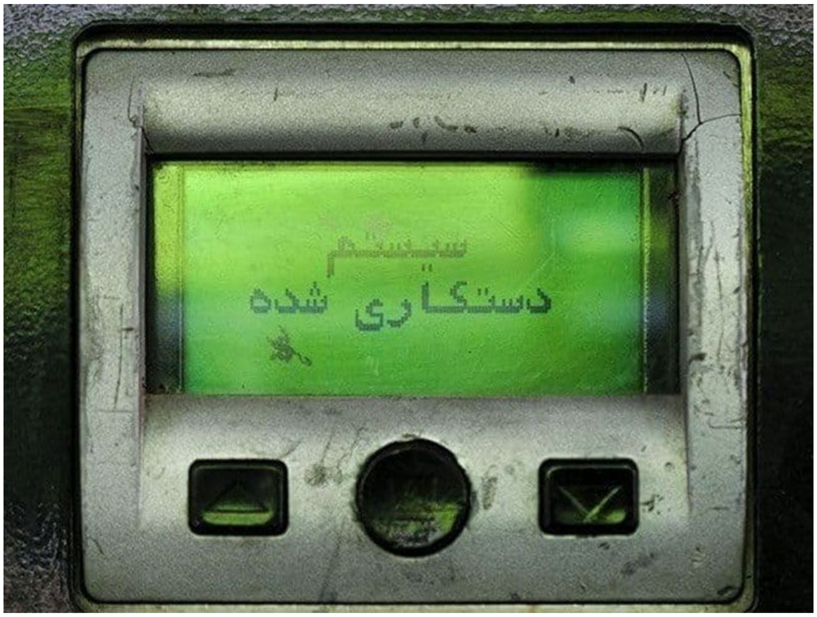
  The same sources also mentioned the compromise of the tech-support server (which exposes a web application) and the discovery of a web-shell backdoor on this system. We could not independently confirm this, find traces of such a backdoor in leaked dumps, or find the web shell among the cluster of uploads related to this incident. What we were able to observe, however, was that the same submitters, in matching time-frames, uploaded various (supposedly malicious) Bash scripts for scan, that have been previously attributed to MeteorExpress and other attacks. We also observed at least one binary, a signed and vulnerable Windows driver, observed in previous incidents and used by MeteroExpress to access kernel space.

Recently, an Iranian company (AmnPardaz) revealed an interesting new malware, the first of its kind documented publicly, that would infect and persist in HP iLO firmware on servers used by unnamed Iranian networks. The company mentions that the first sample and related incident was identified in 2020, dating long before the attack against gas stations but closer to when similar incidents happened against the Railways and Ports and Marines organizations. Attacks against HP iLO or similar solutions from other vendors are not new and have been explored in depth before. However, this is the first publicly known example of exploitation and implant deployment based on them. Padvish has not released any malware samples, but based on their technical analysis report, we can highlight two important notes about the case. Wiping the hard disk of servers is a main feature of this implant and likely how the malware was initially spotted in the wild. The second noteworthy point is the attempt by implant developers to survive iLO firmware updates by faking a successful upgrade while preserving the old version and persistence. While the Amnpardaz report considers this an advanced and sophisticated implant deployed with a long persistence goal, the fact that it attempts to wipe the server disk for sabotage continuously is contradictory to that and makes the characteristics of the implant closer to a wiper malware more sophisticated than typical Operating System level infections and more challenging to clean up and recover from. This aligns with cases where the goal is to prolong damage and downtime against a target. The second interesting point is how this malware persists and survives firmware upgrades. The malware tampers with the original upgrade process and prevents it from happening while showing all the expected logs and messages displayed to the user during the process. This is indeed a neat behavior by malware, but as the report highlights, the malware fails to use an up-to-date HP iLO welcome message image once a fake upgrade has finished. The malware displays an outdated vendor image to the user while the software claims to be current. An implant designed and meant for long-term persistence would try to update and keep up with such changes, while in this case, it seems to be left alone for a long period (since HP has changed the iLO welcome screen) and unmaintained by attackers.

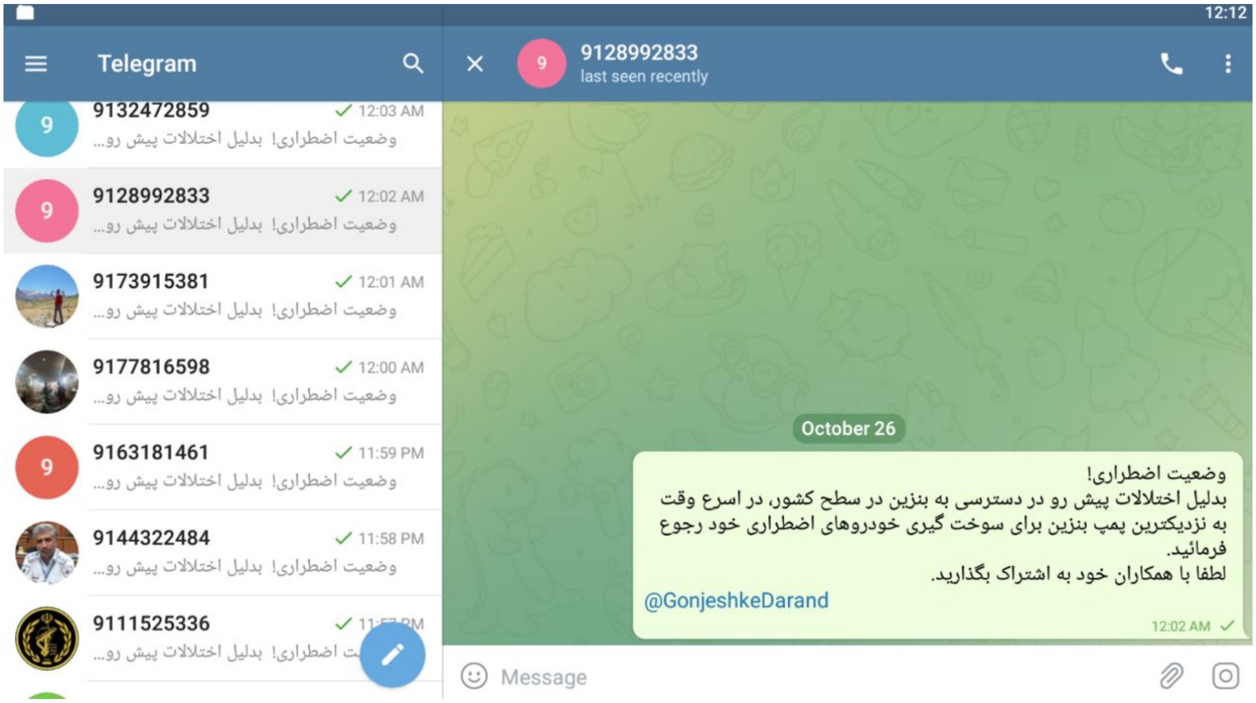
What makes this newly uncovered malware interesting and likely relevant to previous sabotage attempts and the gas station attack incident is its wiper capability, behavior, and timing of deployment and usage. It is unclear whether the malware sample was found while investigating these attacks. Still, it should be considered a potential persistence and lateral movement method in Shabake-Dolat.

The Incident:

On October 26th 2021, around 11:00 AM local time in Tehran, nearly all of 4300 gas stations across the country started going out of service. Within about two hours, every POS device of every gas station goes offline and into an irreversible state, effectively bricked. Random POS devices (the exact number is unknown) remain powered on but are out of service. Instead of the usual message, “Cyber Attack 64411” was shown on the POS display in Farsi. The infamous 64411 number, already known to us, is the phone number of the supreme leader's office, which was also used as part of the **message** delivered during previous cyber attacks.



This happened a few hours after the attackers sent a warning message to a selected group of individuals through Telegram, likely chosen based on their positions and responsibilities involving emergency services, ambulances, and fire bridge stations. The message warns these individuals to be prepared for an upcoming and expected outage of gas distribution and to refuel their vehicles as soon as possible in a nearby gas station before the outage occurs. The attackers planned and sent this warning to avoid or minimize potential life-threatening downtime of emergency service vehicles due to the attack and lack of fuel to keep them operational.



9132472859 ✓ 12:03 AM
وضعیت اضطراری! بدلیل اختلالات پیش رو...

9128992833 ✓ 12:02 AM
وضعیت اضطراری! بدلیل اختلالات پیش رو...

9173915381 ✓ 12:01 AM
وضعیت اضطراری! بدلیل اختلالات پیش رو...

9177816598 ✓ 12:00 AM
وضعیت اضطراری! بدلیل اختلالات پیش رو...

9163181461 ✓ 11:59 PM
وضعیت اضطراری! بدلیل اختلالات پیش رو...

9144322484 ✓ 11:58 PM
وضعیت اضطراری! بدلیل اختلالات پیش رو...

9111525336 ✓ 11:57 PM
وضعیت اضطراری! بدلیل اختلالات پیش رو...

October 26

وضعیت اضطراری!
بدلیل اختلالات پیش رو در دسترسی به بنزین در سطح کشور، در اسرع وقت
به نزدیکترین پمپ بنزین برای سوخت گیری خودروهای اضطراری خود رجوع
فرمائید.
لطفا با همکاران خود به اشتراک بگذارید.
@GonjeshkeDarand
12:02 AM ✓

[Predatory Sparrow early warning message before launching their attack.]

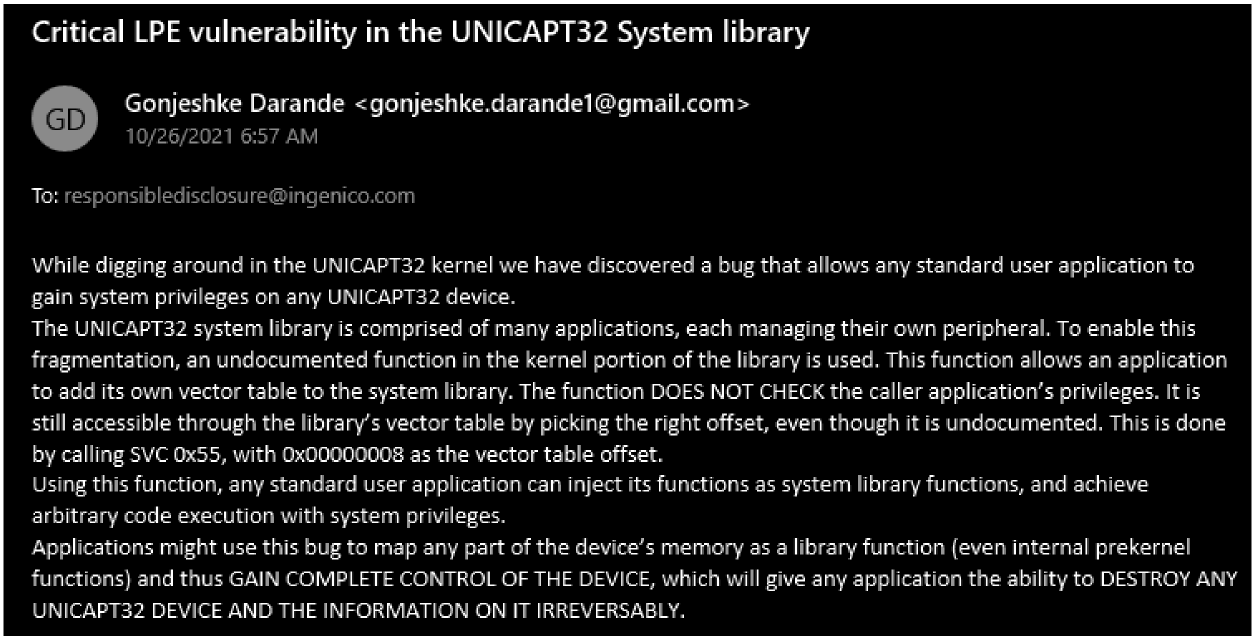
Within two hours from the first reported POS outage, the entire network collapsed, and most gas station terminals were bricked. Bricking a POS is not as simple as wiping a regular workstation. A corrupted image or flash command must be issued to all of them to brick them. Due to the standard security architecture and management model of payment POS terminals, flashing them, or any configuration update, must come through the legitimate remote management channel and be digitally signed. A configuration update was pushed to some of them to show a custom message on POS LCD screens, which means the management infrastructure for POS terminals in the data center was fully compromised. The only other scenario in which attackers could have pushed configurations and signed firmware images (with malicious data) to POS devices is if they have compromised the vendor's signing keys. This is much less likely to be the case and would be catastrophic for Ingenico, too, not just their Iranian customers. We failed to identify a corrupted or tampered POS firmware image used to brick the device among obtained artifacts and data. Without such an image or a postmortem flash dump from a bricked POS device, we can only assume that attackers used malicious commands and potential vulnerabilities in the POS firmware to sabotage the terminal and likely corrupt the bootable image on POS flash memory. Attackers have already mentioned in their public announcements finding at least two vulnerabilities in Ingenico products and exploiting at least one to perform their attack to sabotage them.

While the threat actor briefly mentioned a second and more critical vulnerability in Ingenico products, they never publicly released any technical details. The Sparrows claimed to have reported the details of the issue to Ingenico instead. In an interesting turn of events, as we reached out to them, Predatory Sparrows provided us with a copy of the email they sent to Ingenico containing details of the second vulnerability. We contacted Ingenico for confirmation and whether they have acted on and remediated the reported issue but have not received any response.

The reported issue mentions a privilege escalation vulnerability in the UNICAPT32 kernel (an SoC used in a wide range of Ingenico products), which would allow attackers to gain arbitrary read/write access to memory and bypass the restrictions in place to overwrite protected memory areas of the UNICAPT32 SoC. Exploiting this vulnerability requires existing unprivileged access to the POS as an application. Attackers already had such access, as they could push arbitrary configurations or applications over the network using the management tools. We have not attempted to examine and confirm the reported vulnerability independently.

[Updated January 13th, 2022]: We tried reaching out to Ingenico through their official contact for responsible disclosure of security issues on 13th January 2021, hoping to get a confirmation and approval before disclosing the details of the issue, but we have not received any updates since their initial response.

[Updated Jan 30, 2022]: Initially, Ingenico did not respond. After another follow-up, on January 20th, 2022 they requested withholding publishing details until February 4th, when they would return with more details. Communications went cold since then. After another follow-up, on January 20th, they requested withholding publishing details until February 4th, when they would return with more details. Communications went cold since then.
Below is a screenshot of the email originally sent to Ingenico by Predatory Sparrow and later shared with us by them.



Critical LPE vulnerability in the UNICAPT32 System library

GD

Gonjeshke Darande <gonjeshke.darande1@gmail.com>
10/26/2021 6:57 AM

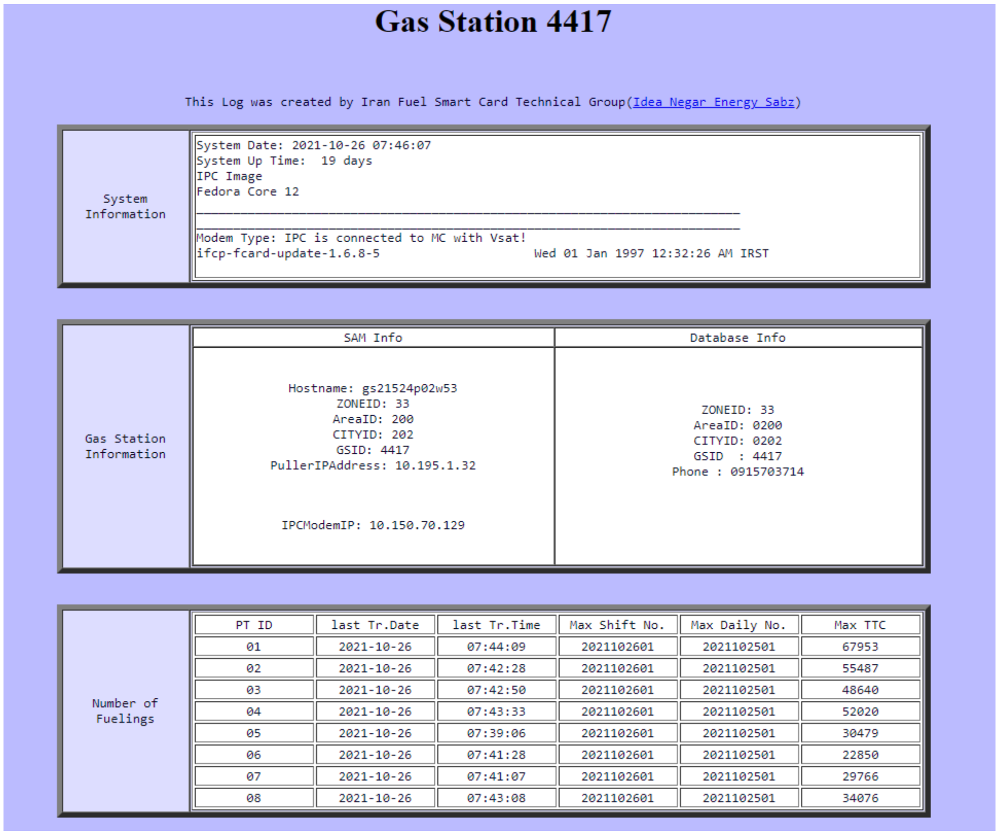
To: responsibledisclosure@ingenico.com

While digging around in the UNICAPT32 kernel we have discovered a bug that allows any standard user application to gain system privileges on any UNICAPT32 device.
The UNICAPT32 system library is comprised of many applications, each managing their own peripheral. To enable this fragmentation, an undocumented function in the kernel portion of the library is used. This function allows an application to add its own vector table to the system library. The function DOES NOT CHECK the caller application's privileges. It is still accessible through the library's vector table by picking the right offset, even though it is undocumented. This is done by calling SVC 0x55, with 0x00000008 as the vector table offset.
Using this function, any standard user application can inject its functions as system library functions, and achieve arbitrary code execution with system privileges.
Applications might use this bug to map any part of the device's memory as a library function (even internal prekernel functions) and thus GAIN COMPLETE CONTROL OF THE DEVICE, which will give any application the ability to DESTROY ANY UNICAPT32 DEVICE AND THE INFORMATION ON IT IRREVERSABLY.

[Predatory Sparrow email to Ingenico, disclosing vulnerability details]

Back to the incident, the attackers did not stop there. Once POS terminals were sabotaged and IPC servers no longer needed to deliver updates to terminals, IPC servers were also wiped out. This was likely to make the disaster recovery annoying enough to demand the physical presence of technicians on-site at every gas station and prevent online remote repair, but not too catastrophic to cause long-term and permanent damage to the infrastructure. The wiping of IPC servers (the scale and number of wiped systems are unknown to us) indicates that attackers have full access to the infrastructure.

As we learned later during the analysis of obtained data, the central system provides a web interface for management and monitoring. This interface, among other things, also monitors and interacts with Pooler and IPC servers, POS terminals, and even VSAT terminals or modems at every gas station. **As briefly reviewed earlier in this post, some of these connection points effectively expose the infrastructure over the internet and contradict Iranian officials' claims about the system operating on a completely isolated network**. Reviewing the source code of some of these components revealed interesting details about how (insecurely) this infrastructure operates and creates multiple points of complete failure and compromise due to vulnerable design decisions. For example, PHP scripts implementing some monitoring features deliver OS commands on various components to obtain information or interact with locally connected external devices such as VSAT terminals through USB or Serial interface or sending AT commands to them.



Gas Station 4417

This Log was created by Iran Fuel Smart Card Technical Group(Idea Negar Energy Sabz)

System Information

```
System Date: 2021-10-26 07:46:07
System Up Time:  19 days
IPC Image
Fedora Core 12
_______________________________________________________________________
_______________________________________________________________________
Modem Type: IPC is connected to MC with Vsat!
ifcp-fcard-update-1.6.8-5                    Wed 01 Jan 1997 12:32:26 AM IRST
```

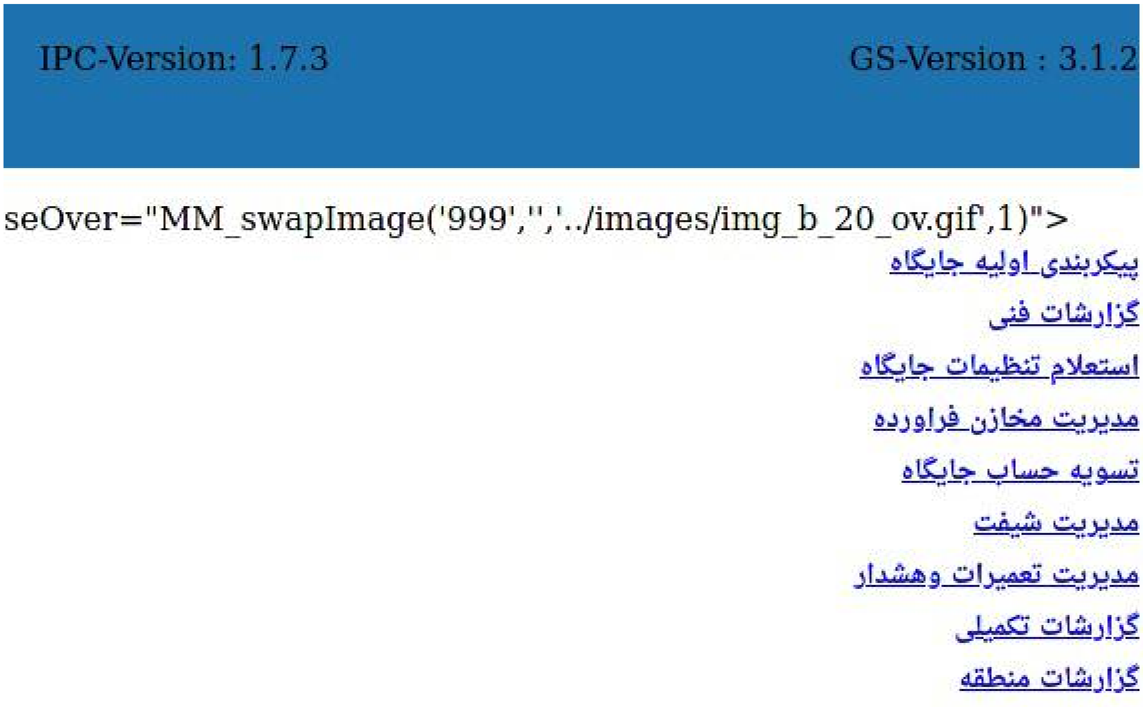
Gas Station Information

SAM Info	Database Info
Hostname: gs21524p02w53 ZONEID: 33 AreaID: 200 CITYID: 202 GSID: 4417 PullerIPAddress: 10.195.1.32 IPCModemIP: 10.150.70.129	ZONEID: 33 AreaID: 0200 CITYID: 0202 GSID : 4417 Phone : 0915703714

Number of Fuelings

PT ID	last Tr.Date	last Tr.Time	Max Shift No.	Max Daily No.	Max TTC
01	2021-10-26	07:44:09	2021102601	2021102501	67953
02	2021-10-26	07:42:28	2021102601	2021102501	55487
03	2021-10-26	07:42:50	2021102601	2021102501	48640
04	2021-10-26	07:43:33	2021102601	2021102501	52020
05	2021-10-26	07:39:06	2021102601	2021102501	30479
06	2021-10-26	07:41:28	2021102601	2021102501	22850
07	2021-10-26	07:41:07	2021102601	2021102501	29766
08	2021-10-26	07:43:08	2021102601	2021102501	34076

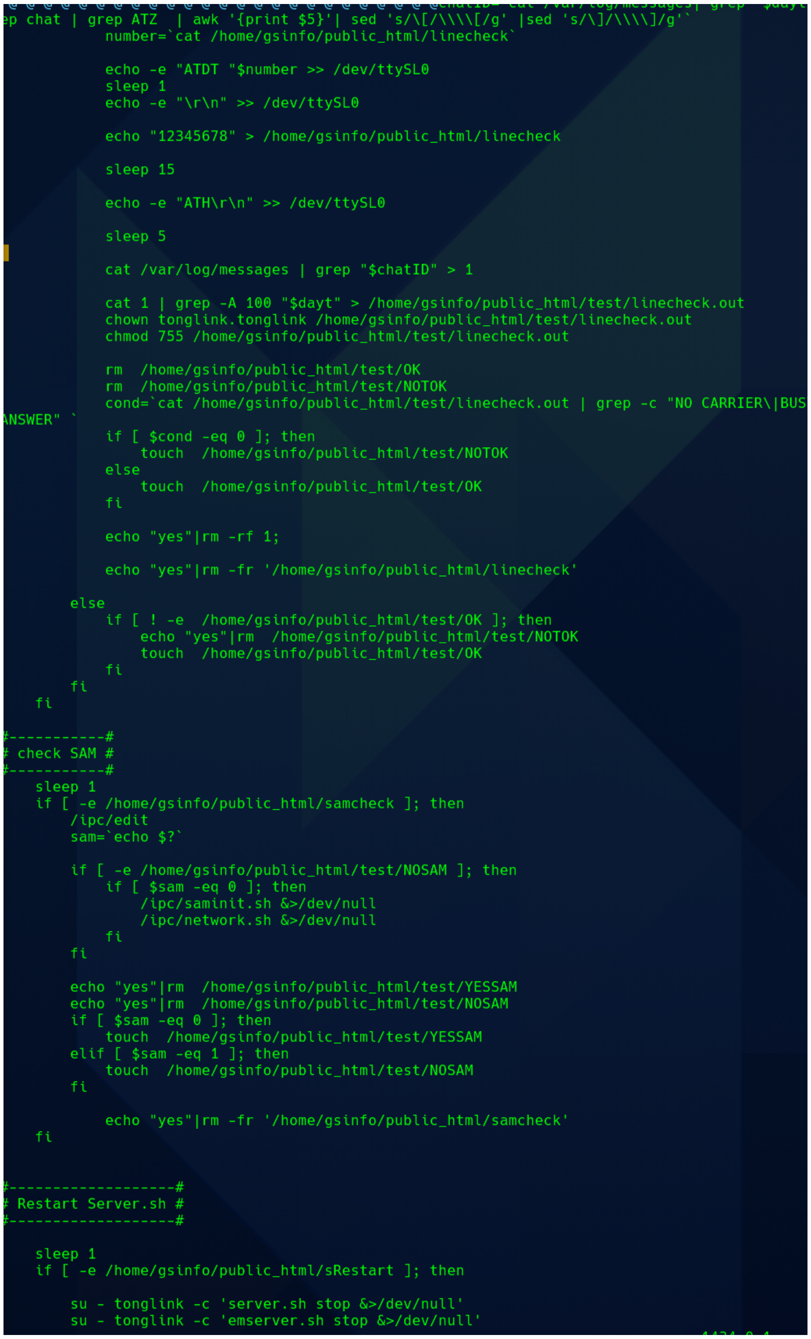
[Screenshot of Web UI of the management system, provided by Predatory Sparrows]



IPC-Version: 1.7.3 GS-Version : 3.1.2

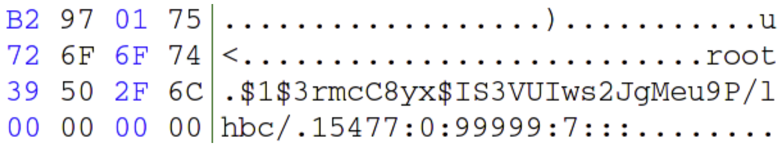
```
seOver="MM_swapImage('999','','../images/img_b_20_ov.gif',1)">
```

[Reconstructed management Web UI from uploaded artifacts]



```
ep chat | grep ATZ  | awk '{print $5}'| sed 's/\[/\\\\[/g' |sed 's/\]/\\\\]/g'`
            number=`cat /home/gsinfo/public_html/linecheck`

            echo -e "ATDT "$number >> /dev/ttySL0
            sleep 1
            echo -e "\r\n" >> /dev/ttySL0

            echo "12345678" > /home/gsinfo/public_html/linecheck

            sleep 15

            echo -e "ATH\r\n" >> /dev/ttySL0

            sleep 5

            cat /var/log/messages | grep "$chatID" > 1

            cat 1 | grep -A 100 "$dayt" > /home/gsinfo/public_html/test/linecheck.out
            chown tonglink.tonglink /home/gsinfo/public_html/test/linecheck.out
            chmod 755 /home/gsinfo/public_html/test/linecheck.out

            rm  /home/gsinfo/public_html/test/OK
            rm  /home/gsinfo/public_html/test/NOTOK
            cond=`cat /home/gsinfo/public_html/test/linecheck.out | grep -c "NO CARRIER\|BUS
ANSWER" `

            if [ $cond -eq 0 ]; then
                touch  /home/gsinfo/public_html/test/NOTOK
            else
                touch  /home/gsinfo/public_html/test/OK
            fi

            echo "yes"|rm -rf 1;

            echo "yes"|rm -fr '/home/gsinfo/public_html/linecheck'

        else
            if [ ! -e  /home/gsinfo/public_html/test/OK ]; then
                echo "yes"|rm  /home/gsinfo/public_html/test/NOTOK
                touch  /home/gsinfo/public_html/test/OK
            fi
        fi
    fi

#-----------#
# check SAM #
#-----------#
    sleep 1
    if [ -e /home/gsinfo/public_html/samcheck ]; then
        /ipc/edit
        sam=`echo $?`

        if [ -e /home/gsinfo/public_html/test/NOSAM ]; then
            if [ $sam -eq 0 ]; then
                /ipc/saminit.sh &>/dev/null
                /ipc/network.sh &>/dev/null
            fi
        fi

        echo "yes"|rm  /home/gsinfo/public_html/test/YESSAM
        echo "yes"|rm  /home/gsinfo/public_html/test/NOSAM
        if [ $sam -eq 0 ]; then
            touch  /home/gsinfo/public_html/test/YESSAM
        elif [ $sam -eq 1 ]; then
            touch  /home/gsinfo/public_html/test/NOSAM
        fi

            echo "yes"|rm -fr '/home/gsinfo/public_html/samcheck'
    fi


#------------------#
# Restart Server.sh #
#------------------#

    sleep 1
    if [ -e /home/gsinfo/public_html/sRestart ]; then

        su - tonglink -c 'server.sh stop &>/dev/null'
        su - tonglink -c 'emserver.sh stop &>/dev/null'
```

[Management shell scripts recovered from uploaded artifacts]



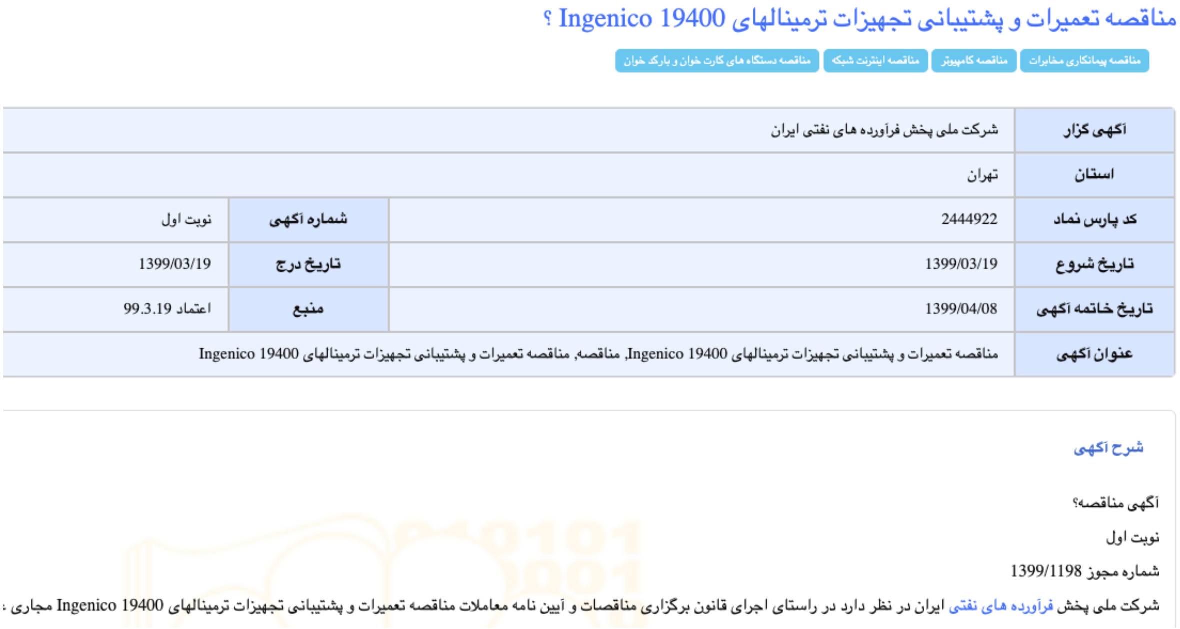
```
B2 97 01 75|...................)...........u
72 6F 6F 74|<...........................root
39 50 2F 6C|.$1$3rmcC8yx$IS3VUIws2JgMeu9P/l
00 00 00 00|hbc/.15477:0:99999:7:::.........
```

[Servers root password hashes recovered from uploaded artifacts]

Almost every identified software component and library in the system's design, from which we could review or obtain version information, was also outdated and sometimes vulnerable to various security issues. While the average audience of news might assume such systems and critical infrastructure of this scale would be closely monitored and securely maintained to meet the latest security standards, the reality is widespread usage of obsolete software is a widespread practice.

OSINT & Initial Footprints:

Soon after the news about the incident broke out, we tried to identify potential attack vectors that attackers could have used. To understand that, we had to learn about who and what operates the system. That became the initial step: figuring out the "who." The National Iranian Oil Products Distribution Company (NIOPDC) occasionally publishes RFPs to outsource maintenance and bulk sales or purchases. Such RFPs are legal requirements and need to be published in official newspapers, and of course, online repositories exist to archive them. PARS NAMAD DATA website is one of such archives, and indeed, combining a few keywords quickly turned up interesting RFPs that answered both the "who" and "what" questions. So now we know Ingenico products are in use at the gas stations. The RFP states "Ingenico 19400", which later turned out to be a typo lost in translation and should have been "i9400".



مناقصه تعمیرات و پشتیبانی تجهیزات ترمینالهای Ingenico 19400 ؟

آگهی گزار	شرکت ملی پخش فرآورده های نفتی ایران		
استان	تهران		
کد پارس نماد	2444922	شماره آگهی	نوبت اول
تاریخ شروع	1399/03/19	تاریخ درج	1399/03/19
تاریخ خاتمه آگهی	1399/04/08	منبع	اعتماد 99.3.19
عنوان آگهی	مناقصه تعمیرات و پشتیبانی تجهیزات ترمینالهای Ingenico 19400, مناقصه, مناقصه تعمیرات و پشتیبانی تجهیزات ترمینالهای Ingenico 19400		

شرح آگهی

آگهی مناقصه؟

نوبت اول

شماره مجوز 1399/1198

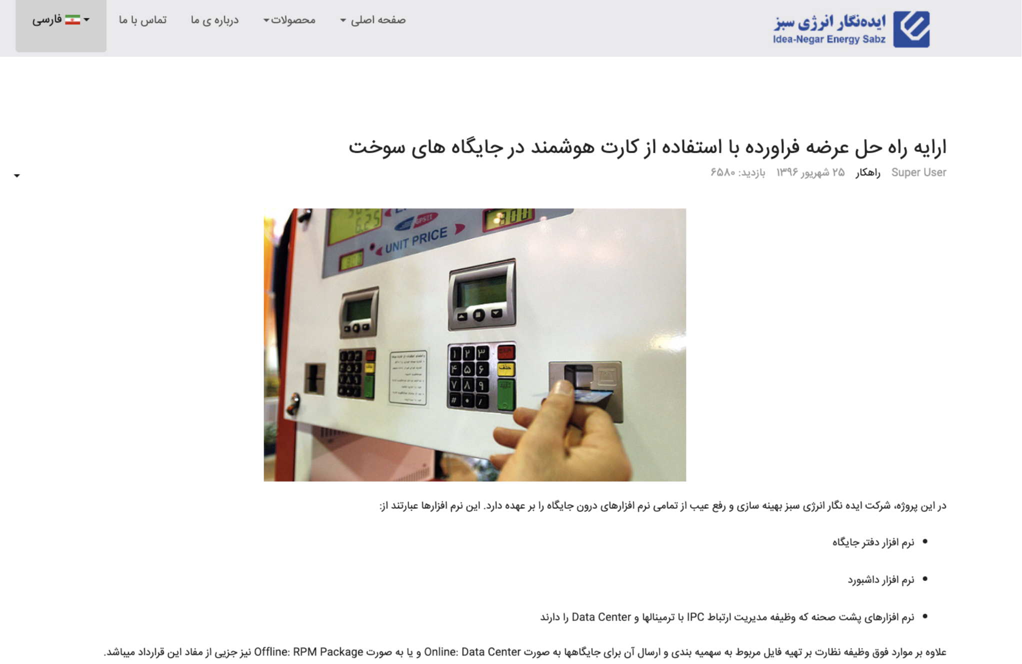
شرکت ملی پخش فرآورده های نفتی ایران در نظر دارد در راستای اجرای قانون برگزاری مناقصات و آیین نامه معاملات مناقصه تعمیرات و پشتیبانی تجهیزات ترمینالهای Ingenico 19400 مجاری

[RFP for technical support of Ingenico products by NIOPDC]

This finding also aligned with some information published online around the same time on Twitter. Posted images, however, lacked any usable details like FCC numbers or serial numbers. The only visible and useful information was the brand name and physical packaging of the board. We could still learn a lot about the architecture of Ingenico products by looking up relevant models, their user manuals, and even board and packaging visual details from relevant FCCs filed by Ingenico.

Among multiple related RFPs, we identified the entity responsible for handling VSAT services for the smart fuel system, a subsidiary company under Bank Mellat. The same method can be used to identify pretty much any supplier related to the fuel distribution project and companies that are or were involved in or Ôprovide technical and maintenance support for the project.

We also assumed the first respondents to the incident might have been NIOPDC engineers. It is not uncommon for people not professionally trained in forensics investigations to submit suspicious files and samples to online services such as VirusTotal or other alternatives. Therefore, we tried to narrow down recent uploads to such services from Iran and also from identified IPv4 CIDRs registered to NIOC and NIOPDC. No luck at the first shot, but we did not give up. Going back one step, we tried to identify more entities in charge of the maintenance or implementation of the system. Naturally, knowing the Ingenico brand in use, we tried to identify Iranian companies involved in importing, maintaining, or re-branding their products. It took only a few minutes to come across Idea-Negar company, claiming to produce products based on Ingenico products for handling payment and management of fueling stations.



ارایه راه حل عرضه فراورده با استفاده از کارت هوشمند در جایگاه های سوخت

Super User راهکار ۲۵ شهریور ۱۳۹۶ بازدید: ۶۵۸۰

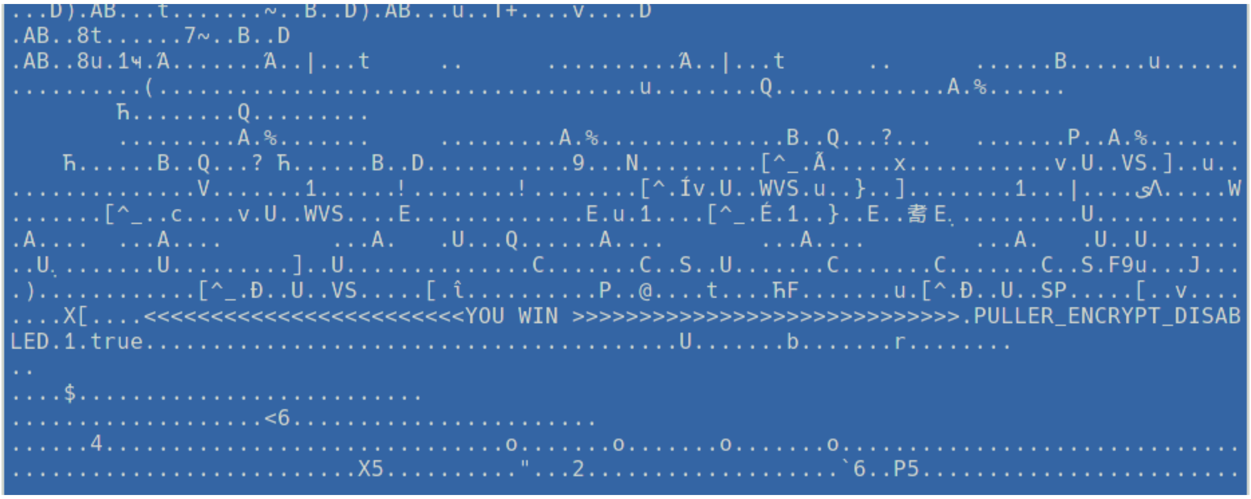
در این پروژه، شرکت ایده نگار انرژی سبز بهینه سازی و رفع عیب از تمامی نرم افزارهای درون جایگاه را بر عهده دارد. این نرم افزارها عبارتند از:

- نرم افزار دفتر جایگاه
- نرم افزار داشبورد
- نرم افزارهای پشت صحنه که وظیفه مدیریت ارتباط IPC با ترمینالها و Data Center را دارند

علاوه بر موارد فوق وظیفه نظارت بر تهیه فایل مربوط به سهمیه بندی و ارسال آن برای جایگاهها به صورت Online: Data Center و یا به صورت Offline: RPM Package نیز جزیی از مفاد این قرارداد میباشد.

Idea-Negar.com content about their fuel distribution system project

We had the what (Ingenico models) and the who (Idea-Negar). It was time to repeat our big data searches and walla! We had our first match among bulk submissions to VirusTotal.



```
...D).AB...t.......~..B..D).AB...u..I+....v....D
.AB..8t......7~..B..D
.AB..8u.1ч.Ά.......Ά..|...t      ..        ..........Ά..|...t      ..      ......B......u......
..........(....................................u........Q.............A.%......
        ħ........Q.........
        .........A.%.......     .........A.%.............B..Q...?...    .......P..A.%.......
    ħ......B..Q...? ħ......B..D...........9...N.........[^_.Ă.....x...........v.U..VS.]..u..
..............V.......1......!........!........[^.Ív.U..WVS.u..}..].........1...|....ى^.....W
.......[^_..c....v.U..WVS....E.............E.u.1....[^_.É.1..}..E..耈E̦.........U..........
.A....  ...A....        ...A.   .U...Q......A....        ...A....       ...A.   .U..U.......
..U̦.......U.........]..U..............C.......C..S..U.......C.......C.......C..S.F9u...J...
.)...........[^_.Đ..U..VS.....[.î.........P..@....t....ħF.......u.[^.Đ..U..SP.....[..v....
....X[....<<<<<<<<<<<<<<<<<<<<<<<<<YOU WIN >>>>>>>>>>>>>>>>>>>>>>>>>>>>>.PULLER_ENCRYPT_DISAB
LED.1.true........................................U.......b.......r........
..
....$.........................
...................<6.......................
......4...........................o.......o.......o.......o.............................
.........................X5.........."...2....................`6..P5......................
```

Following that trail and going through multiple iterations of search based on newly found binaries, strings, and meta-data led to the identification of multiple clusters of relevant binaries and submitters. We identified three major clusters and uploaders. Two uploaded most memory dumps from two geographic locations (or cloaked IP addresses). The third one has only uploaded a few specific shell scripts and (Windows) binaries, most of which can be attributed to previous attacks against Iranian targets.

The Leaks and 4th Party Collection:

What we started as and assumed to be a hunt for malware samples quickly became much more interesting. As the number and size of upload clusters grew, we started to go through them, mainly looking at strings and trying to make sense of binary data. It eventually hit us as we struggled and failed to properly restore, parse, and reverse some of these binaries as standard ELF or PE files in ARM or x86 format. **The individuals, company, or government entity in charge of the incident response and forensics of the case were loudly broadcasting their work to the world!** You just had to tune in to the right channel to watch them. We were not looking at randomly uploaded binaries. What we managed to cluster and download were actually segments of memory dumps from operational servers running the fuel distribution system! This was like asking for a can of Cocacola but receiving its secret formula instead! Our submitters somehow believe that their best course of action is to submit a large part of the live memory dump of the smart fuel system production servers, possibly acquired by the first respondents from the data center and gas station IPC servers.

By their nature, forensic investigations begin as need-to-know basis work until the scale of an attack or incident and potential data at risk are identified. This is done in an even more secrecy and controlled environment. The Iranian government often has no interest in releasing TTPs and IoCs when sensitive infrastructure or government-related entities are compromised. This is a common practice by them. Naturally, this is to protect the intellectual property and potentially sensitive data. Yet, in this incident, we observed a stream of closely guarded technical details and data dripping off the forensics investigators.

We identified the private company in charge of the forensics and the government entity that would likely be responsible for handling this and other similar incidents, AFTA. Their cat was already out of the basket, so we attempted to reach out to both entities, offering our insight and interest in obtaining more samples to make the process of identifying and clustering similar works of this new threat factor faster. Initially, both entities refused any comments and naturally denied even their involvement. After providing a few examples to them, communications went cold, and we gave up. Ironically, the stream of leaks did not stop! Perhaps we were not clear enough about our source of information.

How Confident Should We Be?

Considering the severity of this mistake and disclosure of dumps, if it has even been a mistake, we cannot rule out the possibility of an intentional leak by the attackers or an unknown third party masking their origin as Iran and France (where our submitters' uploaded data from). If so, it would not be the first time a threat actor would piggyback the operations of another group or even use their infrastructure to leak information under false personas or identities. The threat actors claiming the credit for this attack themselves seem to be hiding behind disposable personas. Based on the social media accounts from which their activities were published, they have at least two sets of accounts. For unclear reasons, if they are the same actors, they did not post about the gas station attack using the same Twitter account they originally used when they first emerged. The only point we can confidently confirm is that they are the group behind the gas station attack, as they privately provided us with some technical details and artifacts that could not be known to another group who would try to impersonate and Tweet under their persona. Whether this Gonjeshk-Darandeh is the same Gonjeshk-Darandeh that originally surfaced in the past would be challenging to confirm.

Obtained dumps have another interesting and questionable property. While the uploaded samples' dates perfectly match the attack's timeline, none of the timestamps or date strings reconstructed from internal web applications and HTTP responses point to a time close to or right after the incident. One assumes that such forensic images are obtained soon after an incident; therefore, any time and date strings and file timestamps must match. In our case, however, we could recover the most recent date string from an internal HTTP request dump on 2021-06-18. This was about four months before the incident. One possible explanation could be that the time and date of the server(s) from which the dumps were obtained were incorrectly set. This can happen on an isolated and offline computer and would not be unusual. However, in a large network of interconnected systems, incorrect dates and times can lead to various issues, with TLS/SSL or VPN handshake being the least. As this system heavily relies on billing data and transaction records, it would be hard to imagine the entire network's date or NTP would be set incorrectly. **This is another reason for not confidently attributing these uploads to the forensics team.** Another explanation could be that uploaded artifacts simply did not contain the latest logs and artifacts. More inspection and reconstruction of data and process memory contents within dumps is needed and might reveal even more inconsistencies. Attributions are hard, but when dealing with inconsistent forensics data "leaks", they become even more complicated.

Reviewing the Dumps:

Regardless of the origin of the uploaded dumps and the intention or reason behind uploading them, we can still proceed with reviewing them. We reviewed, reversed, or reconstructed only a small and selective subset of the dumps. Still, we learned a great deal about the system implementation, how it works, and, most interestingly, how it can be attacked. Coming from a security research and penetration testing background, this soon turned into a scavenger hunt challenge, looking for potential vulnerabilities and repetitive cycles of coming up with attack scenarios and looking in the artifacts to find and confirm the possibility of it. While the attackers have never revealed their steps, and we also have no official forensics reports that would reconstruct the attack, we were able to independently identify multiple attack vectors and vulnerabilities that can be exploited to compromise various parts of the system, gain privileged access to servers or even compromise VPN connections. Various encrypted and clear-text credentials were also recovered during the process, some of which would effectively provide the same level of access to the internal network as an IPC server.

The Analysis Report by Modaberan Co:

In parallel with observing the leaks, we also followed multiple leads provided by individuals or posted online in social media or open discussion groups. Interestingly, after a few days, a private company in Iran named Modaberan released a report of 104 pages about the incident. This report was not officially posted online through their official channels but it was also not labeled as private information nor addressed to any specific client or entity and is worded in such a way that it seems to be for limited public release. Nevertheless, this report has been openly circulating between individual Iranian discussion groups. We will not release and include the complete report here, but we will address some key details.

MFP
مدبران
ارایه راهکارهای جامع شبکه، امنیت اطلاعات،
مجازی سازی و امنیت سیستمهای کنترل صنعتی
Gilbarco

گزارش تحلیلی از
حمله سایبری به

سامانه هوشمند توزیع سوخت

تهیه شده توسط

گروه فارنزیک صنعتی شرکت مدبران

www.modaberan-ics.com

۱۴۰۰/۰۸/۰۷

[Modaberan’s report cover page]

The report's authors address the main fact right at the beginning; despite the misleading title, this is not an actual forensics report and is mainly speculations based on the company’s previous experience and knowledge about the smart fuel system. They also address their lack of involvement with the incident (which we can confirm since we already identified another company in charge of the forensics). Considering the contents of the report, their lack of involvement or current access to forensics data or even operational systems, their intentions behind releasing such a report quickly go off the track.

The report goes on 95 pages about the system's design and how the infrastructure is organized and managed. It includes a colorful array of screenshots, hardware photographs, and details that one would consider should remain private unless we are directly investigating and analyzing their involvement in the incident. The report then goes on for two pages speculating about potential attack vectors, some of which are unrealistic but other guesses aligned with our investigation results based on obtained samples and memory dumps. **Interestingly, they also speculate about a potential attack vector being a compromise of server remote management solutions such as iLO. As mentioned, a few weeks ago, another Iranian company published an analysis report about rootkits found in Iranian networks that would compromise and backdoor the iLO**. To their credit, they repeatedly made it clear in the report that provided details are purely based on speculations and not facts.

The report is finally wrapped up by proposing a few ways to improve the security of the infrastructure. Some of these recommendations have notable technical mistakes, indicating a lack of understanding about proposed solutions. Overall, the report seems to be an attempt to vaguely answer some questions, unnecessarily releasing some technical details (mainly translation of Ingenico documents and security standards notes) and perhaps an attempt to use the opportunity to advertise the company.