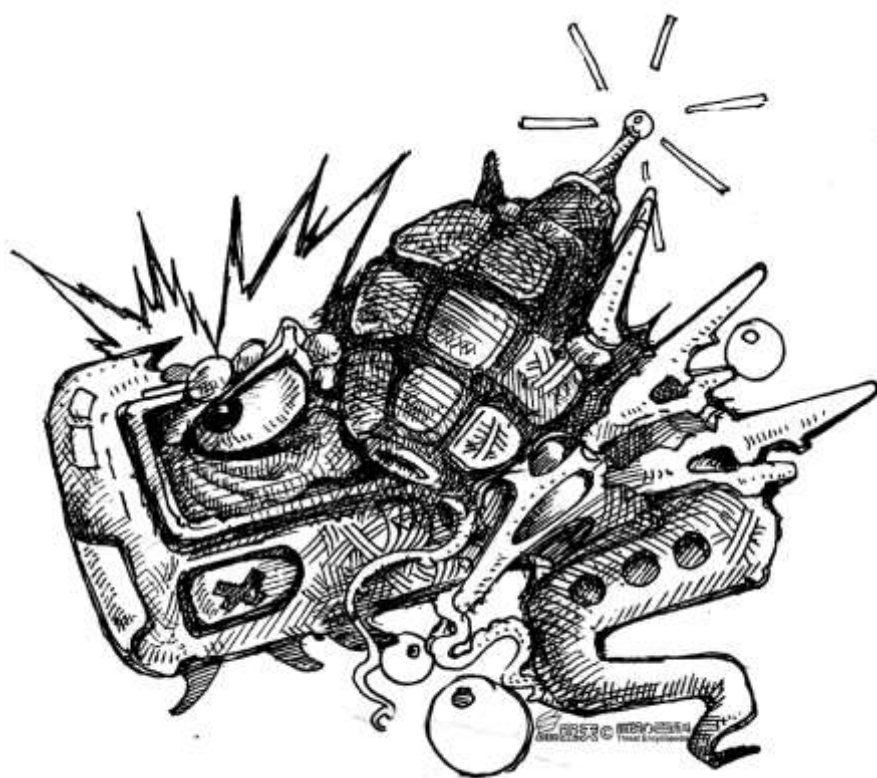




# Analysis and Research on the Bombing Incident of BPMs in Lebanon

Joint Analysis Group of Antiy

*The original report is in Chinese, and this version is an AI-translated edition.*



Completion time of first draft: 23: 15, September 18, 2024

First published: 01: 04, 19 September 2024

This edition was updated at 10: 00 on 24 September 2024



Scan QR code for the latest version of the report

# Table of Contents

---

1. overview of the event1 .....	1
2 Scope of impact of the event 1.....	1
Guess the cause of pager explosion 2.....	3
Pager operation process 5 .....	5
Analysis of explosives 5 .....	6
5.1 Battery energy analysis 6 .....	7
5.2 Type Information and Guess of Explosive Charge 6.....	7
5.3 The explosion escalates again (new content in this update) 7 .....	8
Analysis of the principle of trigger explosion of pager 8 .....	错误!未定义书签。
Analysis of supply chain presetting 9 .....	11
8 Conclusion 10 .....	12
Appendix I: Reference Link 13.....	16
Appendix II: Media coverage and analysis of the pager explosion in Lebanon 14 .....	17
1. incident development and response 14.....	17
Related analysis on the explosion 15 .....	18
Appendix III: Information of the Institutions Participating in the Preparation of the Report 16.....	19
Appendix IV: About Antiy 17.....	错误!未定义书签。

*Note: On the 17th, a large number of pagers exploded in Lebanon, and Antiy organized an analysis team to follow up, analyze and report the incident on the Internet, and observed mixed information and many wrong guesses, in order to clear up the misunderstanding of the public. After making necessary deletions and additions to key contents on the basis of the submitted version, we released the public version report on the public account of Antiy Vertical Response Platform at 1: 00 a.m. on the 19<sup>th</sup> September. Due to insufficient inspection and proofreading, the manuscript has many typographical errors. After this re-proofreading and supplementation, it will be re-published in the public account of Antiy Group, and the website version will be updated synchronously.*

## 1 Overview of the event

---

On the afternoon of September 17, 2024, local time, a large number of BPMs exploded in Beirut, the capital of Lebanon, as well as in the southeastern and northeastern parts of Lebanon. Lebanon's Hezbollah immediately posted on its Telegram channel that the explosion occurred at around 3: 30 p.m. local time, affecting "staff" of Hezbollah agencies and "a large number" of people were injured. As of 16: 00 on the 18th, the Times of Israel, citing data from the Lebanese public health sector, said that 11 people were killed and some 4,000 injured in the blast, including about 500 people who were both blind. 19 local time, including the walkie-talkie explosion, Lebanon's minister of public health said the explosion has killed 37 people.

Based on the fact that this event was initially reported by multiple parties as an event triggered by a network attack, to sort out the actual situation, Antiy formed a joint analysis team composed of three teams, namely Antiy CERT, Strategic Intelligence Center and Wireless Security Technology Research and Development Group, to conduct the analysis. After comprehensive research and judgment, we preliminarily believe that this is based on the supply chain (including distribution and logistics) side, combining explosives and communication equipment, and using remote signal to activate the control circuit. Serious event to realize batch trigger explosion. The overall judgment and analysis process is as follows.

## 2 Scope of impact of the event

---

In accordance with media and online information, that explosion took place mainly in the Hezbollah-strong areas of Lebanon, particularly in the southern suburb of Beirut and the Bekaa area, The reason for the explosion was the use of certain brands and models of pagers, including Gold Apollo Pager AP-900 GP and AR-924 according to

the information collected so far. The above models are pagers of the brand of Golden Apollo Company in Taiwan Region of China. But there are also insufficiently verified reports that the exploding pagers also include Motorola LX2, Teletrim and other brands. The communications equipment that exploded is a pager that has been abandoned by the vast majority of people in the era of mobile phones. However, since that pagers are one-way signal receive equipment and do not transmit signals, they have the advantage of being difficult to be located, It is heavily used by members of Hezbollah and key government posts in Lebanon. Cyber sources say Hezbollah ordered more than 3,000 pagers from Kim Apollo to distribute to members across Lebanon, as well as to Hezbollah allies in Iran and Syria. After the incident, Hezbollah confirmed that a large number of its members were injured, and Iran's state media, IRNA, confirmed that Iran's ambassador to Lebanon, Mujtaba Amani, was injured in the pager bombing.

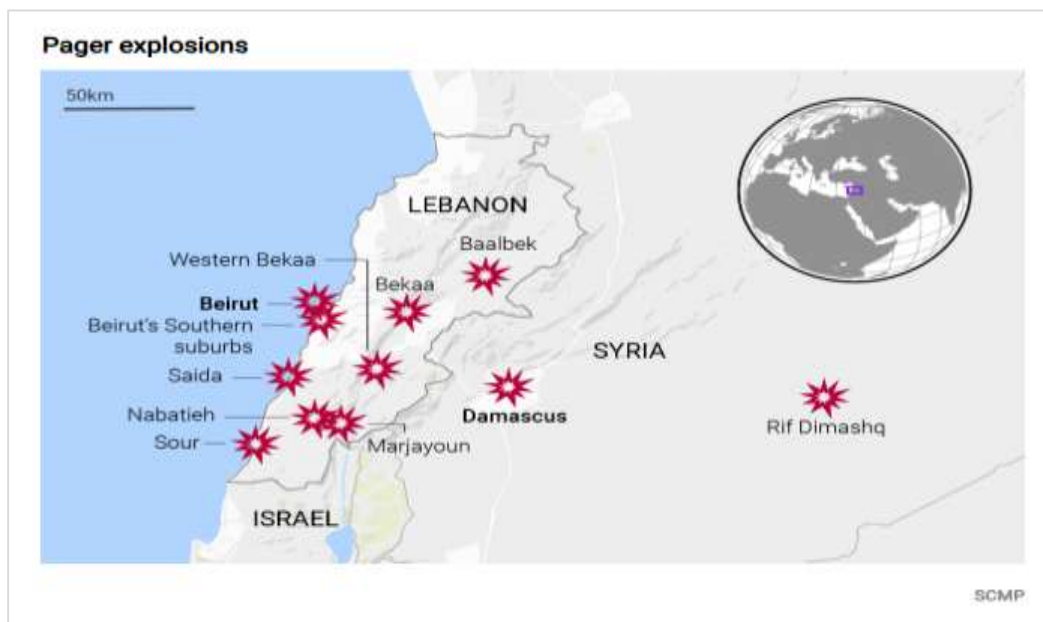


Figure 2-1 Pager expansion map provided by scmp1

Electronic surveillance technology is playing an important role in Israel's attacks on Lebanon. Israel has installed surveillance cameras and remote sensing systems in Hezbollah's areas of activity, and has regularly sent surveillance drones across the Lebanese-Israeli border to monitor Hezbollah, the Israel Defense Forces said earlier. In addition, according to sources, according to mobile phone location data, the Israeli air campaign has precisely targeted the removal of several senior Hezbollah commanders. As a result, starting in February 2024, Hizbullah ordered to abandon the use of mobile phones and other devices to avoid the penetration of Israeli and American spyware, and to adopt older, less technical means of communication. Including pagers and verbal transmission of code words. However, it can be judged that that explosion targeted specific message code sent by specific pagers of a specific

type, and was clearly aimed at the target population of Hezbollah in Lebanon, through supply chain presetting and the combination of explosives and communication equipment, Directed attack activity activated by remote signals.

Israel's military conflict with Lebanon has continued for years, and just hours before the bombings, Israeli security agencies said, Thwarted Hezbollah's attempt to assassinate a former senior Israeli official using a controlled remotely detonated explosive device. Kim Ghattas, a Lebanese journalist and staff writer for The Atlantic, said in an interview with CNN on Sunday that "this was clearly a targeted Israeli attack" on Hezbollah operatives, The attack may have three purposes: One is to show the ability to control intelligence, the other is to deter Hezbollah into submission, and the third is to create internal chaos in Hezbollah as a prelude to launching a large-scale attack on Lebanon.

### 3 The guesses the BPMs explosion cause

According to the photos of the site debris, the exploded pagers pointed to two pager products, AP-900 GP and AR-924, made by Gold Apollo in Taiwan, China. But Kim Apollo 18 released a news that the explosion of the pager was made by a European agent company, Hungarian BAC CONSULTING KFT, authorized by the company's brand. Established a partnership with this European agent three years ago. As a whole, we tend that even if the pager is made by BAC CONSULTING KFT, its entire process and specification should be the same as that of Golden Apollo, which can be regarded as OEM OEM and OEM, and there should be no big difference in its mechanism.



Figure 3-1 Related picture of the pagers1

The event-related pager models and parameters are shown in Table 3-1 and Table 3-2.

Table 3-1 AP-900 pager parameters 1

Product appearance		
Product model	Ap-900	
Frequency range	Uhf 450 ~ 470 MHz Vhf 135 ~ 174 MHz	
Paging threshold	1200bps-7 $\mu$ V / M 2400 bps -9 $\mu$ V / M 512bps-5 $\mu$ V / M	
Pocsag code rate	512 / 1200 / 2400 bps	
Channel spacing	12.5khz, 25KHz	
Coding format	Pocsag	
Interference suppression	40db	
Alarm tone intensity	87db @ 10cm	
Message code	8	
Type and number of batteries	Aaa alkaline battery, including 1 cell with the product	
Dimensions	80.7 mm (L) 55.4 mm (W) 20 mm (H)	
Weight	49.6g	



Table 3-2 AR-924 pager parameters

Product appearance	
Product model	Ar-924
Frequency range	Uhf: 450 ~ 470MHz
Paging threshold	512bps: -110dbm 1200bps: -108dbm 2400 bps: -106 dBm
Pocsag code rate	512 / 1200 / 2400 bps for POCSAG
Channel spacing	25khz
Coding format	Pocsag
Interference suppression	> 40dB
Alarm tone intensity	Unknown
Message code	8. frame independent
Type and number of batteries	Lithium batteries, up to 85 days of use, 2.5 hours full battery charge, USB-C charging, protection circuit module (PCM) technology
Dimensions	73 (L) 50 (W) 27 (H) mm
Weight	95g (battery included)

## 4 The working process of the pager

Pager is a kind of wireless communication equipment, which is mainly used to receive short messages or notifications. It transmits information through radio signals between the sending end and the receiving end, and is widely used in situations that need instant communication, such as medical treatment, service industry, emergency rescue and so on.

The paging system is composed of a transmitting end (paging center / base station), a paging transmitter, a control system, a transmission medium, and a receiving end (pager), and its operation process is shown in Figure 4-1.

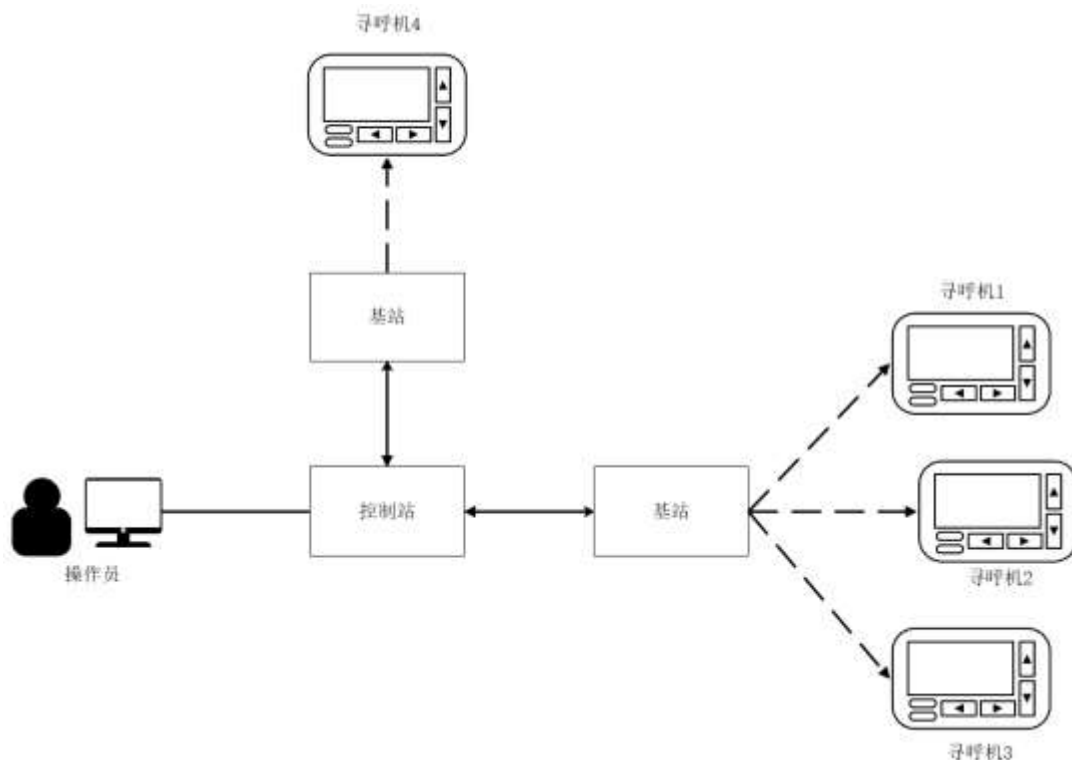


Figure 4-1 The schematic diagram of the operation of the paging system 1

When the paging system is in operation, the operator first sends a message to the control station through the control terminal, and specifies the number or address of the target pager, the control station modulates the transmission information, codes the transmission information and transmits it through the base station. After receiving the signal from the base station, the pager demodulates and decodes the signal, judges whether its own number or address is consistent with that in the message, and if so, sends a prompt to the user and displays the message content.

## 5 Explosive analysis

In the initial reports of this incident, many described Israel's cyberattack on the pager, which caused the explosion by warming up the battery. According to the follow-up comprehensive information analysis and technical analysis, it is obvious that the relevant reports do not conform to the actual situation.



## 5.1 Battery energy analysis

Taking the AAA alkaline battery used in the AP-900 GP as an example, the total energy stored can be calculated.

Capacity: Typical capacity of AAA alkaline batteries is about 1000 milliampere-hours (mAh)

Voltage: Nominal 1.5 volts (V)

The total energy stored by the battery can be calculated by the following formula: Energy (in watts) = voltage (in volts) x capacity (in amperes), converting the capacity from mAh to amperes: 1000 mAh = 1 Ah, Calculate total energy: Energy = 1.5 V  $\times$  1 Ah = 1.5 Watt-hour (Wh), convert energy into joules (J): 1 Watt is equal to 3600 joules, energy (J) = 1.5 Wh  $\times$  3600 J / Wh = 5400 J. The total energy storage of the battery is about 5400 joules.

However, the power of explosives lies not in the total energy but in the rate of release of energy, the total energy released by an explosion of 1 kg of TNT being less than the total energy released by complete combustion of 1 kg of quality coal, However, explosives such as TNT, which can release all of their explosive energy in a few millionths of a second, are fundamental sources of explosive power. No alkaline battery or lithium battery has the condition of instantaneous release mechanism. Therefore, judging from the casualties on the scene, even if the battery short-circuit causes a fire, the rate of releasing energy is far from sufficient to cause such a degree of killing power. It is absolutely certain that the explosion was caused by a high explosive.

## 5.2 Type information and guessing of explosive charge

From the point of view of energy release rate, it is impossible for alkaline batteries and lithium batteries to achieve the explosion consequences in video and text messages in the existing information. It is generally accepted by technical experts that the explosion is clearly caused by an explosive based on its intensity and speed. In term of that specific type of explosive, it must not be ordinary explosive such as black powder or pyrotechnic composition, but can only be high explosive. In the event, the explosive should be stable (it must be stable in the process of transportation and loading of the pager), easy to detonate, small in size and with sufficient power, and high sensitivity such as silver fulminate (silver fulminate). In general, unstable peroxides such as TATP made by folk people are unlikely, and aromatic nitro compounds such as TNT, which require a large amount of priming agent to detonate, are not likely to detonate easily. The explosive of nitrate ester such as PETN (pentaerythritol tetranitrate, pentaerythritol tetranitrate, also known as PETN, whose intensity is higher than that of TNT is more likely. Taken as a whole, the pager itself acts as a remote trigger plus explosive carrier in the event. At present, the network information is mostly


inferred as PETN (pentaerythritol tetranitrate), and the information about whether the explosive charge is inside the battery or inside the pager is not enough to support the judgment. The analysis team as a whole tends to have explosive charges inside the battery, which may also explain the explosion of other electronic devices that are currently undetermined from the source feedback, as a result of loading the battery with explosives into other electrical devices, But other information is currently difficult to determine.

### 5.3 Explosion escalates again (new additions to this update)

With less than 24 hours to go before the pager exploded, the bombings escalated again on 18 September, with Lebanon's Health Ministry saying a large number of walkie-talkies exploded in a new explosion that killed 20 people, according to the BBC, At least 450 people were injured. The manufacturer of the walkie-talkie known to have exploded is Japan's ICOM (ICOM), a model of the ICOM V82 series handheld walkie-talkie, and the Japanese radio communication company involved said that the ICOM model was discontinued in 2014. Sources point out that Hizbullah purchased these ICOM V82 series hand-held walkie-talkies five months ago, almost at the same time as the purchase of pagers. In addition, the working principle of the slave interphone and the pager is to communicate by radio, and the main difference is that the communication mode is different from the coding and decoding mode, wherein the pager is the single receiving communication, The interphone is two-way communication (half-duplex communication equipment). It is also noteworthy that the communication frequency band of the interphone in the event is VHF frequency band, and the specific frequency range is 136-174Mhz. This range is exactly the same as the VHF band operating range of the AP-900 model pager. Therefore, it is not excluded to adopt the unified software radio scheme to simulate different broadcasting technical schemes, or transmit the broadcasting signal through the pager network or the interphone equipment alone, and aiming at the triggering principle of the interphone, In accordance with that data analysis of ICOM V82, at present, the product support the function of triggering the prompt tone, that is, the physical signal of trigger the prompt tone after receiving specific "information" can be set, In addition, that device can be use as the condition of physical signal for detonating the explosive, and support multiple "trigger information" setting and group call, so as to realize group range control based on "call information" as the trigger condition. Based on the above situation, we infer that the equipment needs to perform two steps of operation in the supply chain, the first step is to configure the "trigger information" for the interphone equipment. In that second step, the circuit of the explosive combine device is preset in the interphone equipment, and the circuit of the detonating condition is modify. After completing the above supply chain operation, when it is necessary to perform an explosion attack, a call request carrying "call information" needs to be sent to a specific group device through a device capable

of sending preset "call information," Equipment contaminated by the supply chain carries out an explosive attack upon receipt of the Call Trigger Message.

**Table 5-1 Parameters of ICOM V82 Interphone 51**

<b>Product appearance</b>		
<b>Product model</b>	Icom V82	
<b>Frequency range</b>	136-174MHz	
<b>Frequency stability</b>	$\pm 2.5\text{ppm}$ (-10 ° C to + 60 ° C)	
<b>Model</b>	F3e, F2D, [F7W optional]	
<b>Number of memory channels</b>	207 channels (200 storage channels, 1 call channel and 6 scan edges)	
<b>The function of triggering the beep tone</b>	Support	
<b>Group call function</b>	Support	
<b>Supported tone formats</b>	Ctcss, DTCS	
<b>Power supply</b>	7.2vdc	
<b>Type and quantity of batteries</b>	Lithium battery or battery box, the battery box adopts 6 AA alkaline batteries	
<b>Current consumption (at 7.2VDC)</b>	Transmitter: 2.6a in the state of maximum power 7W; Receiver: 250ma in the maximum audio state; In standby state, it is 80mA; In that pow saving state, it is 30mA;	
<b>Dimensions</b>	37.5 (L) 54 (W) 139 (H) mm	
<b>Weight</b>	390g / 13.8Oz	

Transmitter	
Transmit power	7w (VHF)
Spurious emissions	< -60dB
Maximum frequency deviation	$\pm 5\text{kHz} / \pm 2.5\text{kHz}$ (wide / narrow)
Receiver	
Receiving system	Two-stage conversion superheterodyne
Intermediate frequency	1,46.35mhz 2,450khz
Sensitivity	Typical value of 0.16 $\mu\text{V}$
Squelch Sensitivity (Threshold)	Typical value of 0.11 $\mu\text{V}$
Selectivity	> 55 / 50dB (W / N)
Intermodulation	65db
Spurious and image suppression	80db (typ.)

## 6 Analysis of the principle of pager-triggered explosions

According to the BBC report and some news reports, the two pager products of Gold Apollo, which are the models of AP-900 GP and AR-924, have exploded. The explosion occurred when the pager user received a string of "alphanumeric" text messages, and it can be inferred that the device had been implanted with "explosives" in the supply chain. The trigger mechanism of the pager is re-coded or the trigger sensor is implanted. For the first inference of re-encoding, we infer that the device requires a two-step operation in the supply chain, the first step being the programmed configuration of the pager device, Triggered by the user equipment; the second step is to preset the explosive binding device circuit in the pager equipment and modify the detonating condition circuit. In that second type of implant initiation sensor, the device needs to be pre-load with explosives and sensors written with initiation logic in the supply chain, and to adjust the electrical connections. We have analyzed the relevant product information including software programming setting information. The triggering principle of various paths is mapped, but information abuse is avoided, the analysis and illustration of specific triggering process are blocked in the public

version of analysis report, and relevant information is only retained in the version submitted to the competent department.

## 7 Analysis of supply chain presetting

The explosion, generally believed to be based on the supply chain side of communications equipment preset explosives. The overall preference pre-setting process should be the warehousing and logistics links rather than the production and manufacturing links. After the incident, Edward Snowden wrote in a post on X (see Figure 7-1) that the incident reminded him of the disclosure of the mass surveillance revelations in 2013. How the National Security Agency intercepts computer network equipment at airports bound for a target country, installs implants and then repackages them for delivery to the target in order to infiltrate the target network. "Ten years have passed, and transportation security has never improved," Mr. Snowden said, alluding to the fact that the Lebanese pager incident had something to do with supply chain presetting by American and Israeli intelligence agencies. Figure 7-1 Snowden's image shows N.S.A. personnel hijacking the replacement firmware of routing devices in distribution 1



**Figure 7-1 Snowden's image shows N.S.A. personnel hijacking the replacement firmware of routing devices in distribution 1**

David Kennedy, a former intelligence analyst at the National Security Agency (NSA), said the explosion seen in the video shared online appeared to be "too large to be a remote direct hack, Causing the pager to overload and cause the lithium battery to explode "It is more likely that Israel has planted personnel in Hizbullah, and the pager may have been implanted with explosives that will only explode when a specific message is received." According to Kennedy, "the complexity required to achieve this is mind-boggling, requiring many different intelligence

components and execution. Human intelligence (HUMINT) is the main method to achieve this, while intercepting the supply chain to make modifications to the pagers. "

Special attention should be paid to the investigation and analysis if the relevant pager is manufactured by BAC CONSULTING KFT in Europe, as stated in the statement of Apollo Kim. This is perplexing because the labor cost in Taiwan is relatively low, and that in Europe is relatively high, and pager is a backward product, and relevant European manufacturers propose to transfer the manufacturing to Europe. Is unusual, whether this is actually the intelligence agencies front layout, still needs to be deeply observed.

## 8 Conclusion

---

It is not unusual to carry out remote control assassination based on telecommunications equipment. In many public security cases at home and abroad, as well as a large number of international terrorism cases, pagers or mobile phones have appeared, but the sharp differences in this incident are as follows:

1. This event pager has dual attributes of both trigger and explosive container; most historical events have the pager as trigger, but not as explosive container.
2. It is possible for the event pager to implement specific signal-based triggering to realize uniform triggering; most events are triggered upon receipt of a signal by the pager, rather than requiring specific signal triggering.
3. This event is a batch directed attack on a particular group; and the historical event is either a directed attack on an individual target or an undifferentiated attack on a group target.

Based on all the above analysis, we have judged that the event is a serious geo-security event based on the operation on the supply chain side, which combines explosives and communication equipment and uses remote signals to activate control and trigger explosions in batches. It is a combination of supply chain presetting, electromagnetic spectrum attack, intelligence collection, human operation and other complex killing chain processes, and is a well-planned joint operation that spans physical domain, network space domain, signal spectrum domain and cognitive domain. In term of operation process, network attack operation may play a role in continuous intelligence collection, such as obtaining relevant logistic information and finding out that operation rules of the target organization. If that final trig signal is not released by the electronic war device, it does not exclude the case that the paging station device is subject to network intrusion. But overall, the dominant factors in this event remain physics,

traditional electromagnetic spectrum and human operations. We should not overstate the role of cyber attacks, but should, based on an objective and rigorous analysis, thoroughly summarize the regular factors of events, including:

- 1. The dominance of network equipment in peacetime and the dominance of physical equipment in wartime are still the basic logic of war at present.**
- 2. For low-network-dependent agents, it is difficult to rely on network operations to achieve critical results, but the collective physical, electromagnetic, and cognitive spectrum can be overwhelming.**
- 3. Trying to achieve their own security by means of reverse informatization may bring about greater security passivity.**

In the face of this composite operation mode, we must go beyond the narrow-band network security perspective, look at the future struggles and challenges from the perspective of overall national security, with the perspective of big network security. Strengthen the combination of civil defense, physical defense and technical defense, and integrate safety elements throughout the whole life cycle.

-----

#### **New contents added in this update:**

Related incidents refer to serious geo-security incidents in which explosives and trigger logic are preset based on the supply chain of communication products, and the incidents involve mass killing of a certain range of people.

It was a serious event comparable to the Nord Stream pipeline explosion, and yet another Pandora's box was opened.

Its disastrous consequences are not due to the application of technical means, whether based on the pre-setting of IT products, using IT products as triggers for auxiliary attacks, or using high explosives for attacks, etc. Including the combination of these technologies, are far from new. Its particularity lies not only in its planning, long-term layout and close organization, which is the normal state of the western intelligence system. Targeted presets for civilian IT products (such as targeted presets of Cisco routers, hard disk firmware, etc.) to universal presets (such as SP800 / The standard contamination of 90 pairs of encrypted random numbers is common in Western intelligence activities, but this prefabrication is at the level of system logic, bringing with it an invasion of data and privacy rather than a direct impact on life safety. So even the Snowden affair has exposed schemes such as "prism," "main road," "dock" and "nuclear." More stress and fear for web users around the world remains on the level of personal information and



privacy rather than personal safety. And this explosion is the first time the use of civil IT products based on the supply chain to achieve a scale of personnel killing incidents.

This incident both violates international law "strictly prohibit the weaponization of objects used by the people," and goes beyond the bottom line. It not only seriously threatens people's lives and causes personal injury, but also shakes the basic trust of global users in the security of basic communication products and global supply chains. The world is never peaceful, but even in the complex format of geo-security, only people with specific roles face specific personal security risks, while the general population faces sporadic and sudden risks. This has basically become a human consensus.

But the bottom line is constantly breaking and penetrating. The incident was an activity of the nature of state terrorism.

In our second-hand market, we try to find the same type of BP machine, to carry out more in-depth analysis of the moment. We absentmindedly returned to July 2010 to analyze the days of Stuxnet: In order to install WinCC configuration software, we purchased used Siemens PLC-300 industrial templates from Taobao and temporarily used a set of heating devices to simulate centrifuges on a foam board. The earliest sand tray that set up the seismic net. To complex attack activity, the condition that carries on counterplan, often and not complete, need to assemble, grope even guess. The reason we rise to a great sense of vigilance and pressure is the regret we feel when we look back on the Stuxnet incident.

The complex analysis of seismic networks was carried out by security workers around the world, In that follow years, the operational mechanism, the modular structure, the complex operational logic and the judgment of the condition, and even the operational mechanism of the centrifuge include Kaspersky, International colleagues including Symantec have conducted in-depth analysis, and the Antiy team has also discussed the USB ferry mechanism, the homology with Duku, and the code framework associated with subsequent sets of malicious codes. And made his own contribution. In that history of mankind, a collective analysis of a single threat with the large number of institutional personnel and the long-term involvement, although it is not organized, Just relying on the original sense of purpose and concern for threats of the various security teams. But our regret is that after this analysis, the global recognition is focused on a new type of virus that uses multiple 0day vulnerabilities, a new technical security risk in the industrial field. It does not rise to the point that this is a network-based approach to the

implementation of the industrial infrastructure of a sovereign state with the equivalent of a firepower combat operation.

As also stated in "Why Stuxnet is not APT," Stuxnet is a combat operation. The Stuxnet incident brought about a very important window of opportunity for diplomacy and the struggle of international public opinion, which could pin Western intelligence agencies to the column of cyberattack in 2010; We can get rid of the western sense of superiority based on technology; we can unite the third world countries to play games with the United States and discuss the code of conduct for national security activities in cyberspace. If we had grasped this historic opportunity, the US policy of naming and shaming our side at the 2012 congressional hearing on "China's cyberspace capability and nuclear capability development" would have lost the international public opinion foundation for its implementation. However, various factors at that time made both domestic and international organizations view the incident according to a new kind of technical risk, and even after the US attack was exposed. Instead, they achieved a strategic effect of showing off their capabilities and implementing deterrence. Finally let the United States, with the intelligence agencies as the instigator of the Stuxnet incident, realized the "thing went to the clothing" magnificent escape. As the first technical team to be involved in the analysis, this is a great regret we can't let go of.

Hence, we must not only carry out threat analysis with extreme objectivity and rigour and solid technical work, but we must also go beyond technology, We should put events in the context of major changes unseen in a century, and put them in the context of global geo-security. We must discuss the nature of this incident of state terrorism and its serious harm to the global system of basic information products and supply chains.

All generalization behavior will bring the risk of behavior out of control, and it will also raise the safety cost and cost of human society.

-----

**In that middle east incident, we can see that only a strong country can be peaceful.**

## Appendix I: References

---

- [1] The Mystery of Hezbollah's Deadly Exploding Pagers  
<https://www.wired.com/story/pager-expansion-hezbollah/>
- [2] At last 3 types of makers were placed with bombs  
<https://twitter.com/clashreport/status/1836105986831966483>
- [3] Hezbollah blazes Israel after pager explosions kill nine and prevent thousands in Lebanon  
<https://www.bc.co.uk/news/articles/cd7xnelvpepo>
- [4] Product Family - Alpha Gold  
[https://americanmessaging.net/wp-content/uploads/2019/10/communication\\_gold\\_pps.pdf](https://americanmessaging.net/wp-content/uploads/2019/10/communication_gold_pps.pdf)
- [5] Alphanumeric Pager (AP-900)  
<https://www.gapollo.com.tw/product/ap-900/>
- [6] Gold Apollo Rugged Pager AR924 - Apollo Systems  
<https://web.archive.org/web/20240917160632/https://apollosystemshk.com/product/42.html>
- [7] Rugged Pager AR924-GOLD APOLLO  
<https://web.archive.org/web/20240917152704/https://www.gapollo.com.tw/rugged-pager-ar924/>
- [8] Analysis × Hezbollah blazes Israel for deeply pager blasts in Lebanon-but how was it done  
<https://www.scmp.com/news/world/middle-east/article/3278939/hezbollah-blazes-Israel-dead-pager-blasts-lebanon-how-was-it-done>
- [9] Circular on Preinstalled Backdoor Vulnerabilities in Several Routers  
<https://xxhjs.nuc.edu.cn/info/1011/1360.htm>
- [10] What we know about the Hezbollah device experiences  
<https://www.bc.com/news/articles/cz04m913m49o>
- [11] Icom IC-V82 VHF FM Transceiver 136-174 Radio  
[https://www.409shop.com/409shop\\_product.php?Id=103886](https://www.409shop.com/409shop_product.php?Id=103886)
- [12] Israel blew up pagers and radios, killing more than 100 firecrackers  
<https://share.ifeng.com/c/s/v006Dq-zUTH4kq5TUy92vQILsp-1SDkJwLkBB-a2-T9fPkIoKxMRDfRp-D1Xfb6L?>

## Appendix II: Media coverage and analysis of the pager explosion in Lebanon

---

### 1. Incident development and reaction of all parties

On September 17, CNN reported that a number of people were killed or injured in the bombing of a pager belonging to Hezbollah staff in many parts of Lebanon. The Lebanese Interior Force said the explosion involved several areas in Lebanon, particularly the southern suburbs of Beirut. Locations include: Dahiyah in the southern suburbs of Beirut, the towns of Ali Nahri and Lijak in the Bekaa Valley in central Lebanon, and Sidon and Thiel in southern Lebanon. At least nine people have been killed in the pager bombing, including an 8-year-old girl, Lebanese Health Minister Firas Abyad said in an interview with Al Jazeera on Sunday. About 2,800 others were injured in the incident, Abyad added.

On September 17, Iranian state media IRNA reported that Iran's ambassador to Lebanon, Mujtaba Amani, was injured in a pager explosion. Iran's semi-official Fars news agency reported that two staff members at the Iranian embassy were injured.

"We hold the enemies of Israel fully responsible for this criminal attack, which resulted in the loss of several lives, the damage to civilians and the injury of a large number of people," Hezbollah said in a statement on the evening of September 17.

On 17 September, the IDF said it would not comment on the bombings in Lebanon.

On September 18, CNN reported, citing the Lebanese state news agency NNA, that Lebanese Prime Minister Najib Mikati said at a cabinet meeting on September 17 that the attack was "an act of criminal aggression by Israel that seriously violates the sovereignty of Lebanon, It's a crime by any standard. The Lebanese government has contacted the United Nations and the countries concerned "to hold them accountable for this continuing crime," Information Minister Ziad Makary said in Beirut.

On September 18, The New York Times reported that Israel had placed explosives in a batch of pagers made by Taiwan's Kim Apollo, imported to Lebanon for shipment to Hezbollah.

On September 18, CNN reported that the founder and chairman of Taiwan-based Golden Apollo said the pagers used in the attack on Hezbollah in Lebanon were licensed under the Golden Apollo brand and produced on contract by European BAC CONSULTING KFT.

On September 19, CNN reported that the Hungarian government said on September 18 that BAC CONSULTING KFT was only "a trading intermediary" and had no manufacturing base in the country.

September 19, the associated press reported that the 18 occurred in Lebanon more than the second wave of radio attacks. Lebanon's Health Ministry said at least 20 people were killed and more than 450 injured in the second wave of attacks. 17 pager bombings have killed at least 12 people.

On September 19, CNN reported that the Lebanese Ministry of Communications said on September 18 that the explosion of the radio walkie-talkie was a discontinued model made by Japan's ICOM company. The walkie-talkie was not supplied by the agent, was not officially licensed and was not vetted by the country's security services.

## 2. A correlative analysis of the explosion

On September 17, Al Jazeera's website posted that it was unclear exactly how the pagers exploded, and speculation centered on the radio network on which the pagers relied, suggesting that it might have been attacked by hackers, Causes the system to signal, triggering a response from a pager that has been tampered with.

On September 17, when CNN posted that hundreds of pagers were exploding at the same time, experts offered two opinions. One opinion is that there was a cybersecurity breach that caused the pager's lithium battery to overheat and explode. Another opinion is that this was a supply chain attack 'in which pagers were tampered with during manufacture and transport. David Kennedy, a former intelligence analyst at the National Security Agency (NSA), argued that from the video online, the explosion was "too large to be remotely hacked, Causing the pager to be overloaded and the lithium battery to explode. " He thinks the second opinion is more reasonable. "It's more likely that Israel has infiltrated people in Hezbollah, pagers have been implanted with explosives that only explode when they receive specific messages." "The complexity required to achieve this is mind-boggling. It requires a number of different intelligence units to execute. Human intelligence (HUMINT) will be the main way to achieve this, while intercepting the supply chain to make modifications to pagers. "


Speaking to CNN on September 18, Kim Ghattas, a Lebanese journalist and staff writer for The Atlantic, said, "This is clearly a targeted Israeli attack on Hezbollah operatives, These agents are low-skilled and they have been

targets for assassination. They were instructed to discard their iPhones, disconnect the internet and disconnect CCTV, "when asked why Israel carried out the attack, Mr Ghattas said." Either to try to show Hezbollah that Israel knows them well and to make it clear that if they launch more attacks against Israel, they will be attacked even harder, "he said. "Or the prelude to a massive Israeli attack on Lebanon that has thrown Hezbollah's operations into disarray"

On September 18, CNN spoke to a number of cybersecurity experts, Justin Cappos, a professor of cybersecurity at New York University, who said, "The devices are deliberately designed to explode when they are triggered, Not the pagers that the rest of the world is using. " Baptiste Robert, cybersecurity researcher and CEO of Predicta Lab, said it was likely that the pagers had been modified prior to shipment, rather than hacked. He said the scale of the explosion seemed to indicate that it was an organized and complex attack. Michael Horowitz, head of intelligence at security and risk management consultancy Le Beck International, also said the explosion could have been caused by a device modification, not a cyber attack. "We've never seen this strategy used on such a large scale, but it does mean it's not an attack that could affect all pagers. If true, this would indicate a very high supply chain penetration of these devices. "

On 18 September, the Jerusalem Post said that Lebanese security sources had revealed that Israel had hacked into the communication systems of individual devices and detonated them.

## Appendix III: Introduction of the departments participating in the preparation of this report

Sector	Department Profile
 <p><b>Antiy Computer Emergency Response Team</b></p>	<p>Antiy CERT aims to continuously capture, track and analyze threats such as APT attacks, targeted extortion attacks, black and gray crimes, and the actors behind them. Promote the transformation of threat analysis results into the detection and defense capabilities of Antiy engines and products, and the judgment of threat events and trends into the knowledge of the government and the public to understand the threat activities. Support the in-depth security analysis requirements of Antiy security services and other scenarios. The Totem of the Division is the Northeast Leopard, with a keen sense of smell, fierce and fierce actions, and quick wins in every battle.</p>

 <p>先进无线安全技术组 Advanced Wireless Security Technology Group</p> <p><b>Advanced Wireless Security Technology Group</b></p>	<p>The Antiy Advanced Wireless Technology Group is responsible for the exploration of security technology in the field of wireless communication security technology, which is affiliated to the Antiy Technology Committee. Totem for the Black Mamba Serpent, the Black Mamba Cobra is the world's fastest crawling snake, a symbol of perseverance, fierce, full-strength mission objectives.</p>
 <p>战略情报中心 Strategic Intelligence Center</p> <p><b>Strategic Intelligence Center</b></p>	<p>Based on the global cyberspace security field, Antiy Strategic Intelligence Center conducts research on strategic trends, tracking of cutting-edge technologies, dynamic analysis of capabilities, and research and judgment of major events. Provide strategic intelligence services for customers such as strategic risk warning, research and judgment of major events and preparation of strategic reports. Section totem for the owl, the legendary god of war, the god of wisdom, take its implied meaning agile, wise, mighty.</p>



## Appendix IV: About Antiy

---

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP), etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat

detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as “Code Red”, “Dvldr”, “Heartbleed”, “Bash Shellcode” and “WannaCry”. Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspace threat actors (APT groups) such as “Equation”, “White Elephant”, “Lotus” and “Greenspot” and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.