PROFITAP

CAPTURING CYBER THREATS AT AIRPORTS

MANAGING CRITICAL IT OPERATIONS IN THE AVIATION WORLD

THE THREAT LANDSCAPE AT AIRPORTS

On July 26, 2013, airport operations halted at the international terminal of Atatürk International Airport, Istanbul, Turkey. Passport and immigration controls became non-operational and all departing flights were grounded. According to Turkey's local Doğan news agency and Hürriyet Daily News, this chaotic event was caused by a breakdown in Istanbul Provincial Security Control's data system – PolNet – allegedly caused by a cyber attack. Though the PolNet system was eventually restored, it was literally paralyzed for several hours, affecting dozens of flights and thousands of passengers. Airport officials did not confirm the alleged cyber attack, but local media claimed that the PolNet system was compromised due to a cyber attack.

In a more recent case, Reuters reported that a cyber attack on Poland's national airline, LOT, resulted in the grounding of 10 flights out of Warsaw Chopin Airport on June 21, 2015. The attack made LOT's computer system, which contained secure information, to go down for five hours. According to LOT, it was most likely a Distributed Denial of Service (DDoS) attack which overloaded LOT's systems. As a result, around 1400 passengers were stranded at the Warsaw airport for several hours.

While cyber attacks at airports are not as common as within other sectors, what is alarming is the fact that airports are not entirely armed and ready to counter these attacks. Airports are well equipped and trained to manage physical threats, but can seem to not be completely prepared for cyber threats. Security checks and screening at airports all focus towards capturing physical, human threats. Though IT systems and networks at airports do have basic protections, e.g. Firewalls and IDS/IPS, they are not capable to detect and thwart the latest methods of hacks or cyber attacks, like spear-phishing and zero-day attacks.

THE IT LANDSCAPE AT AIRPORTS

Airports have network security and protection mechanisms housed centrally within their datacenters. This is as per the standard network design, and perfectly fine for major businesses. However, there are two key factors that make an airport starkly different from a regular organization:

1. Coverage Area

Airports, especially international airports in major cities, are built over very large spaces, spread over at least a million square meters of area. Spreading the IT infrastructure to cover such a huge area, is in itself a huge task. Monitoring and protecting this IT infrastructure is another challenge. Other commercial enterprises, in spite of how large corporate head offices are, are still much smaller in coverage area.

2. Public Access

By definition, airports are public spaces. Though of course there are specific areas restricted from public access, there is still a large area used by the general public. Some of these areas have public internet access for passengers and visitors in the form of Wi-Fi hotspots. Most of the modern international airports manage these Wi-Fi hotspots themselves and offer public access for free. Business enterprises in contrast, are private spaces meant primarily for employees, with a small proportion of visitors whom are confined to specific reception areas.

When it comes to physical security, airports have multiple layers of checks. Yet this has not been the case for their IT infrastructure. IT networks at airports were traditionally closed-circuited with propriety protocols running on legacy systems. Today, the IT landscape at airports has changed. Modern airports rely heavily on information and communications technology for boarding passengers, baggage check-in, and border control, as well as for the complex operations involved in handling aircraft. The integration of the internet, and the influx of internet access available at public lounges, exposes airports to cyber threats. Even a relatively small-scale cyber attack could disrupt airport operations. Airport authorities are gradually realizing that their IT networks require a different approach in design, management, and protection.

" ... the most bone-chilling evidence we collected in this campaign was the targeting and compromise of transportation networks and systems such as airlines & airports in South Korea, Saudi Arabia and Pakistan. ... [the hackers] achieved complete access to airport gates and their security control systems ... We witnessed a shocking amount of access into the deepest parts of these companies and the airports in which they operate."

Excerpts from the Operation Cleaver report, published by Cylance Inc., Dec 2014

DOUBLE-EDGED THREAT VECTOR

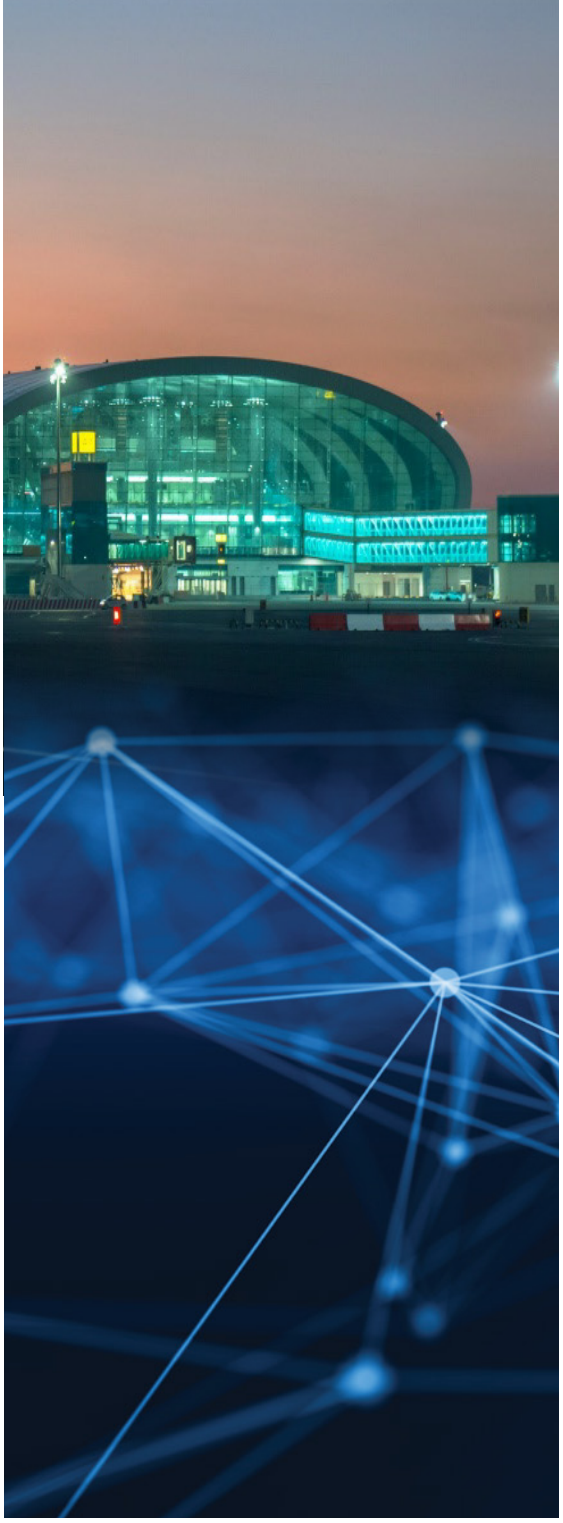
On one hand there is public internet access available to passengers and visitors, and on the other hand internet access is available on the workstations used by airport employees. This creates a double-edged threat vector: external and internal.

1. External

Accessing the public internet via an airport's Wi-Fi hotspot is the external threat vector which could find its way into any peripheral or main part of the airport's network. A hacker could use this path to penetrate into an airport's internal network, unleash a network worm, or even launch a DDoS-style attack to sabotage any of the airport's system. What is even more dangerous is that a hacker could use this free public internet access to launch a cyber attack to any other part of the world, while using the airport's IP address.

2. Internal

Employee workstations having internet access could become a victim of socialengineering techniques, like spear-phishing. The primary purpose of these techniques is to drop a malware on a system by making the user click or visit a fraudulent but legitimate-looking link or site. Once the system is infected, the malware can do a range of malicious activity, including giving external access to a hacker to the user's system. Since the activity was initiated by the user himself, and malwares becoming sophisticated day by day, not even a Firewall or IDS/IPS can detect such attacks. This threat vector has to be taken seriously. Airports are the prime targets in cyber warfare targeted towards critical infrastructure of a country. In their December 2014 report, titled Operation Cleaver, the cyber-security firm Cylance Inc. revealed startling facts about a cyber covert operation targeting critical infrastructure organizations worldwide, allegedly planned and executed by Iran. According to the report, as many as 6 airports and 7 airlines – in South Korea, Saudia Arabia, Pakistan, and United States – were attacked with hackers penetrating into the internal network of these entities. One of the main methods used for these attacks was spear-phishing. The repercussions of such attacks do not end up in the cyber world. They can carry on to the physical world too. For example, according to the Operation Cleaver report the hackers stole large amounts of confidential data including employee information, schedule details, identification photos, airport and airline security information, and PDFs of network, housing, telecom, and electricity diagrams. The consequences of exploiting such sensitive information to coordinate an attack in the physical world are beyond measure.



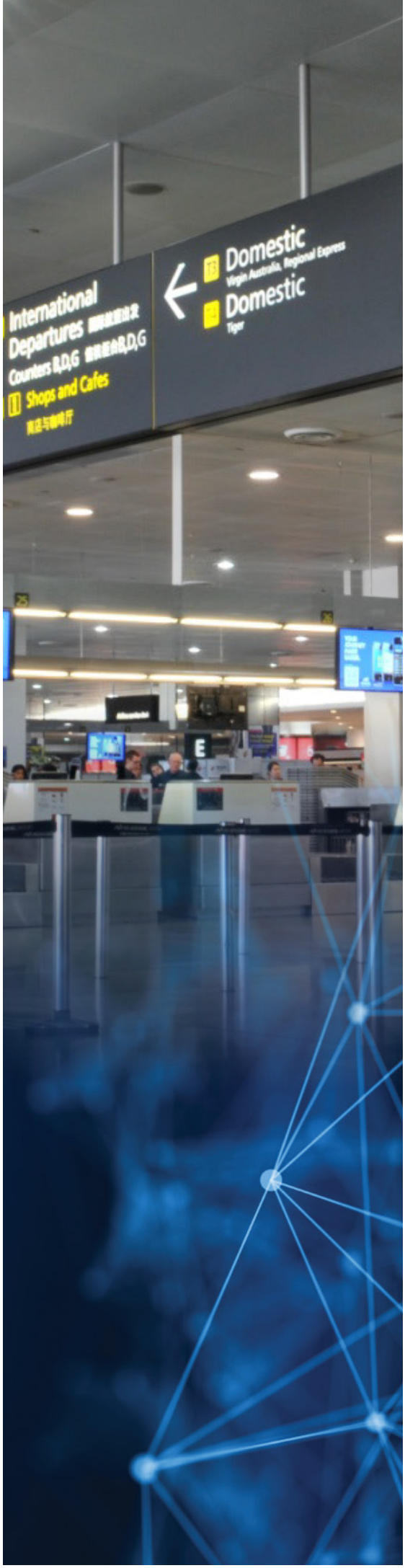
While there are several tools to detect and prevent malicious activities related to cyber attacks, there are occasions where a threat is executed, resulting in a compromise of data, without those tools capturing any information, such as in the event of the isolation of a part of airport with the main network. A hacker could make an airport's area disconnect from the main datacenter by coordinating another malicious activity in the physical world. In such cases, it becomes inevitable to conduct either a real-time or post-event forensic analysis to identify the source of attack, detect the next moves of the attack, or measure the damage done so far.

USING NETWORK FORENSICS FOR THREAT DETECTION AT AIRPORTS

Forensics in the physical world has found its digital counterpart in cyberspace as well, which deals with two domains: data-at-rest, and, data-in-motion. The first domain is mostly about computer forensics which involves post-event analysis of infected computers and their memory or storage. The second domain deals with inspecting data as it occurs in motion, i.e. travels over the network, and is known as "network forensics". While both domains of digital forensics are equally important, however, network investigation is considered to be more useful and critical at crime scenes. For example, if an attacker erases all data from a compromised host, or if the hard disk is damaged after an event, then network-based data traffic might be the only available evidence for forensic analysis. Network forensics is also trickier as it deals with volatile information occurring dynamically. Once network traffic is transmitted it is considered to be 'gone', and hence network forensics is a proactive and concurrent investigation.

Network forensics, also referred as packet forensics, is done by capturing network traffic (i.e. packets) to analyze data, reassemble digitally transferred files, intercept and parse digital communications. The entire content of emails, chat conversations, web surfing activities and file transfers can be recovered and reconstructed to reveal the original transaction.

Thus the cybersecurity teams need to have the ability to intercept network traffic and capture data packets in real-time. Organizations usually set up their traffic capture mechanism according to the size and architecture of their network. For example, enterprise organizations would have their packet analysis appliance hosted centrally in their data center. However, referring to the two key differentiating factors described in the previous section, airports need to have a different strategy. Since airports have an enormously large network distributed over several areas, with the possibility of isolation of an area, it is recommended to have the ability to perform network forensic analysis at the affected area, even if it is disconnected from the main data center.



Such an ability could only be possible by having a portable network forensics kit to do an on-the-spot analysis on an on-demand basis. This portable kit could also be helpful in situations where the main packet analyzer appliance in the data center malfunctions, or incurs an internal connectivity issue with the rest of the network. The beauty of a portable kit is in the flexibility to carry it on to any field location with the ability to instantly plug it on any network segment, without needing a power source. That is, the kit should be ready to hit the ground running.

For forensics analysis on an on-demand basis, a portable kit can be built using the following 3 things:

1. A laptop

The first thing you would need is a laptop with the right specs for a network forensics job. A memory of 4GB, storage (SSD) of 500GB, a network card of 1Gbps, a USB 3.0 port, and a battery backup of 3 hours, are the bare minimum. Most modern laptops today already come with these specs. A key point to remember is that this laptop should not be a common machine under routine use by the IT team, as that would mean lots of applications installed on it, with significant registry changes and memory load, resulting in slower performance. Rather, this laptop should be a specific machine dedicated for special purposes, such as forensics analysis.

2. A packet analyzer

Next, a packet analyser (also known as packet sniffer) would be required, which is a tool (software or hardware) that can log, parse, and analyse traffic passing over a network. As data flows over the network, the packet analyser receives the captured data packets and decodes the packet's raw data revealing the values of various fields in the packet (e.g. protocol headers, session details, etc). There are various open-source packet analysers available, out of which WireShark (software) is the most popular, and free too. It has a GUI front-end with integrated filtering options which are really useful to sort through the packets in less time. Any other commercial packet analyser tool can also be used.

3. A portable network TAP

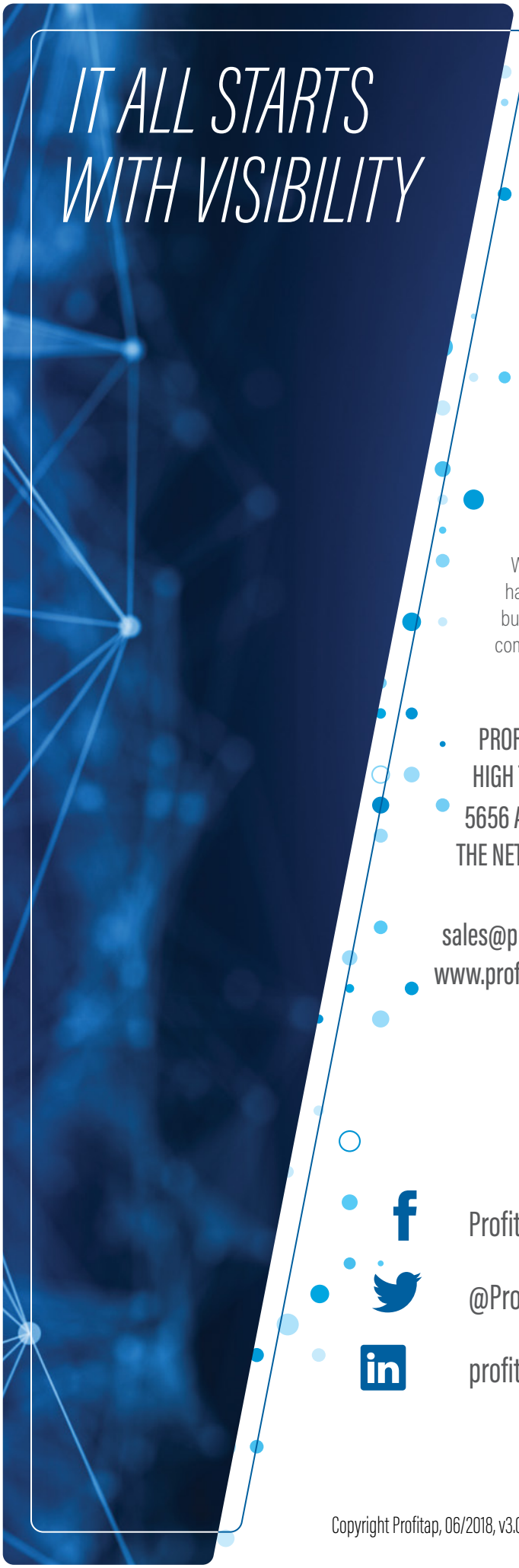
For packet analysers to work, a packet capture mechanism is required for intercepting and capturing packets from the live traffic. This is done by 'tapping' into a network segment by installing a network TAP. TAP technology has evolved rapidly since past few years. Amongst the various types of TAPs available today, portable TAPs are fast gaining popularity due to the flexibility to carry them on the field and deploy them instantly at any location. They easily hook up to your laptop, and with a tool like Wireshark installed, your laptop turns into a portable kit ready to dig into any network forensics job.

Most manufacturers have their own variety of portable TAPs. However, not all of them are as good as they may sound. Some of them are powerful but complex as well to handle without being truly portable. They require a lunch-box PC to connect with additional configurations to be done. Thus they are not truly portable in the first place. While others are easy to deploy, they are not powerful enough to capture the full traffic – they either drop packets while copying to the laptop, or mess with the timing of those packets. This fails the original purpose of the packet analysis activity – missed packets or messed timing is not going to help. A portable TAP that is powerful enough to take on the full traffic – copies every packet without messing the packet's timing – and yet easy to deploy on the field fast enough, is the right tool to have.

THE BEST PORTABLE TAP FOR CRITICAL IT OPERATIONS

Meet ProfiShark 1G – the world's best, fastest and truly portable network TAP ready to hit the ground running for any kind of packet capture in any field location. ProfiShark 1G is pocket-sized and yet powerpacked. It works as an all-in-one packet capture tool without the bottleneck of any packet drop or time delay. With the 2 x Gigabit network ports, it easily combines the two traffic streams to transport over a single monitoring port. It does not use a Gigabit NIC as the monitoring port. Instead, it utilises the power of USB 3.0, which can transfer data at up to 5 Gbps. Hence it can easily transport 2 Gbps of aggregated traffic stream (1G from each direction) over a USB 3.0 link. This means that the buffer memory doesn't need to drop any packets and doesn't have to store packets long enough to impact its timing. And because it can easily connect to your laptop's USB port, the best part of the plug-&-play ProfiShark 1G is that it is not dependent on an external power source. Combined with a laptop, you have a truly portable network forensics kit ready to use at any location without depending on a power source. All packets are captured in real-time with nanosecond time-stamping at hardware level on each packet as it enters the TAP. This allows real-time analysis of captured traffic with nanosecond resolution.

Thus you can rely on this handy tool for any kind of on-demand network forensics analysis job, especially in times of security crises. ProfiShark 1G is your new sidekick to assist in critical IT operations at airports to ensure that passengers and flights reach their destinations on time. If you are interested in meeting your new sidekick and seeing what it can do for you then please contact us or visit our website for further details.



IT ALL STARTS WITH VISIBILITY

PROFITAP

Profitap develops a wide range of state-of-the-art and user-friendly network monitoring tools for both SMEs and the enterprise sector. Our wide range of high-density network TAPs, field service troubleshooters and network packet brokers are extremely performant, providing complete visibility and access to your network, 24/7.

We've been creating monitoring solutions for network analysis and traffic acquisition for more than 33 years. Therefore, we are experts in our field and our award-winning ProfiShark® 1G stands to prove it. This lightweight, advanced and portable network TAP is one the most innovative products on the market.

With more than 1,000 clients from 55 countries, PROFITAP has become a must-have solution for many important businesses, many of which are among Fortune 500 companies.

PROFITAP HQ B.V.
HIGH TECH CAMPUS 84
5656 AG EINDHOVEN
THE NETHERLANDS

sales@profitap.com
www.profitap.com

Profitap

@Profitap

profitap-international