SenseCy on Ynet

In late July and early August 2013, a Gaza-based hacker group named "Qods Freedom" launched a cyber-operation against Israeli websites. The attack comprised distributed denial-of-service (DDoS) attacks, website defacements and attempted bank account breaches.

The DDoS-affected sites were Israel Railways, El Al (Israel's national airline) and a leading daily newspaper. The attacks were all effective, topping at about 3.2 Gb/sec, rendering the sites inaccessible for many hours.

The group defaced over 600 sites, most of them related to two hosting service providers (likely to have been compromised). The defacement messages suggest that the motivation for the attack was to commemorate "Quds Day" – the last Friday of Ramadan.

The group did not attempt to conceal its actions. Quite the contrary – it has an official Facebook page and Imageshack account where it posted images purportedly depicting the breach of Israeli bank accounts.

The political affiliation of the groups seems very clear – hardcore Palestinian, anti-Israeli. This was also evident from pictures they posted on the defaced sites that included images of the Dome of the Rock, the Palestinian flag, footage of protesters skirmishing with IDF soldiers and a portrait of Hezbollah leader Hassan Nasrallah and a quote from his famous "Spider Web" speech, which he delivered in southern Lebanon in 2000 (where he predicted that Israel would break apart like spider webs in the slightest wind).

After the attack subsided, several cyber intelligence analysts at SenseCy, a Cyber-Intelligence company, decided to take a closer look at the actions of this so-called Palestinian group. Gilad Zahavi, Director of Cyber Intelligence, recounted: "Something just didn’t add up. We were seeing many indications that this group was not what it portrayed itself to be, so we decided to dig deeper."

This is a good time to pause and explain what cyber intelligence is. Cyber security, focused on the protection of IT systems, has been around for decades - almost since the inception of the first computer virus. Over time, organizations have realized that cyber security has two facets – the technological one, including all the software and hardware components designed to defend the organization (antivirus, firewalls, etc.); and the procedural one, including permission management, password policy and best practices (like the ban on surfing Facebook on some networks).

Following several severe security breaches, organizations have recently come to realize that a third component is also required – intelligence. One could say, metaphorically, that organizations have built such high (fire) walls around themselves that they are unable to see the threats in their midst. Cyber intelligence fills this void by looking OUTSIDE of the organization and assessing and providing alerts pertaining to imminent threats to the organization. Not surprisingly, this requires the implementation of tradecraft used in "real" intelligence operations. One popular method adopted from the military intelligence paradigm of Signal Intelligence (or SIGINT) involves collecting electronic signals, interpreting them and deciding which pose a threat.
The "Internet" way of doing this is to use automated search engines to "trawl" the web, detect computers generating SPAM email or distributing malware, and try to block their access to the IT infrastructure of the organization, before they manage to penetrate it. But even though these means are employed by all major antivirus and cyber security vendors, they still lack the ability to provide advance identification of the culprit or target.

In most cases, it does not help much to identify the source of the attack after it has transpired, since hackers are very good at covering their tracks and usually launch the attack via remote computers or gateways, which they sometime control without the knowledge of the owners (Botnet).

But a new breed of cyber intelligence experts is taking a different approach, one similar to an age-old, tested and proven methodology – operating agents (aka Human Intelligence, or HUMINT). The only difference is that these analysts operate virtual, not real life, assets. This enables them to "manufacture" agents as needed, according to the target audience.

Need access to a password-protected Russian hacking forum? Create Sergey.

Need to befriend an Islamic hacker group? Create Ahmed the Hacker.

So, going back to the guys from Gaza – Gilad's team set out to investigate. The team comprised ten analysts from intelligence backgrounds who are proficient in different languages relevant to the cyber arena (for example Arabic, Farsi, Turkish, Chinese, Russian, Spanish and other European languages), and with extensive experience in investigating such incidents.

Using virtual entities (some of which have been in operation for some time, and are used to collect information on the vibrant hacking scene in Gaza), they started sniffing around on Palestinian forums and social media groups, but no one seemed to know much about this group. With little else to do, the team looked again at the "signature" the group left after defacing one website. And there it was – a very uncharacteristic typo in the transcript of Nasrallah’s famous speech, one that no native Arab speaker would make. This raised suspicions that this group might not be Arab at all. A closer look at the font used to type the message confirmed that it originated from a Farsi-language keyboard.

Focusing on the Iranian connection, the team uncovered several other indications of the true origins of the group. For starters, "Quds Day" is mostly celebrated by the Iranian government and Hezbollah, not by Palestinian Sunnis. Secondly, the only references to these attacks (anywhere in the Muslim world) have come from the Iranian media. Two additional Iranian groups, "Iranian Data Coders" and "Persian Flag Guards" use the same defacement signature, indicating at least some affiliation to Iranian cyber groups. The last telltale sign was that Iranian hacker groups often choose to masquerade as Arab hackers, choosing Arabic instead of Farsi names. A notable example is the "Izz ad-Din al-Qassam Cyber Fighters", perceived to be linked to the Palestinian Hamas organization, but in fact operated by the Iranian regime.

So there you have it – an Iranian group with high technical capabilities, masquerading as a Palestinian group and attacking Israeli sites. This scheme was uncovered not by fancy
computer forensics but by good old-fashioned intelligence work, built on linguistic and cultural expertise, combined with a deep understanding of the cyber domain and intimate knowledge of the Middle East hacking scene.

The investigation of post-event incidents is only one of the many uses of cyber intelligence. Using the same skill set, SenseCy infiltrated numerous hacker groups and was able to issue an alert BEFORE any hacking operations transpired. Naturally, such a preemptive alert, issued days or weeks prior to the actual attack, can be invaluable to the defender. One hour of service denial can cost businesses up to $20,000 (by industry estimates). Mitigation methods can also be quite expensive. So knowing when an attack is planned, how many participants intend to partake, and which tools they will use – are all highly important pieces of information for the defending organization's IT team, who can then fine-tune their defensive mechanisms and save valuable resources.

Sometimes, no matter how great the security standards of an organization, something extraordinary happens that put their customers' information in jeopardy. Such was the case in late 2013, when the retail giant Target was breached and over 100 million customer details were stolen. This type of stolen information usually ends up on the "Russian underground", a generic name for a multitude of websites operated by Russian organized crime and hacking groups, some of which reside on the infamous "DarkNet", which has become THE marketplace for anything cyber.

SenseCy analysts are very familiar with this dynamic world, and operate dozens of virtual entities on numerous platforms – hacker R&D forums, stolen credit card trade sites, malware development and trade forums, "Hacker-for-hire" sites and many more. Soon after the breach was made public, SenseCy analysts set out to uncover who was selling this huge quantity of credit cards. Within days, new credit card trade sites (or simply "carding" sites as they are known in underground jargon) sprang up, offering the goods for sale: credit card details complete with CVV codes and user details, just waiting for some criminal to embed them on naked (or white) credit cards and use them for all sorts of credit card scams around the world.

The main problem is that these sites are not listed anywhere – they are not indexed by search engines and many are password-protected (which makes them almost invisible to search engines and automated crawlers) – so access is restricted to members only. Employing some of our more established entities in the Russian sphere, entities that have been operating for years and have built up considerable reputations, SenseCy's Russian analysts were able to identify one such platform and register to it. After the initial login, we detected an EBay-like website, with an appealing user-interface, where the buyer can easily filter the "goods" according to country, bank or credit issue name, etc. From there on, it was a piece of cake to identify which cards belonged to SenseCy clients (or clients' clients) and notify them so they could cancel or block them. A closer look at one of the forums revealed how the details were stolen, employing Point-of-Sale (POS) malware, which is used to copy credit card details from the point of sale (cashier’s device) and store them, and later dump them on a remote computer. Such malware is frequently developed and sold on certain platforms, and with advance knowledge, combined with appropriate patching of their
systems, customers can avoid such Target-type attacks in the future. Whenever possible, SenseCy analysts acquire malicious malware and conduct technical research on it, for analysis and to provide additional technical information to our customers.

Identifying the huge, growing demand for cyber intelligence, SenseCy is now expanding both its personnel and technical capabilities, adding cyber experts to its veteran cadre of intelligence specialists. Aiming to offer services to a much larger customer base, SenseCy is increasing high-end tailored services in the form of cyber intelligence feeds. These are already provided to large banks, the stock exchange, shipping and aviation companies and international corporations, and customers can subscribe to on the SenseCy website and enjoy up-to-date intelligence.

"We believe that even intelligence that is not customer-specific is relevant" says Assaf Keren, SenseCy Co-Founder and VP Cyber Solutions. "Even if your name was not specifically mentioned as the target of an attack, the minute someone offers a piece of software that can penetrate your defenses for sale, your threat level rises and you need to act fast."

We believe that awareness levels are extremely low, especially among the general (non-IT) population, but also within higher management. To this end, to complement our intelligence services, we also offer intelligence-based training, both for C-suite and IT professionals. Lessons learned from real cyber incidents, highlighting the unique manner in which your organization is perceived by the attackers, allows managers to make smart, informed decisions about IT purchasing and policies. It is much better to be aware of the real threats and not act out of ignorance and fear. Cyber is no longer "the IT guy's problem" -- it is a challenge for all organizations, and everyone in the organization should understand this and act to resolve threats.