INSIDER THREAT AND COMPUTER SECURITY: IS THERE A SPECIFIC PROFILE?

OLIVIER FICHOT
Radioprotection and Nuclear safety Institute (IRSN)
Fontenay aux roses, France
Email: olivier.fichot@irsn.fr

Abstract

Insider threat in nuclear facilities is a well-known threat, however is there specificities related to insider threat in computer security within these facilities? The paper intend to demonstrate through real life examples that unskilled insiders with the right physical access to network or terminal devices represent a real danger if they act with malicious computer security experts outside the facility. Two criteria should be considered: the physical access and the possibility to established a covert communication channel between the outside team and the tool left behind by the insider.

1. INTRODUCTION

For the infosec community, insider threat is a “buzz word” which covers several different meanings and a wide range of actions, from clicking inadvertently on a malicious link in an email to plugging an infected USB thumb drive on a computer or hiding a wireless enabled raspberry pi connected to the network. The Insider threat is indeed mostly feared because it can come from any trusted individual working for the targeted company and hit deeply inside its organization with considerable consequences.

Indeed, how fearful is the insider threat? Could anybody really harm a computer network from the inside? To fight an insider threat efficiently, it is important to characterize with precision the different approaches of such a threat. The first question that comes to mind, does a malicious insider targeting a computer network has a specific profile, is an evaluation of his/her competence and background a criterion to consider when trying to detect this individual and identify specific ways to protect the system?

In the first part, a definition is given of an insider threat in computer security, afterwards this will be narrowed down to the nuclear field and the IAEA definition. The second part, draws attention to the fact that an individual coming from the computer and network specialist community is obviously one of the main profiles, nevertheless other insider profiles should be taken into consideration in the case of a targeted attack. An in depth analysis of a specific attack showing why and how an insider is needed, helps to identify, which parameters are relevant to describe the insider threat and how to mitigate this threat.

2. INSIDER THREAT, COMPUTER SECURITY AND NUCLEAR FACILITIES

Today, the insider risks in relation with the IT industry are increasing considerably. Since 2016, the average number of incidents is growing and the threat is more and more taken into account. For example, certain companies in energy & utilities incurred average costs of $10.23 million due to malevolent insider cyberattacks beyond other consequences. The definition of an insider threat is however very broad and covers various insider profiles. In their 2018 report [1], the PONEMON Institute defines the insider as: “a careless or negligent employee or contractor, a criminal or malicious insider or a credential thief”. Most incidents are caused by insider negligence (64%) however 23% of the serious attacks [2] are linked to criminal and malicious individuals working for the targeted company even as subcontractors.

Knowing this, let’s narrow it down to the nuclear security field. IAEA has defined the insider threat in the Nuclear Security Series nr.8 [3], the agency’s implementing guide related to Preventive and Protective Measures against Insider Threats, as “an adversary with authorized access to a nuclear facility, a transport operation or

sensitive information". Which means that the threat is coming from an individual voluntarily and purposely acting to cause damage to a nuclear facility or transport.

Of course the IAEA definition encompasses all types of physical actions and can therefore be applied to the computer security domain as well: many functions in nuclear facilities are now digitalized, especially the Physical Protection System (PPS) which relies mainly on digital network, and Instrumentation and Control (I&C) of nuclear facility processes which are also computer driven. Computer networks are indeed natural targets, either for espionage or sabotage. The IAEA definition is close to the already mentioned PONEMON definition of the malicious or criminal insider or the well-known National Institute of Standards and Technology (NIST) definition [4]. The cyber malevolent insider can thus be considered as an adversary with authorized access to the information system inside a nuclear facility.

3. WHO IS THE MOST DANGEROUS INSIDER ?

3.1. IT specialist

Computer networks in a nuclear facility are often very complex and extended. Member States effort to strengthen security and the increasing awareness concerning cyber threats have had positive outcomes and in this sensitive domain, computer networks have implemented basic and efficient security measures: segregation, compartmentalization, careful administration have considerably hardened the networks. Another security layer that is often found is "airgap" networks, where networks are physically isolated from other networks. In that case, creating a significant impact, like a major denial of service, extraction of sensitive data or takeover of the industrial process, can thus be tricky and difficult for a malicious actor, especially from the outside of the facilities. The remaining threat lies thus inside.

By an insider threat, the small "club" of IT specialists, network administrators or architects, maintenance engineers or computer security engineers, working for or in the targeted facility, have the knowledge and the skills to perform such attacks, they are even able to operate alone and could carry out an entire attack by themselves, and they form therefore the most dangerous insider profile.

But they are not the only ones, by far.

3.2. Unskilled individual with the right physical access

Considering indeed critical infrastructure such as nuclear facilities, targeted computer attacks, often named APT (Advanced Persistent Threat), are a major threat and as defined by the NIST, the advanced persistent threat [5]:

(a) pursues its objectives repeatedly over an extended period of time;
(b) adapts to defenders' efforts to resist it; and
(c) is determined to maintain the level of interaction needed to execute its objectives.

In the above mentioned scenario, another type of malicious insider must thus be considered: an individual who will have a very limited role in time and should be able to execute one and only task, often not a technical one (Fig1), in relation with an organized and experimented team acting outside the facility, behind the anonymity of internet. This individual is never the scientific and technical brain of the operation.

Fig 1 A custom wifi enabled raspberry pi inside an anonymous plug (credit: Europol)

This type of insider threat involving an unskilled individual has already been highlighted in different case studies by analysing TTP's (Tools, Tactics and Procedures) of cyber-attacks. For example the security company Kaspersky has been investigating a series of attacks, named "Darkvishnya" [6], on eastern European banks which caused damage with an estimated amount of about tens of millions of dollars. Each attack had a common springboard: an unknown device directly connected to the bank's local network. The first stage of the attack consists in a cybercriminal entering the organization's building posing as a courier or a job seeker connecting a device to the local network, sometimes hidden or blended in the surroundings in order not to arouse suspicion. The devices used in the Darkvishnya attacks were a netbook or a cheap laptop, a raspberry pi or a "bash bunny" (special USB HID tool).

4. THE ROLE OF AN INSIDER WITHIN A COMPLEX TARGETED CYBERATTACK

As for the above mentioned example, by an APT the targeted attack is executed by a team of malevolents, each specialized in a different field of computer security: hacker, network, windows or Linux specialist, retro-engineer, social engineer etc…, the brains of the operation. They will try to gain entry by any means in the targeted network and from there, will discreetly study it, execute reconnaissance and adapt their attacking tools to gain better logical access until they reach their goal and strike. These attacks planned over a long period of time are interactive, which means that the attackers are continuously interacting with the tools which they have placed inside the targeted network in order to understand how the system works and how to achieve their goal.

When confronted with an physically isolated (named "air gap") or a very well hardened network, the malicious group will encounter difficulties to penetrate the outward perimeter, they will thus tend to leverage an insider not necessarily skilled to access the targeted network.

This insider will be used by the main team waiting discreetly and anonymously outside only because he has a physical access to the network and is able to plug a device which will allow the team to establish a communication channel with the network.

In that case, the insider has just a very basic and one-time role to play, namely to plug a device (Fig 2) or execute one single action, the rest of the attack is conducted from elsewhere thanks to the remote connection and the malicious team will then proceed to the next steps of the attack by escalating privilege and moving laterally until they reach their ultimate goal (sabotage or espionage).

Fig 2 A computer mouse trapped with a malicious HID device

5. CHARACTERIZATION OF THE INSIDER THREAT IN COMPUTER SECURITY

5.1. The insider himself

When analysing the role and the profile of the insider in this type of sequential targeted computer attack, certain parameters are to be considered:

- The insider has a limited role in the operation but nevertheless extremely essential in order to access the targeted network, at least once.
- The insider doesn't need to be scientifically and technically skilled to carry out the requested action. In fact, the individual can be a cleaner, a delivery man, a visitor or a mechanical technician.
- The insider just needs to have a physical access to a network device, and logical access is not essential but might be potentially useful. The device used by the individual could be an endpoint, switch, firewall…. or a simple Ethernet plug.

5.2.1. The insider's tools

The tools an insider could use are numerous and they cannot be exhaustively listed. However, they can be divided in 3 types, it could be either:

- a software if the insider has the right logical access to the system,
- a USB connected device, like a malicious Human Interface device (HID). The device is plugged into the targeted system via USB and communicate with the outside through a covert channel,
- a connected microcomputer like a raspberry Pi. The device is plugged into the system via Ethernet or Wi-Fi and communicate with the outside through a covert channel.

All these tools need to communicate with the outside malicious team which will continue the attack and thus a communication channel should be established

Network connections and internet are privileged channels for a malevolent adversary to lead the cyber-attack, nevertheless technological progress in the fields of protection devices like firewalls, private VLAN and Intrusion Detection System (IDS) have made more and more difficult to use these channels, especially if they are monitored by a Security Operation centre (SOC). Moreover, airgap protection, often use in sensitive network like nuclear power plant instrumentation and control is an obstacle which will lead the attacker to use a covert channel.

These covert channels are very diverse: Wi-Fi or GSM radio frequencies are some possible exploitable channels but other “exotic” ways could be used, like powerline communication, ultrasound or LED lights. In these cases, attackers should control components of computers inside the targeted network

Awareness should thus be raised around these malevolent methods and practices despite the difficulties and the variety of the existing communication channels.

To sum up, in addition to make the attack work apart from insider involvement with a physical access, there should be a possible communication channel between the tools implanted by the insider in the targeted network and the outside world. Generally speaking the adversary has no exhaustive knowledge of the targeted system and is therefore not able to program an autonomous malicious code (unlike Stuxnet which is a counter example). This is the reason why the opponent needs to communicate with the tools.

To counter this type of threat, physical protection on network devices and logical network access control mechanisms are essential, in conjunction with surveillance of possible covert channels.

6. CONCLUSION

Never assume that the insider threat comes necessarily from a person with an extensive computer and network knowledge or with exhaustive access rights such as for example computer specialists. It should be stated that there is no specific profile defining a malevolent insider, which increases the level of complexity by the detection and prevention of insider threats in computer security.

In the context of APT attacks, it’s essential to protect the infrastructures against this type of unskilled malicious insiders, who can cause severe damages, in conjunction with an experimented team outside. As already mentioned, they are difficult to detect, the only criterion to consider for defense is their potential physical access to network devices, for example endpoints, switches, firewalls or Ethernet plugs.

Measures described in IAEA Nuclear Security Series nr.8 (NSS.8), the agency’s implementing guide for Preventive and Protective Measures against Insider Threats, are the ground principles to prevent, detect or delay an insider, including in the cyber field, and they should be complemented by certain technical computer security measures like network access control and a strict physical protection of the network devices and plugs.

REFERENCES

[1] PONEMON INSTITUTE, 2018 Cost of Insider Threats: Global, (2018)

[2] Ibid.

[3] IAEA, Nuclear Security Series N°8, Implementing guide, Preventive and Protective Measures against Insider Threats, Vienna, 2008

[4] NIST, https://csrc.nist.gov/glossary/term/insider-threat

[5] NIST, https://csrc.nist.gov/glossary/term/APT

[6] KASPERSKY, https://securelist.com/darkvishnya/89169/