ENISA Flash Note

FN01_2013 [2013/03/13]

Cyber-attacks – a new edge for old weapons

The EU's cyber security agency ENISA has analysed recent major cyber-attacks and is calling for Europe's businesses and government organisations to take urgent action to combat emerging attack trends. These are characterised by old attack methods, being given a new edge because they are being used in a smarter, more targeted way.

As reported in the media, there has, in recent weeks, been a series of targeted cyber-attacks directed at high-profile targets – government and operators of critical infrastructure:

In the last days of February, the MiniDuke cyber-attack was discovered by Kaspersky and Crysys affecting users in governmental organisations across the EU. The news came only weeks after Mandiant published its report about a range of cyber espionage attacks, involving the theft of terabytes of data from hundreds of organizations, including operators in the EU's critical sectors. Another cyber espionage attack, known as Red October, was discovered in January of this year and is said to have been targeting governmental and diplomatic organisations across the globe for several years.

These **targeted attacks** follow a common and well-known pattern. Attackers send an apparently genuine email, which is in fact a **spear-phishing** attempt. The email contains a link to an internet page containing malware, or it contains a maliciously prepared attachment. The malware is able to exploit **software vulnerabilities (in the case of Miniduke a flaw in Adobe's Acrobat reader)** to allow the attacker to gain sufficient control over the target and to start gathering intelligence. Often the attacker uses the intelligence gathered to attack other victims or other machines in the same organization (this is sometimes called 'lateral movement'). This technique was also used in targeted attacks aimed at financial fraud – e.g. the cyber-attacks on online banking called High-roller.

Concerning these recent attacks, we would like to highlight the following points:

- **Cyber-space has no borders:** There is much discussion in the media about who is behind this or that attack. Cyber attackers operate across borders and attackers can easily operate across continents. It should be stressed that attribution of cyber-attacks is in general difficult. In

cyberspace it is very easy to wipe traces or to create fake traces. This severely complicates identification of the attackers, and makes prosecution highly problematic. The fact that one or more computers used in the attack are located in one country does not mean that the attack originates from this location. For example, it is not uncommon to see attackers hijack the botnet infrastructure of other attackers, for their own purposes.

- **Common attack methods**: The attacks use a combination of two attack methods. 1) An innocent looking spear-phishing email, which to the victim seems like a genuine and harmless email. Sometimes attackers create webmail or social media accounts using names of colleagues or they spoof the sender address of the email completely. Cyber-attackers use this method because it is of low-cost, easy to launch and very effective. 2) A software vulnerability which is used to take control of the victim's machine. Some investment is necessary to obtain information on latest vulnerabilities (i.e. as close to zero-day as possible).
- **Failing security measures:** Many organisations have phishing filters and antivirus products. However, these measures do not seem to be always working when attacks are performed over a long period of time. Phishing filters and anti-virus products can protect organizations from certain large-scale attacks, but there are many ways for attackers to stay under the radar. The attacks discovered recently had gone unnoticed for years probably because attackers were targeting few victims, making sure antivirus companies did not easily spot them. It is possible that recently reported incidents and detected attacks are only the tip of the iceberg.

As said, it is inherently difficult to identify the origin of attacks in cyber-space, and this will leave room for discussions in the media about who did it. Regardless of the origin: The impact of these cyber-attacks was very high and the attacks show critical vulnerabilities in the defences of organizations against such targeted attacks. It is important to address these vulnerabilities and we would like to make the following three recommendations in this regard:

- **In cyber-space, prevention is key:** If targets are unprotected, their weaknesses are going to be exploited by adversaries, regardless of their origin and motives. Prevention (ex-ante) should be the primary defence against attacks. Prosecution (ex-post), after the attack has succeeded. may not be possible in all cases.
- **Email is insecure:** E-mail is universally used, by consumers, businesses and government organizations, but most email systems do not provide any kind of authentication, i.e. it is very hard for users to understand where the message originates from and whether or not the sender is a trusted party. This makes it is very easy for attackers to send fake messages or to pretend they are someone else (spoofing). In the short-term, organisations in critical sectors should mitigate by using encryption solutions (like PGP/PKI) and/or sender authentication frameworks (like DMARC, SPF, DKIM) to avoid becoming an easy target of spear-phishing. In the long term, industry, government and businesses should investigate alternative communication channels which better protect users from spoofing or phishing.
- **Software vulnerabilities:** There are trade-offs between software features and software security. The more features and interoperability features software has, the more difficult it is to ensure that the software is free of vulnerabilities. There is a similar trade-off between convenience and security: the easier it is for users to access confidential data or critical systems, the higher is the impact when the devices of these users are compromised. Organizations and businesses should proactively reduce the attack surface by reducing the complexity of software installed on user devices and reducing the permissions of users to access other devices, services and applications by applying the principle of least privilege.

Concluding we would like to highlight the importance of the recently published European Cyber Security Strategy which provides a roadmap for enhancing prevention against cyber-attacks and failures while setting important cornerstones, for example regarding incident reporting, collaboration among European cyber security organisations and education of users to better address cyber security threats.

****

For more information, please contact:

Graeme Cooper, Head of Public Affairs, on +30 6951 782268 or Dr Louis Marinos on +30 6948 460123 email: press@enisa.europa.eu