ONGC 197 CR. FRAUD: HACKER USING APT FOR CYBERHEIST

International business trade is facing an unprecedented threat of frauds from organized crime, particularly, an intelligent, knowledgeable group of hackers and recent fraud with ONGC is one of the crime involving huge amount of Rs. 197 Cr. Such scams earlier known as Man-In-the-Email Scam now involves sophisticated modus operandi and targets businesses working with foreign suppliers that regularly perform wire transfer payments. Cyber Crimes have become lucrative with a high returns coupled with low risk and as such the hackers have become very focused and motivated. They are not in hurry to launch and attack quickly but act in a slow and steady but aggressively and successfully penetrate the network with various different attack methods and then, clandestinely hide its presence while achieving a well developed, multi-level foothold in the environment.

The fact of the case as revealed from various news in the media indicates that the commercial transactions regarding sale of naptha between ONGC and Aramco, a Saudi Arabia based Oil Company were exploited by the hackers to commit Cyberheist crime involving the misappropriation of the highest money so far in India. The ONGC aggrieved to deliver 36,000 ton of naptha to Aramco for Rs. 100 Cr. and communication on behalf of ONGC were being carried out from email address 'patel_dv@ongc.co.in. The company did not get the money for the consignment on time and on enquiry, got the response on the email that the payment has been delayed due to public holiday and meanwhile, the company has also delivered the second consignment of naptha worth of Rs. 97 Cr. to Aramco. Later on, the company came to know from Aramco that the money have been transferred to Bangkok Bank Public Company Ltd. on the request of ONGC which has been received from email id patel_dv@ognc.co.in. The said account in which the money was transferred does not belong to ONGC nor the ONGC has sent any request.

The first phase of the attack requires the hacker to identify the target entities and the access to the commercial transactions which may become soft target for cyberheist fraud which is done through phishing. Through phishing, the hackers identifies the potential and soft targets and for the purpose of phishing the hackers may use various techniques such as spoofed emails, deceptive URL, URL Obfuscation, Link Manipulation, DNS Based Attack, Malware Based Attack, Content Injection, SQL Injection & Cross site Scripting etc. The information based on the successful compromise of the targets are analyzed and the targets are identified.

In the second phase, after identifying the target, hackers collects the complete information of the entities involved, authentication details as well as systems and designated employees as such crimes require update and continuous information of the transactions. For this purpose, Remote- Access Trojans are used which will install itself, in such a way, at the target computer that it would become active every time the computer is started subsequent to the installation. Once a Trojan client, such as W32.Shadesrat, FAKEM, BlackShades, Back Orifice, Netbus, Bionet, or SubSeven, is installed on the target computer, the controlling computer is able to intercept information about the target computer. Through this covered channel the master

computer will be able to download files from and upload files to the target. These crimes are committed by the fraudsters who are highly intelligent and knowledgeable and takes over the communication between the parties and would act as Man-In-Middle. These intelligent fraudsters monitor and analyze the identified targets and protocol necessary to perform wire transfer within specific business environment.

In the third phase, the attackers would execute the attack by either changing the bank details in the invoice which are being sent by the seller to the buyer or would sent a separate mail for change of bank detail to receive the payment from the buyer. At this stage, since sensitivity is high and any suspicion to either of the parties may foil the game plan of hacker, the hacker normally resort to the creation of fake emails so that the seller may not come to know about the change of bank detail and if any query regarding the change of bank detail is raised, the same is also replied by the hacker to satisfy the buyer regarding the genuineness of the bank details.

In the fourth phase, the attackers after receiving the money immediately transfer the money to various other accounts over different jurisdictions and even can convert the same into virtual currencies whereby, through different layering, it is not possible for the investigation agencies to find out the beneficiaries. The money is transferred to the accounts of unwitting money mules who are recruited as a bogus work-at-home jobs and as such these person also become victim of these scams and they receive the fraudulent funds in their accounts and then, directed by the fraudsters to transfer the funds to other jurisdictions.

The offence is scattered in international sphere as the fake email may have been originated from one country, target computer is in another country, funds may have been misappropriated in another country or subsequently transferred to different countries. As the crime crosses international boundaries, the investigation of such complex issues shoots up exponentially and the chances of the criminal been identified, recovery of misappropriated money and prosecution of the criminal decreases. Further, the police may lack the skill to investigate these technical crimes and to find the type of malware with which the system is infecting, source of malware etc. The investigation of such cases requires the analysis of various interdependencies and the information which may be required from various countries. In the absence of any International Treaty to expedite and facilitate the investigation of such crimes and extradition of offenders makes it difficult to bring the case to the logical conclusion. Further, the volatile nature of electronic evidence, different legal systems and lack of cooperation between countries ultimately reduces the probability of detection, prosecution to nullity.

Given the present scenario and the manner in which cyber crimes are exponentially increasing, becoming more and more technical and organized by intelligent criminals, the companies cannot eliminate these threats but it can protect itself by introducing appropriate security mechanism, security awareness, security training and preventing these threats from exploiting vulnerabilities in its environment. The cyber threats have acquired alarming proportion particularly in India due to non-registration of the cases, lack of skill with the police to investigate and absence of forensic capabilities with the law enforcement agencies. The cyber security skills are still being interpreted in terms

of security softwares, forensic hardware/software, firewall etc. and the recent breaches in the case of Sony Hack, JP Morgan, Target etc. have clearly establish that these gadgets would play very limited role in protecting the information security enterprise architecture. The need of the hour is to have strong security structure of the enterprise information framework and to implement preventive model which can be supported by the detective, recovery and corrective mechanism to strength the enterprise security infrastructure. The companies need to include the clauses in the agreement with the parties which can cater to the risk emerging from the cyber threats which are dynamically changing and would require the involvement of information technology expert.

Read Full Story at –

http://www.neerajaarora.com/ongc-197-cr-fraud-hacker-using-apt-for-cyberheist/

Regards

Neeraj Aarora
Cyber Lawyer

http://in.linkedin.com/in/neerajcyberlawyer