Cyber crime and common reaction

Labour intensification, new technologies and modern materials are general parts of business development... The same is true about crime development where labour intensification, new technologies and modern materials are also the general parts.

Modern high-end crime is developing as fast as modern economy and business and independently from our opinion and recognition. While most of small enterprises suppose that they are still far from criminal's interest, giant businesses believe they have impenetrable IT system. Both concepts are proved to be wrong in reality. Cyber crime changes methods and tools after each recognition and discovery. Vulnerability appears in the most protected points sometimes.

Cyber attacks performed by use of advanced technologies are more frequent than the banal property theft, while having much more serious consequences. Luckily, the Russian Federation is far from worldwide leaders in this field, but the number of attacks, as well as losses, real and indirect, becomes more and more significant.

Hundreds of thousands of cases and tens of thousands of recorded crimes occurred over the last 12 months, with the average loss amount per case for corporate market in Russia being around USD 3 to 5 million.

The overall amount of loss for the Russian economy is estimated to about USD 2 billion. Financial companies and industry including the fuel and energy sector are at a major risk.

We are facing the future with such modern trends as:

- A growing total amount of cyber incidents
- An increasing amount of targeted attacks
- A moderate increase in banking phishing
- A growing amount of incidents related to ATMs
- The spread of cyber crimes beyond the financial market.

Evidently, until there is no guarantee against cyber crime, insurance remains an efficient way to mitigate the negative consequences. In order to increase the consciousness of the necessity to insure corresponding risks we have to deliver hot tips to an insured.

The range of attacks that could be undertaken against companies and persons is very wide:

- Non-targeted attacks (phishing, carding, SMS fraud)
- Targeted attacks (financial fraud, database theft, industrial espionage, DDoS attacks, blackmailing)

Dmitriy KHARITONOV, General Director of LABB, loss adjusters bureau

- Internal attacks (theft, destruction of data, abetting targeted attacks).

Potential losses are also quite different, for example:

- Direct loss (theft of funds, loss of data, damage to software, equipment breakdown etc.)
- Business interruption losses
- Third party liability (for inflicted damage, information disclosure)
- Loss due to industrial espionage or theft of intellectual property
- Reputational losses
- Additional expenses (PR, legal services etc.)

LABB is one of the leaders in providing independent insurance loss investigation and adjustment on the Russian market. Working in cooperation with leading international companies specialising in the prevention and investigation of cyber crimes and hi-tech fraud, LABB offers Pre-risk audit and Loss adjustment services, including the following steps:

Pre-risk audit

- Estimation of risk protection of an object
- Detection of potential threats
- Development of scenarios of the most probable losses
- Recommendations on upgrading the security level and prevention of possible losses
- Drafting emergency response plans
- Identification of the potential effect of cyber incidents on the business processes
- Calculation of financial figures and possible losses.

The risk protection of the target IT system is usually assessed on the basis of an extensive test, which may include:

- Web intelligence of the affiliated net resources
- Automated vulnerability scanning
- Manual exploitation of detected vulnerabilities
- Stress test of critical resources
- Other security tests of different types.

The resulting report includes the conclusion on the protection level of the target company, the description of the risks together with the financial figures necessary to create the most reasonable and efficient insurance coverage.

Investigation and loss adjustment:

- Instant response to emerging threats (suppression, recommendations on loss mitigation measures)
- Investigation of circumstances and cause of the loss, tracing the liable party
- Legal analysis, acknowledgement of an insurance case
- Calculation of the loss
- Assessment of subrogation aspects and assistance in recovery.

Loss adjustment results in a report with recommendations on the loss settlement, which is agreed with the insurance market.

One important issue worth being emphasised is that, as distinct from a wide range of other crimes, cyber frauds can be revealed rather quickly. In many cases the intruders were captured before they had a chance to spend stolen funds. In this context we assume recovery to be a highly prospective issue in cyber insurance, which is to be considered from the very first moment of each loss.

The examples below, being only a small part of cyber crimes in Russia, are provided by our partner Group-IB, one of the global leaders in preventing and investigating high-tech crimes and online frauds.

Germes group

The biggest bot-net in Russia interconnected 4.5 million infected computers. The amount of thefts arranged via the bot-net is estimated over RUB 150 million. The head of the criminal group acting across several countries was found and arrested.

Hameleon group

First bot-net in Russia intended for theft of funds from banking accounts of individuals. The criminals made attacks on banks' clients using counterfeit SIM cards. The head of the criminal group was found and arrested; thefts amounting to over RUB 1 billion were prevented.

Dragon

Inventor of a bot-net for the organisation of DDoS attacks. Several British and Russian companies became the victims of the group including one of the TOP-10 largest Russian banks. The organiser of the criminal group was found and arrested.

Pump Water Reboot

A hacker liable for DDoS attacks on "Tinkoff. Credit systmes", "Alfa-Bank", "Promsvyazbank", "Kaspersky laboratory" and large web-portals. He blackmailed for attacks cancellation. The hacker was found and arrested.