More than 1 billion rubles, 100's of thousands of Credit Cards and vast amounts intellectual property has been stolen by a new group of cyber criminals

'Anunak'

22.12.14 Moscow, Amsterdam -

Group-IB and Fox-IT, in a joint investigation effort, release a report about the Anunak hackers group. This group has been involved in targeted attacks and espionage since 2013. Group-IB specializes in cybercrime investigations and Fox-IT offers innovative cyber security solutions.

Anunak targets banks and payments systems in Russia and CIS countries. In Europe, USA and Latin America criminals were mainly focusing on retail networks as well as mass media resources.

"Anunak" aims to target banks and e-payment systems. Malefactors can easily get into banks networks and gain access to secured payment systems. As a result, the money is stolen not from the customers, but from the bank itself. If malefactors gain access to state institutions' network, the goal is espionage.

When malefactors gain access to internal networks, they have total control over system administrators, record videos of key workers actions to understand how the work is organized. They then take control over e-mails to monitor internal communications and set up remote control to the network by changing its hardware parameters.

Experts discovered that hackers had access to cash machines management systems and could remotely infect them with malware for the purpose of getting money from them upon request in future.

In the report, Group-IB and Fox-IT describe in detail the methods and software that were used by hackers, and the methods and tools that can be used to protect networks and counter targeted attacks.

Some of the report's key takeaways:

- Average theft in Russia and CIS countries for this group is **2 million US dollars**.
- Anunak group had access to more than **50 Russian banks, 5 payment systems, 16 retail companies**. Most of retail companies are outside of Russia, while not a single US/EU bank has been attacked.
- As of now more than **1 billion rubles** has been stolen by the group in total, most of that during the last 6 months.
- Average time from the moment the group gains access to internal network till the money is stolen equals **42 days**.
- Today, the Anunak group is still in operation which is why Group-IB and Fox-IT forecast an increase in the number of targeted attacks in 2015.

"We have seen criminals branching out for years, for example with POS malware," says Andy Chandler, Fox-IT's SVP. "Anunak has capabilities which pose threats across multiple continents and industries. It shows there's a grey area between APT and botnets. The criminal's pragmatic approach once more starts a new chapter in the cybercrime ecosystem."

The report is available here http://blog.fox-it.com/

About Group-IB

Group-IB is one of the leading international companies specializing in preventing and investigating high- tech cyber crimes and fraud. The company offers a range of services on preventing financial and reputational damages, consulting and auditing of information security systems, and on computer forensics. The company also develops a number of innovative software products Bot-Trek used to monitor, detect and prevent emerging cyber threats.

The Group-IB team is made up of experts with unique skills and solid practical experience. They are internationally certified by CISSP, CISA, CISM, CEH, CWSP, GCFA, and also have information security state certificates. In 2013, computer security incident response team CERT-GIB operated by Group-IB became a member of FIRST - Forum of Incident Response and Security Teams.

For more information please contact the PR Department, Group-IB:

pr@group-ib.ru | +7 (495) 984 33 64 | www.group-ib.com

About Fox -IT:

Fox-IT creates innovative cyber security solutions for a more secure society. We are dedicated to our clients, our values, and our integrity. Fox-IT delivers solutions before, during and after attacks. InTELL is our real-time cyber intelligence product. It provides a unique intelligence approach: InTELL gives full real-time insight in the global threat landscape. Actionable data feeds into operational risk decision systems. Real time threat information allows for tactical decisions and mitigation. We base our intelligence around actor attribution. This angle drives the most pro-active way to deal with on online threats. Information is delivered through our collaboration portal, alerting, and through automated feeds powered by STIX & TAXII.

For more information please contact Eward Driehuis:

driehuis@fox-it.com | +31 6 4382 4529 | www.fox-it.com | www.foxintell.com