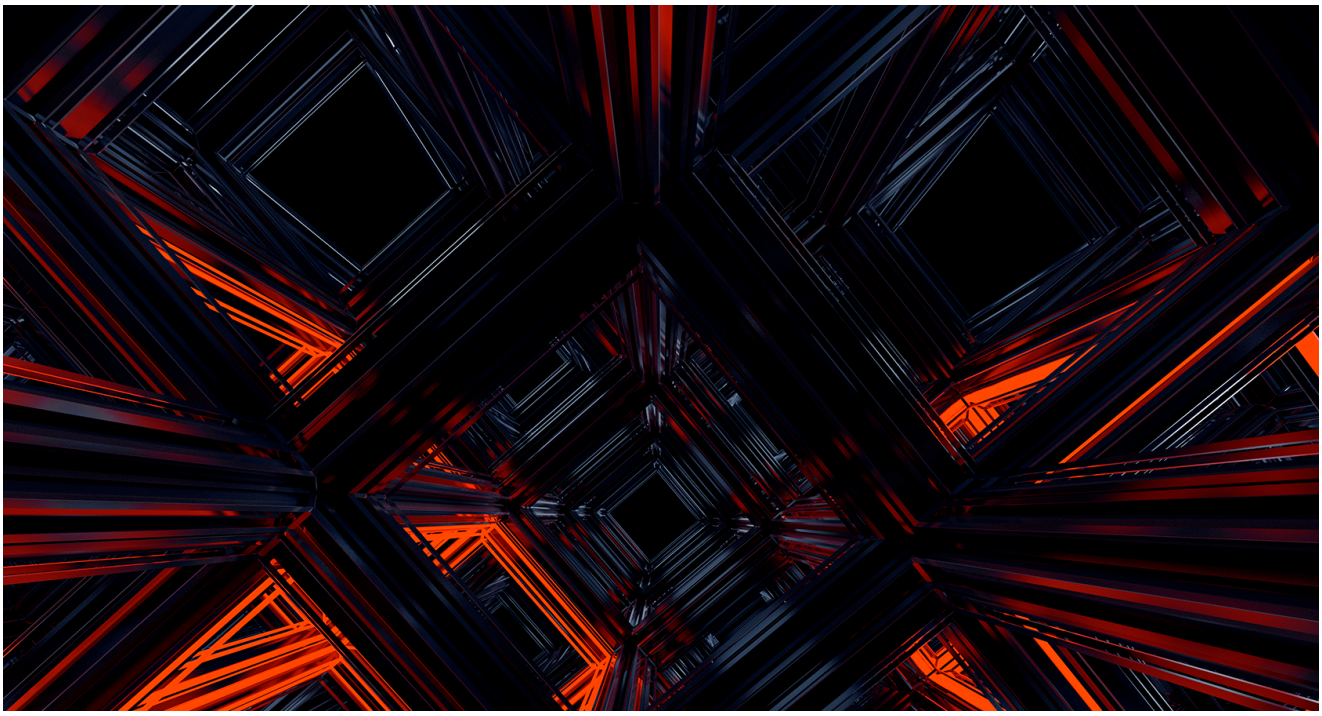
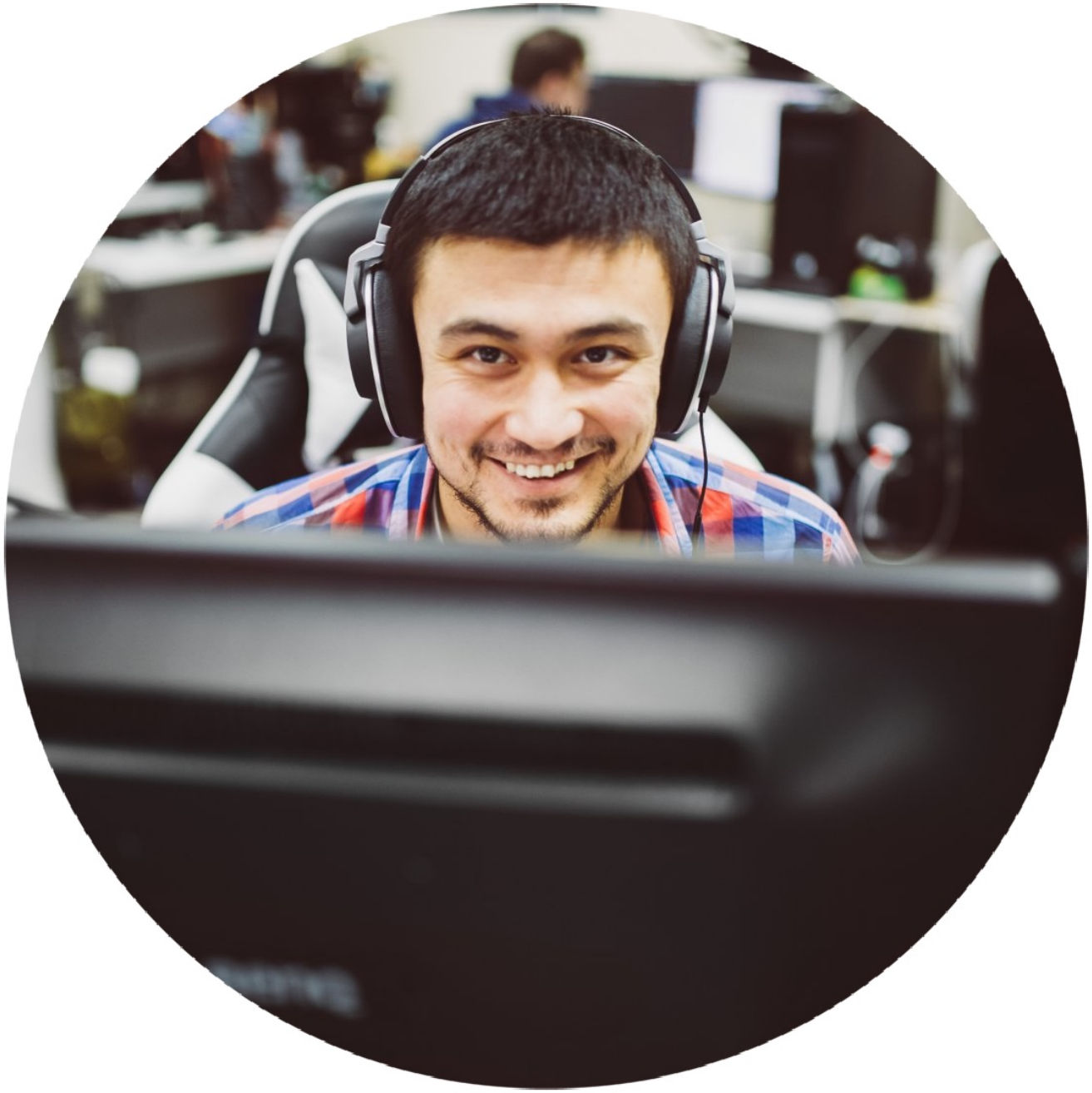
Cobalt Renaissance:new attacks and joint operations

group-ib.com/blog/renaissance



29.05.2018

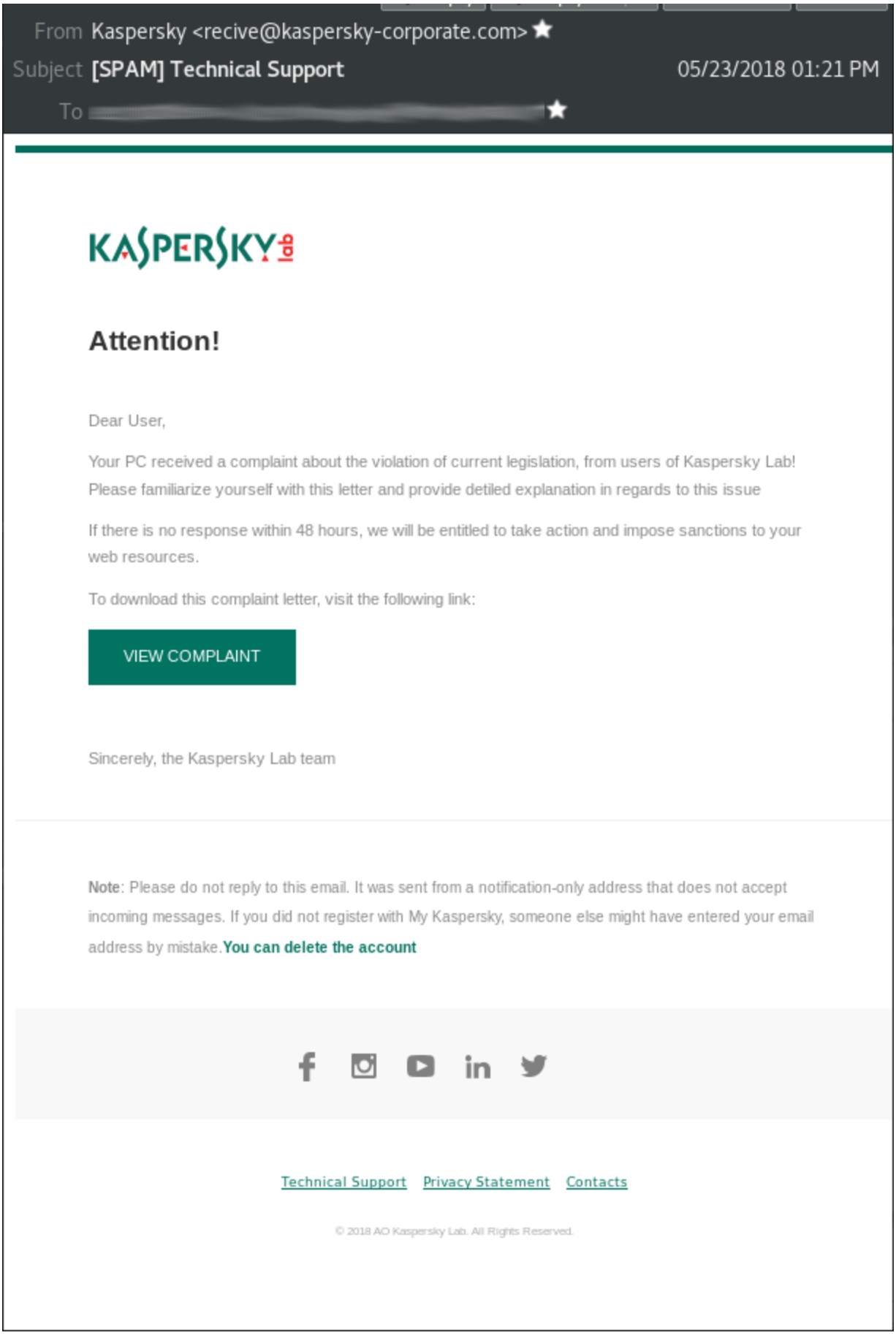


Rustam Mirkasymov

Threat Intelligence Expert

On March 26, 2018, Europol reported the arrest of the Cobalt gang leader in Alicante, Spain. The Bank of Russia named Cobalt as the main threat to banks. The scale of its activities is fascinating: according to Europol, the group has been linked to thefts of approximately one billion euros from 100 banks in 40 countries: Russia, the United Kingdom, the Netherlands, Spain, Romania, Belarus, Poland, Estonia, Bulgaria, Georgia, Moldova, Kyrgyzstan, Armenia, Taiwan and Malaysia. But, in spite of the arrest of Cobalt's group leader, and (a little earlier) that of the head of the money mules group and several of his aides, remaining hackers continue to attack banks. Therefore, it is far too soon to dismiss Cobalt.

On May 23, 1:21 p.m (Moscow time) Group-IB tracked a new large-scale Cobalt cyberattack on the leading banks of Russia and the CIS. It was like a challenge: phishing emails were sent acting as a major anti-virus vendor. Bank employees received a "complaint", in English, that their computers allegedly violated legislation. The users were asked to carefully read the attached email and provide detailed explanations. If a response was not received within 48 hours, the "anti-virus company" threatened to impose sanctions on the recipient's web resources. In order to download the email, the user was asked to follow a link, which would then infect the Bank employee's computer.



From Kaspersky <recive@kaspersky-corporate.com>
Subject [SPAM] Technical Support 05/23/2018 01:21 PM
To [redacted]

KASPERSKY lab

Attention!

Dear User,

Your PC received a complaint about the violation of current legislation, from users of Kaspersky Lab! Please familiarize yourself with this letter and provide detiled explanation in regards to this issue

If there is no response within 48 hours, we will be entitled to take action and impose sanctions to your web resources.

To download this complaint letter, visit the following link:

VIEW COMPLAINT

Sincerely, the Kaspersky Lab team

Note: Please do not reply to this email. It was sent from a notification-only address that does not accept incoming messages. If you did not register with My Kaspersky, someone else might have entered your email address by mistake.**You can delete the account**

Technical Support Privacy Statement Contacts

Group-IB experts found a connection between the emails and Cobalt quite quickly: the unique Trojan "CobInt", which has been in the inventory of the group since the end of December 2017, was involved in the attack. The emails were sent from a domain titled "kaspersky-corporate[.]com. Upon review it was discovered that this domain name was registered by a person with the same name as with previously registered domains for Cobalt attacks.

However, there were peculiarities: the anti-virus vendor name was being used for the first time, and the first wave of emails contained an empty ThreadKit exploit without any payload. Previously, the Cobalt hackers did not make such mistakes. However, after finding the error, the attackers corrected it.

The targets of this cyberattack might not only have been banks in Russia and the CIS: the phishing email was written in English, suggesting western banks as targets. The list of previously targeted emails, which was analyzed by Group-IB experts, contained the addresses of over 80 organizations, including banks, mass media, insurance companies, IT companies all over the world.

Again, the company's experts rate the quality of phishing emails as high, the text in English is stylized as a "legal complaint", the fake website kaspersky-corporate[.]com also has a high level of quality, which is not typical of Cobalt. These and other signs again pointed to the possibility that the remaining members of the Cobalt group were conducting a joint operation with other criminal groups, in particular, Anunak.

Detailed information with technical indicators of the groups' operation is provided in the report "**Cobalt: Evolution and Joint Operations**".
Technical overview

On May 23, 2018, phishing emails were sent from the following mailboxes:

•recive@kaspersky-corporate[.]com

•info@kaspersky-corporate[.]com

•r.levis@kaspersky-corporate[.]com

Subject: "Technical Support"

The kaspersky-corporate[.]com domain name was registered on May 21, 2018, and at the moment it is resolved to the IP address 172.217.22[.]110. Previously, it was resolved to 194.58.112[.]174 and 62.76.40[.]207.

The address of the mail server from which the emails were sent, mail.kaspersky-corporate.com, has an IP address: 62.76.40[.]207.

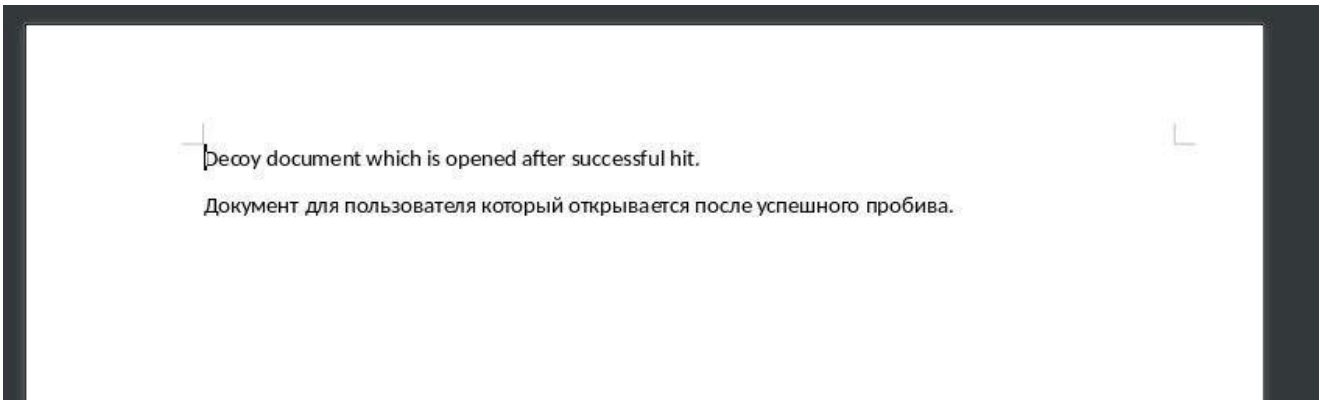
The email contains a link to the Complaint.doc file (hxxps://kaspersky-security[.]com/Complaint.doc). After clicking the link, the user receives .doc exploit, generated by ThreadKit framework.

Complaint.doc

MD5 fa354151a3fc6d0dce69e8eeaa8cd197

Size 192706 bytes

However, the attacker made a mistake and forgot to configure the exploit build, which meant that the exploit was empty and did not install anything in the system. Moreover, the hackers did not change the standard decoy document set by the author by default. After opening an exploit, the error page was displayed.



The kaspersky-security.com domain name was registered on May 8 2018, and is resolved to: 91.230.121[.]86.

Later, the link led to the Complaint.scr file, CobInt.Downloader, which was the usual executable:

MD5 7b55c7ae346efb428aaf63d25ca0fcc7
size 278016 bytes
Compiled on May 18, 2018.

This program, classified as CobInt, is a self-developed backdoor of the Cobalt group. The modular tool has capabilities to collect initial intelligence information about the compromised machine and stream video from its desktop. If the operator decides that the system is of interest, the backdoor will download and launch CobaltStrike framework stager.

CobInt has C&C at foxsecit.com [185.86.79[.]156], and the domain was registered on May 18, 2018.

It is worth noting that the domain names kaspersky-security[.]com and foxsecit[.]com are registered by a person with the same name as with previously registered ibm-notice[.]com, which the Cobalt group used in March. And it in turn is associated with the domains

spamhuas[.]com и hoteltoren[.]com.

And the domains hoteltoren[.]com, dns-verifon[.]com, spam-huas[.]com, used by the Cobalt group to attack hotels and aggregators, confirm the fact that Cobalt hackers can diversify and extend their activities.

Considering that the latest attacks by the Anunak/Carbanak group were also targeting a number of hotels in order to obtain card data, the probability of a connection between these two hacker groups is high. This fact is not the main reason to link these groups, but it additionally confirms our hypothesis of their joint operation in 2017.

In our new report on Cobalt activities, we revealed the relationship between these two criminal groups, and carefully considered the joint attack on the banks.
foxsecit[.]com
185.86.79[.]156
kaspersky-security[.]com
91.230.121[.]86
ibm-notice[.]com
37.1.212[.]129
37.1.211[.]165
162.243.38[.]176
162.243.38[.]178
hoteltoren[.]com
172.81.132[.]131
kaspersky-corporate[.]com
194.58.112[.]174
62.76.40[.]207
172.217.22[.]110
mail.kaspersky-corporate[.]com
ibm-cert[.]com
138.197.128[.]24
ibm-warning[.]com
ibm-notice[.]com
dns-verifon[.]com
107.181.160[.]16
spamhuas[.]com
swift-sipn[.]info
85.143.166[.]158
swift-fraud[.]com
62.76.179[.]147
185.86.78[.]139
85.143.166[.]99
cloud.yourdocument[.]biz

31.148.219[.]177
ecb-europa[.]info
62.76.179[.]110
secure.n-document[.]biz
185.180.196[.]53
api.toshiba.org[.]kz
31.148.219[.]195
7b55c7ae346efb428aaf63d25ca0fcc7
fa354151a3fc6d0dce69e8eeaa8cd197
e5795f4418b28888a287e976f741dfbe

- recive@kaspersky-corporate[.]com
- info@kaspersky-corporate[.]com
- r.levis@kaspersky-corporate[.]com
- v.constancio@ecb-europa[.]info
- admin@swift-sipn[.]info

Joint operations

The report, "Cobalt: Evolution and Joint Operations", provides an analysis of the development of one of the most aggressive hacker groups responsible for financial damage to banks and financial services organizations in the Americas, Europe, Middle East and South East Asia.

Cobalt has continued target internal financial services systems to steal from Card Processing, ATMs, payment gateways and SWIFT systems. Group-IB experts provide insights in our reporting directly from first hand incident response and covers their activity from the beginning of their operations in 2016.

First success

The Cobalt group first committed thefts through SWIFT in Hong Kong, in the spring of 2016, and then in Ukraine. Millions of dollars were stolen in both cases, which required technologies and contacts with money mules that would be able to transfer large amounts of money withdrawn through SWIFT. These, and other factors, suggest that the group probably did not act on its own.

After the Ukrainian episode, attacks involving the system of interbank transfers suddenly ceased. The Cobalt group switched to attacks on banks through card processing and ATMs, which was much simpler and safer for mules (people who deal with cash withdrawals). Cobalt's first major independent success was the attack on First Bank in Taiwan, where the hackers managed to steal $2.18 million. In September 2016, Cobalt gained access to a bank in Kazakhstan. It took two months to prepare for the attack and explore the bank's infrastructure. In November, Cobalt successfully stole about $600,000 through card

processing. These attacks were then perfected and intensified. In 2017 the Cobalt group set "personal best" in attempting to steal EUR25 million from a European bank via card processing.

Cobalt only conducted new attacks on SWIFT 18 months after the April 2016 incidents. In December 2017 for the first time in Russia, they made a successful attack on a bank through SWIFT. This incident was the first SWIFT theft in the history of the Russian banking industry. For a considerable time, Cobalt's continued success was because the hackers constantly tested new tools and schemes, often changing the location of attacks and familiarizing themselves with how internal banking systems functioned. After gaining access to computers on a target bank, Cobalt often spent three to four weeks to study the internal infrastructure of the organization, collecting information about and observing the function of payments systems, and only then conducting their attack. The average damage from each successful attack was 1.5 million USD based on incident response conducted by Group-IB and publicly disclosed estimates from Europol.

In 2018, major strides were made to disrupt Cobalt group's operations when the leader was arrested by Europol and local law enforcement in Alicante, Spain. Following this arrest, Group-IB has continued to monitor new activity from the group, including attacks on March 10th, March 15th and even on the day of the announced arrest, March 26th with spear phishing emails sent to organizations acting as SpamHaus, a non-profit organization that fights against spam.

M & A

Group-IB has been investigating targeted attacks and cybercrime for over 15 years. Through incident response and joint investigations with law enforcement, we have monitored joint operations of various cybercriminal groups and the recruitment of individual hackers to commit attacks on banks and other organizations. We expect that this trend will only intensify over the coming years. This report publicly discloses the joint operations of the Cobalt Group and Anunak (Carbanak) which were identified privately before arrests, and provides an overview of their key attacks in the period 2016 - 2017.

In 2016, Group-IB released the first public report on Cobalt providing detailed information on their attacks, which is available online. This attributed the appearance of the Cobalt group with the termination of another infamous gang – Buhtrap. There was a three month break between the last Buhtrap attack and the first Cobalt attack.

In these three months, Cobalt prepared infrastructure and committed thefts through SWIFT in Hong Kong and Ukraine. We were confident that Cobalt was involved in these attacks because of the unique loader (stager). It was found in these incidents and has only been used by Cobalt. However, these attacks as well as their method of cashing out money were surprisingly sophisticated. This indicated that Cobalt group did not act alone. Communication with the Anunak group was discovered only 18 months later (in 2017), when during incident

response we detected the same unique SSH backdoor that was employed by the Carbanak group in 2014.

Arms Race

In 2017, Cobalt invested heavily into their technology – from reverse engineering of malware samples, it appears likely they enlisted a team of developers who created new tools for Cobalt group, and adjusted exploits in order to evade detection by security vendors.

Their work allowed Cobalt to act more efficiently: hours after PoCs for 1-day exploits were posted publicly, Cobalt group began using modified versions in attacks on banks and updated them in real time to avoid detection.

New tools and tactics allowed them to attack their targets - SWIFT, card processing, and payment gateways – with more success and set a "personal best" in attempting to steal over 25 million EUR from a European bank via card processing.

New tools and modified programs employed by Cobalt in 2017 are described below:

Cobalt encrypted the network of one small bank in Russia using this now well- known ransomware. After they failed to steal money through card processing, hackers used a self-developed modification of Petya ransomware named PetrWrap. This low- level modification is written in C. It is worth noting that to create such modification the author should be able to disassemble and clearly understand how and what they want to modify, which indicates a high level of technical skills. The majority of computers in the bank's network were disabled, which mildly complicated incident response and investigation.

In May, they began testing a new tool, the PE library (DLL), which was used as a reconnaissance module. However, this tool was never employed by the group, as they shifted to test a new JavaScript backdoor, which was designed to perform reconnaissance and complicate their discovery and analysis. This backdoor was used for the first time in attacks leveraging compromised servers of an integrator in the US. The malware was delivered through high-quality phishing emails with real reports from the SWIFT system attached. The program was used in attacks not only in the CIS countries and Eastern Europe, but also for attacks on western English-speaking companies.

In September Cobalt implemented JavaScript backdoor functionality in the executable file, but without the ability to load and run. In September attack they used InfoStealer 0.2. This only exists in memory and does not leave traces in the file system. This tool was employed in attacks on insurance agencies, the media, and software developers, whose compromised infrastructure was further used for attacks on banks.

In December, they started using a new Java loader, generated by the CobaltStrike framework, but with a unique payload that loads a unique Recon backdoor CobInt. The backdoor receives the modules from the C&C server for further execution. This complicated

attack vector is very similar to the tactics used in targeted attacks by professional state-sponsored attackers and the Lurk group.

Supply chain attacks and non-typical targets

A major change in the tactics of Cobalt was the shift towards indirect attacks. In February 2017, we tracked the first successful attack on a system integrator, which was then used as a vehicle by Cobalt for further attacks on companies in Russia, Kazakhstan, Moldova, as well as their subsidiaries in other countries. During the next 9 months, Cobalt infiltrated at least four integrators located in Ukraine, the US, and Russia.

In March 2017, Cobalt began to prepare attacks on companies that provide electronic wallets and payment terminals. In April, they adopted an attack scheme and created a unique program to automatically generate fraudulent payments through payment gateways. In September, the group for the first time attacked an e-wallet vendor and successfully stole funds through a payment gateway. In this incident Group-IB was able to discover clear evidence of Carbanak involvement.

More recently, the group has begun to attack insurance agencies and the media. In these attacks, they obtain control of mail servers or accounts to further use the victim's infrastructure for attacks on banks.
Cobalt: reboot

Cobalt returned in 2018 in fine form - both in terms of technology and infrastructure. The March arrest of the Cobalt gang leader in Spain has not yet led to the conclusion of attacks against financial institutions by this group. Remaining members reduced their activity in Russia and the CIS, temporarily focusing on other regions. It is interesting to note that phishing emails, which were tracked in March, purported to be from US companies, for example, IBM, Verifon, Spamhaus:

On March 7-10, letters were sent from the domains ibm-cert.com, ibm-warning.com, ibm-notice.com.

On March 15, a new phishing campaign was detected – hackers employed the dns-verifon.com domain, leveraging the brand of VeriFon, the largest vendor of POS terminals.

On March 26, phishing emails were sent acting as SpamHaus, a well-known non-profit organization that fights against spam and phishing. For this campaign, the attackers registered the spamhuas.com domain, which is indistinguishable from the official one (spamhaus. org).

On April 3, emails sent from the compromised mail server of the Swedish company were tracked.

On May 18, Cobalt sent emails from the name of SWIFT with JS backdoor, previously used in the Cobalt's attack against USA and Europe banks.

On May 23, Group-IB tracked a new large-scale Cobalt cyberattack on the leading banks of Russia and the CIS. It was like a challenge: phishing emails were sent acting as a major anti-virus vendor.

On May 28, hackers sent emails as European Central Bank with JS-backdoor.

Given the technological evolution of the group and the fact that in spite of the arrests of the Cobalt gang leader and malware writer, Cobalt has continued to strike, the most likely scenario is that remaining Cobalt members will join existing groups or a fresh "redistribution" will result in a new cybercriminal organization 'Cobalt 2.0' continuing attacks on banks worldwide.

"Cobalt: their evolution and joint operations" learn about Cobalt's development and modification of tools and tactics which were used to steal approximately 1 billion dollars from over 100 banks in 40 different countries.

Request