May 2018

group-ib.com

SHORT VERSION

COBALT

evolution and joint operations

Access to the full version of report is available only to Group-IB clients.

Register for a free product tour to test drive all the benefits of Group-IB Threat Intelligence and receive the full version of the report.

Introduction

On March 26, 2018, Europol reported the arrest of the Cobalt gang leader in Alicante, Spain. Cobalt is one of the most aggressive criminal groups, responsible for targeted attacks on banks and financial services providers worldwide. The scale of their activities is broad: according to Europol, the group has been linked with 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, Malaysia and others.

Group-IB forensic specialists were amongst the first to investigate Cobalt's attacks on banks, and in November 2016 issued a public report on the activities of the group. Since then we have continuously analyzed the evolution of their tactics and tools.

Initially, hackers focused on logical attacks on ATMs. But their targets developed and the Cobalt group successfully stole multiple times from payment gateways and card processing systems. By the end of 2017, for the first time in Russia, they made a successful attack on a bank using the system of interbank transfers (SWIFT). The Central Bank of Russia considers that Cobalt are the main threat to the Russian financial industry.

For a considerable time, Cobalt's continued success was because the hackers of the group 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.

The arrest of the Cobalt gang leader in Alicante, Spain, occurred significantly before the official announcement on March 26th. It has not yet led to the conclusion of attacks against financial institutions from this targeted attack group. On the date of the official announcement, Group-IB's Computer Emergency Response Team identified spear phishing emails which were sent by Cobalt acting as SpamHaus, a well-known non-profit organization that fights against spam and phishing. Continued attacks in South East Asia have been identified into April 2018.

Key findings

Cybercrime investigations

Group-IB has been investigating targeted attacks and cybercrime for over 14 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 Carbanak 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.

First success

Cobalt's first major independent success was the attack on First Bank's ATMs in Taiwan, where they managed to steal $2.18 million. Around the time of Group-IB's public report, Cobalt began to act more cautiously, switching to attacks on card processing, which are less dangerous for the money mules involved. Simultaneously, the group also began to reinvest into their TTP – modifying their exploits and stagers to complicate their detection and attribution.

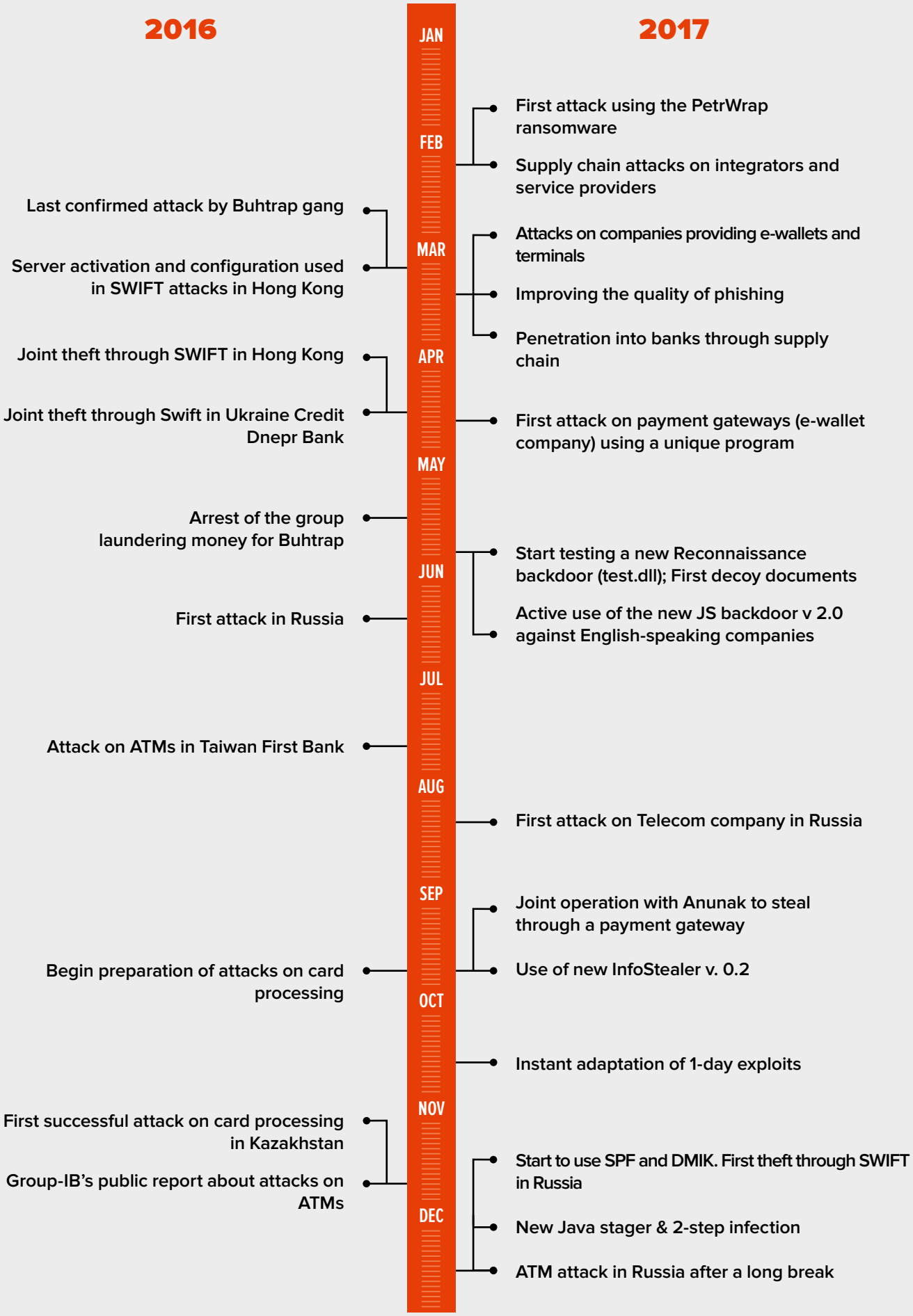
In September 2016 Cobalt gained access to the networks of a bank in Kazakhstan and began preparations for a new type of theft – through card processing. This took around 2 months to prepare for the attack and in November they successfully stole about $600,000. The theft timeframe was subsequently streamlined for card processing attacks. Following this, card processing has become a major theft target in banks worldwide. See Group-IB's report on MoneyTaker group for more information.

Importantly, focusing on card processing has made attacks safer for 'money mules' who deal with cash withdrawals as they no longer have to be specific ATMs (as in logical attacks). Their safety became a priority for the group after mules had been detained in Taiwan, Romania, and Russia.

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.

The most significant development events of Cobalt



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:

- **Petya.** 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.
- **JavaScript backdoor.** 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.
- **InfoStealer.** 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.
- **Recon Backdoor (CobInt).** 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

A major change in the tactics of Cobalt was the shift towards indirect attacks.

In February, 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.

Non-typical targets

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 23, Group-IB detected a new phishing attack launched by Cobalt, targeting banks in Russia, the CIS, and purportedly western countries.

For the first time, phishing emails purported to be from a large anti-virus vendor.

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.

Targeting Card processing

As early as in September Cobalt gained access to the network of a bank in Kazakhstan and began preparations for a new type of theft – through card processing. It took 2 months to prepare for the attack and in November they successfully stole $600,000. In 2017, the Cobalt group set a “personal best” in attempting to steal over 25 million EUR from a bank in Central Europe.

Cobalt learnt a lesson: when attacked banks and their ATMs were located in the same country, the mules who withdrew cash were often arrested.

Their safety became a priority for the group after mules had been detained in Taiwan, Romania, and Russia. **Focusing on card processing has made attacks much safer for money mules due to the following factors:**

- No need for complex cash-out schemes. Attackers withdrew cash immediately.
- All that was needed was to obtain or buy some bank cards to ensure cashing out.
- Withdrawing money in another country helped hackers to gain time, since the bank’s security team could not promptly contact the police and obtain video records from surveillance cameras.

The scheme is extremely simple:

- They legally opened or illegally bought cards of the bank whose IT system they had hacked.
- Money mules – criminals who withdraw money from ATMs – with previously activated cards deployed and waited for the operation to begin.
- After getting into the card processing system, the attackers removed or increased cash withdrawal limits for the cards held by the mules.
- They removed overdraft limits, which made it possible to go overdrawn even with debit cards.
- Using these cards, the mules withdrew cash from ATMs, one by one.

Step-by-step timeline of the attack on card processing

Step 1. Infection:

- On **September 7, 2016,** phishing e-mails with malicious attachments containing the Cobalt Strike payload were sent to various e-mail addresses including those of bank employees.
- On **September 8, 2016,** at 08:38:45, the malware ensured persistence on an employee's workstation and started distributing Cobalt Strike across the bank's IT infrastructure.
- On **September 9, 2016,** Cobalt Strike was downloaded on different workstations, after which the hackers gained a covert communication channel for monitoring the bank's IT infrastructure and taking control of all active nodes.
- From **September 9, 2016 to November 10, 2016,** the hackers collected data on domain and local user accounts using Cobalt Strike tools.

Step 2. Reconnaissance:

- On **November 10 - 30, 2016,** the hackers explored the card processing system using Cobalt Strike and compromised user accounts.
- They performed multiple connections to the system in order to develop several alternative routes for access to the control module.
- System capabilities were explored in order to detect specific settings of card accounts, setting credit limits, changing limitations on cashing out from card accounts.

Step 3. Money mule preparation:

- From **November 4 to December 12, 2016,** the criminals opened legitimate multicurrency cards in 4 different branches of a bank in Kazakhstan.
- Most of the issued cards were transferred from Kazakhstan to the Russian Federation, Latvia, Estonia, France, Austria, Germany, the Netherlands and Belgium.

Step 4. Theft:

- On **December 18, 2016,** a standard withdrawal scheme was implemented. The hackers, having gained unauthorized access to the bank's IT infrastructure, connected to the payment system using compromised accounts, set credit limits for their cards and removed cashing out limits for these cards.
- On **December 18-19, 2016,** a trained group of money mules performed cashing out according to set credit limits at the command of cash-out organizers.
- On **December 19, 2016,** the bank employees discovered an illegitimate setting of credit limits and, at 11:30 cancelled all cards and card accounts.
- On **December 20, 2016,** the last attempt of money mules to withdraw money was tracked.

Indicators

Hashes

01A0E6E1AC4CA9AE8A8D314F3812D63A
02DCB557D377470DF02558F5914F2DB9
032D63EC4CCFEF5648A414BEAD337B72
036FAF1F7E39E44C0DB25B9149B45786
04267FB0DBD0728A882298E120F70860
0C34AE326A8FD68D4A67EA3484B7CF81
0D21832C171E817E947837BBFB67380E
0D753E128C3F5BD088DD3FD7813A74B9
0E7952FB5990C4782A939E2E61615F6F
1593AC2AD08666E5BD6294174EA9121D
16EA8BB383BB33C5DF951794B6607456
178117C3D3829DBFB43008B4AF44A5AF
17C25C8A7C141195EE887DE905F33D7B
1B394EFC804F6B08AFA86DB0924D75D4
1D07EDBD16CBE529500C37245E613A47
1DF85C34E9FF432DE52F939D45916ABE
22AEF81AD5073421298846EE22996B73
23543750E343C70F6B2D0F1D63893675
240E12D258EE70909C3151C249647224
276DD9B30CBF8553F4AEBF5558158196
2AFFE3974213F831629FB1FFBB252252
2BC838A1B62B94F710E2EB0B36B0C57E
2D53C67EB0F16024C0843158149E9E5F
2D65E9263942E2A96811CC971FBE01D9
2DB35B260EB5C26FDFABD667648D55E2
2E0CC6890FBF7A469D6C0AE70B5859E7
2FD718F06B65D3C16659845AC1B5E36F
334870FC3C0F0DD2A8FA828393DDACCD
336452149B04E9C4C64B8C5015E64CCD
337005359179441 7E3282F7B40AE8AD
33A0FDFE54090F31E5ACC20BD0666D6D
33EDC70615DE35B71E54F046D7FA3038
3533C61681C33D5C17D8FF7A769E1592
35E0449CBE9FBE43E95B920C246828B2
37ADED8F7FF56D6F170845E7E9CACBF3
37D1F4B225EA7008A1A5C0641D99A8A0
3B2B116DB9569F50C9E7A272C7530B18
3EA9EF46E89F07920D87255AEF9261BA
417BBEF21CA0B964AFF5C8690B8307C9
45B1809AC884DA61954A1EC77A81C141
4673EBAD94126FC2404AF32A32DD2D95
470B4A700ED17CEF328BC6017B7E01FE
4AD39B50B9716C85A2C9377BF2FB1CA1
4B67A15C48C3DB6F3BA89EA6BB8F2DA2
4C1E6FC86270F3AD5E33C1DA50D27BE8
5387CE39A795CFE6477B91AAD2A617DF
53C31C8F47F6B421867E94EE2582F4FE
53C460BC660DB253E06673CA3FCD9282
555399C93B5F01FD9FAD5F903DA768D3
56487B799755F50C6E56C41870D43624
56A3A4C857939AC9BED4F2E0084FB037
5A34AACBBFCCD307D0394D0770AB6742
5A566B322605835A895E5408D2488E24
5AB6C208607F6F92697015D4F84D6B69
5B3968B47EB16A1CB88525E3B565EAB1
5B9677BEBE2B4392CC58F5836FE96A74
5D11C7B17633332B787992EE617D3552
5D139043028591159855AD589ADD1C41
5F6EFD501A5356D8F3C53B760B9EB616
60C61A79CD1B04936BFBAB75E9332107
60EBD9C7E7A911922C5EC16AB8128061
63F92615FBD133B98A02365AE5CFA232
6469A3862115B768C7D8465F73E79355
655E81C7758220E79D2F9066D853B642
670A1312AD4F1AC077D285BBC46E242C
699FFB65463A6F62DC11207FE30CB2AA
6ABCB743A649F136A7AF82C0DBCCAE0F
6D355FFA06AE39FC8671CC8AC38F984E
6DDA24EAC03876879F1404671646B79F
70469E15F04B799930BAEC1D3D64CD54
70E022CC5CD7F867A36D7E4932B637F6
712E11E5217EF06847EA96A83E952566
72EA2C440B522607EED37429A1675D8E
731654ED318DB772B50FC055A498F472
73AD7E37CE7A97C3BB5F69A87FE9358C
749CBCC0EC509FFCF8BFFAA9874E4F14
74B113E6FAE947FE9CED001432D6F152
74D5576A036F8A28EA423F053FCD89E2
752FC2B1736B7B6E124EF8012C744C33
77ECE7A13D98AC81E5022F8239985F9B
785DED9A20D7E63942E175A947D45F9F
7C5E8302AC75588B16A88B158AB3B595
7FA1AF2ADBA39EF6EFE0F870C057554D
80623478382370476D0B3DDC7FE68A88
820299C5BC8357743B222C11A3E50734
83DEE40F12F67634C5DA640F6D6F2EFB
84245BD582CAF2BB26681FCD9D1FB09E
85D074AA473F3AE94275F885F8A7D37E
87325B2522F8A48B8E5F149DD5E8EEA2

SHORT VERSION

87AA6F8B236F77EA6BA2960E339A2418
87CD2FA87920D8F16EB10DB54F9274C3
87D595E68A7B871564D9C70B1A9066F5
88B33FE677772431F7C37751C89DCB47
89889ADB22C63186EB8C72323F34B1FD
8993F927BEAF8DAA02BB792C86C2B5E0
89D910180AEAAC1029C98D7AE4FE746C
8C8A24A1F8014A171C96C80EFAB30FC2
8C99D3520D8220D58C1990D962647A39
9075432F928A166BFF386A0598E15618
95862A286C6F2C6205DC7D97ED12F753
95A1A53B1F3309B07722A2FD5B9AD1B5
966CC404A4F6BF6D77565004A952B3E3
96B420F072CD135ED7CAC2C6880C1727
96BABDCF4DBCAE1C40E28443A0535DD2
9713863011D0DB13DA1943931FF33B92
996054B4EBF1A81661B6B450113257A2
9A395E8ACA699190E724AC03B70B2924
9AFA9E95A7DCD3DEFD357292D843AF4B
9B6892E8470CFBD605F7037F844DC191
9CEA189EB6935013603619E998150AF9
9D443E225E21F160014E79B62C5AEA3D
9EAAAC2857AC71CE73C2554152042101
A57E0D0EC7AE26FFD9C1557BE6AE0864
A7ED424CF7C78E31BFBD0915B841C6E2
A9160049A5E449440FAD78482ED5D951
A99DB3460AE1BDDCA50EBB49E7FF98C9
AB6800A0A5CE088F9C9655672A42A446
AC9ED9C15244888D0635B698D1ED87C3
AE0E00E8BF6B9722D376CB84EAAE2251
AF75147E525ED8E52BF728466D66B9D0
AFF47AD6EE85747EC3FE5FCBD8441CF7
B175140A52ACA83833A8203AC81E7475
B182A813DA9B6E24321997FB3FAD1748
B1E2D42DB32952026DF6D5D7CC7ED9E1
B32C8B937EF0F319765F8B63F2209AF2
B4403222C7E0D02EEE471C409D2F1A61
B4A2799E4E50DF6813E5FB1AB7D4B094
B4F4CE145147C24D5AB339E877C57F88
B57189A131E7CBC53853D3AB58E2DE12
B5BABFA5EDDFA129862B02D125C9070C
B5BB3F04B6DCF61576E0436FAB88A22B
B6F640A14CC416E366E9BF899481FD6A
B7DD435A9CC841F7BADA2A064AFB4D3C
B9A7C0706087A0FECBD9B6F1002A2B96
BB6E7886BB38C10931152F9110A47A8F
BCC9AC70AB4048F60A2F6D658FBEE123
BD07B04E008093A40F60E48B903C59CF
BFABBEFB0ACD397A164E8F7EC3E467E9
BFB9688AC2747017C7975921FFE77BE9
C138D751DB967C0C7461A503FF987162
C2C753F440314D1EC88C1569AA845AC2
C6AC59164B4C637DBA6436E2A30144B0
C783CEE95BDC2E973415366215D15998
C8239719F5D3D3C0CF3EA76ED626BBE8
C8BCE60C90CE26B0E2B96770071C72D2
C91658349005A2F1C92A20132DE38486
C9ED3C1C6944341E106C5506F8D75D91
CAFAB9CC40AD0BD1CBEC2164E17C8216
CC70AAA5A8A792FAEAB8C873A4D73174
CE38E8D857794560FC8469C92AB16A66
D0F16357D10B5817C43554D5B6F540C8
D152C9DF5FE1E5540B003EAE557CF320
D3D3494DC630694C20A21F1DA327B551
D41C13C4A37EB358F6F314F6125343DC
D456A2719D1054BDBD0544A2DED6A354
D46DF9EACFE7FF75E098942E541D0F18
D4FF8E87F66150E36E4F70C65F422524
D529218495F0318B99E60477368BB55E
D6FF1AA189524A993836507B8D23EC64
D906F35FFCCF7F08AFCC193A2804DC5A
DB0D8569BC52E259BD327B10D0317174
DB334FC7BD6D351AAD6E93E87E837760
DB4FC02E5F5A21E38E93D867CC70FE54
DB6A8169F55A20838C0CA6F383C11E23
DD8664286D6EC3F6F90A3B80AF095479
E167322A628BDEC5348EE443EA9C9534
E249FC0578B0FBD00FC171A1B98CBC87
E38F081CF6628DF63FE8F79CB6ED62FA
E4A6E9824A12D0D3ACE6ACE9B3B79FCC
E54C635381B677E4BD2715013E19526B
E5C58D2EF3B20C5370C73B70E273B9B0
E5FCC477CD5176D4C6655C57B7A0274E
E7AA5608C81BA4FCD8D166501B90FC06
EB162CC34EFAE1CB621CC7157EF36514
EC4CCA1D9117A662573AEFD5284393DB
EF72BE586832AF0528D3A9B3C5347722
F2B1D948AF17F0006985B9EAEE48D490
F360D41A0B42B129F7F0C29F98381416
F3E52AC8B82CDC048F48BFD03868B072
F4F4EB32A90483A9A0FCA214FFAFB32C
F5AEA645966319C96D4DBCADCE2A10E0

F726CAD84718BCCFDC81C7F17700A4D1
F86ECC69CAAB5D627F9FE63F73B56936
FA04623CB547FA967F20F2630B750AF0
FA7654D7E2BE803DD7AF72B3457C1934
FAE3D240AD10FCE0E4CEC85AAE446237
FBDB2469B83944061E4847BFC5B3A08B
FBF25B39A15A011D8648BF20895F496A
FE44C14403F36C6E451BDA391A1D1CA7
649ad824358a4b00d7e7b8126cdbb28f
05493DEB5ACC8E54F8A500468983B9AF61734BEF
070CE979AC0A36C4AFC14BBF35CD8BDAECB10385
1989FEE716DAB57AEE2D7262309976EDCFB4FA85
1ACC9FA452CA967C7339D483FA3C2F07B30F4F1E
1CD36C26F0149DAA4AED1533BF4553B92FC55510
228C23A5F1EAD8DE24FF8DC626C8B3E274B46C66
24CEE03FEE0B63B200A6ABE1D73925EE594965A0
30B970761A5FDABE995BF4C2E8958750A641AE09
30C53E27C4E5928852E5C4D8F25FA7424AC01F9F
40AD156BCE130F5FA20C3D229115E1EB6E5AC208
4C230BB70B1949067ABB8643F2C4E8B015830BE9
51F56F8FD80B6F89C4E182F140C2BE0F7FCAEAEC
5B49F1D21C0C52D4E50D48D650EAB41B2397EF45
5E7046539FC51460F353A2A20E97135DA8E1C946
7365686C113B20E789F324FC11AEC6245519D3BD
7FD9CD1EC3E7E174A87157C21122E27C3A946F11
99C690BAA8C8DBBA851673134F8103520AA0460E
9A7A0A05A34633F6506A887986C915DAAB9A4191
9CA5777E3D653E4161E2675620FFBE8F30FBE49B
A86F5F63FEE80A9DA758B78BE406DF2868FD9EF8
BCA5A0CC43ED15E20540D6AE4033F589B1055386
CA1C4E239A9572A17A60F3ABC215F27D73435A8B
CB3D1222D735566CD042BFA26B38040C9519C265
CD2F33578B74991174423D172F1E2CDCEF32F1AA
D6FF511A13B527E74DE2CC134261A14A4491A628
DD9BDF212CAC50ACE88D39F14E153936B8A16052
EECD6C130A26F87FBA173C19C4006C6535D770B4
922e3bccd3eb151ee46afb203f9618ae007b99a758ca95caf5324d650a496426
022BBD6734923308F84765C1B5E64CD7B7160FB46731BE821A4F1EE4031429F9
083E096C90CE5DCBCCE2E47F9992F3DEBF1BC468E3C4998D355432BE88382E7A
08FD104D0C5A65912EFD699C213E48E446D1F5AD15DF0CD3E367176708800D46
0A10E844F1B6D8E6E6F653D6BD2F65902EC669D563FE0A52A3B0EEE34A2D3AB9
0A424531B7C46A72A6F1E2B5A0449B487D30B2F5389A2B86720E278F07AE976B
0B025090229123A49329267A2D455AACAB517809CCA1F5DD4745004744F0B45E
0CDE1B0614431CC124A35A200156458C04D0BB03DF92C6555937370016D189C8
0F2076CA59666727CF4E0FD9139A8FE87212FEAE09AD03CA7AABA3CC5D0D1502
106FCDF4D95957A156AE311E3D032B237D97385807949629AEDD018429D4D155
17F9DB18327A29777B01D741F7631D9EB9C7E4CB33AA0905670154A5C191195C
19CA92213B894397315F2B97B020C59D89AF911CFA5D83560A28BC00DBC8F1EA
1A31F9C5271E128B27E0F360041FEF4905309318C9A9C21FF0224F2BD9EBEA9F
1E933AC1B3FF56DD3E767FFEBB1EB9B05509F5E733719E174B09E52E26680879
20711584CEC6887D76F20519A73353C13E40A71C816B27AB132D1639C00FBC68
231A110AF055DD4579D7759FBA7D1C0F8F06486B45F2F8A0FDA1C5215A572313
232B7F918079D393D6F0F0F89018D773F5197BB22BBBDA06F0E7594C6B53123C
25C46C068DBEE7BD77CF762ED140C80DDAF439D118F51080E92478F982848A30
2B36C2A238C5DC44BCC2C5B9049DF207F2EA04CB499A7603EDD1B0547B9ECC7D

2D23B519931072632B8B6C0C9560D95414DD1639DF895694DFF7E5EA19FE5182
2E75D78A47C377C6AB720276BA52F919FFE4BBB88B9B48508851738F0992E816
3120B6EF21698C651479287F93E8252AE146543F5FB4868FD484DA695B714960
363881C87AB0795C20F2F171ACAC1A5325673A48DD9B391A81D9574E470143E5
36A53DAFA65C766A4AB746D3304A9BDB75E3D58B932487B5B7ADE66C40717D78
387DCBB30689BD778631249016EA5C0F10C87245D6229D77AF1D21E5DB1F8018
391038713033AD9D90F32CC0F2680F62C362E369BBA32FDF6009DCCAA4BC6FA7
39AC90410BD78F541EB42B1108D2264C7BD7A5FEAFE102CD7AC8F517C1BD3754
3A87B40C4DD2C8BCE991C7EE930E4F746B72C26FCD93D96D594ABC3E3146BC9A
3DB7364B4797A840E35D808B9F65C9DD30E4D0D73988D76BA419706108AE7A21
4035D977202B44666885F9781AC8755C799350A03838FF782EB730C0D7069958
405D1F1D3CC198FDA1E6D7FBF848EFCFA08EB67848C0812BB403D6F3BCCFD1DE
43F62CCDA103ED31A0726F5E422C363AD296FD7C39FFC2CE8D71467094F0E1CC
44FB5685527F8FAF9A721FF81CA4CE14E4E8DA5F796C8568146D2E9145F1FF1D
4847CB5894D2C8F674237714B60B7E3D6560CF0941621ACA462EA040A1EE57BB
484C9C1DC40308988371FEC737A9EFF9D3C4334705C2B8A97E0697324164C199
4E71EC1E4CA7069AD7FC535C8D9B6053BEFE1184B6E6B55043B4D901E15B0F5E
4E73334972D6B01650C572FD58596479E68EDEB8337962A19E0A76579A9B4ECC
52D69C91FBA8435398870D480F37E87F0A9F7EE721473C98659F5B94B1C91ABB
5513F579EF278A5CD20338810A7748D351243E4BFB254259B10E38A1480199B1
5595A6B04510E99D5B0C357D76B3BE0CCC506AAF91F9A08A72E0B92AC6D3D952
5674AA7B0E6E3DC0BE838351D57E75DC41B5F438BCB8B6ACC37BDD647FA68487
5F0D7423D889EB9DCE5E79E5BB8202AEA335F255BD88E4EABF21BFF8890BBC90
5F434901D4F186BDC92EE679783BDFAD80281423848462E445704D5A10B0DC20
5F48841D06D9059AA23965BDBE0E96BB01CD7DC6E2A5930E2EB46DEAE7FB99A2
5F70C76B6771B7C56BC5DA34E424EB9A090CEDEB807C795795A88C415A2E772C
60656140E2047BD5AEF9B0568EA4A2F7C8661A524323111099E49048B27B72C7
60982EE489398897B0EDEB78D1CF69DDB872BA8AB386438D65F78A60A73AFF32
61AFC2BF91283CCC478406A4C1277A0C8549584716D8B3A89D36F9BCDC45C4FE
64418056D8CE1C632ABE8FECE8E5E60B17530019ECA8299CAC1BF7B575DF351C
64A3F8B0E04356026372D48365A35CE3AF89830B7945E32F1D56A7F337BA51C5
66725E4C25E5D44F530E830C55D17FF43EBB9224BB1F31EE074D405BA8F50EBD
66BE70AA7D2EEC60DD9823037B55A603A83B3DA3B2862244BB5907CB8F392140
688C7160874A2525FAAF218A3365071BD16446A6D5C981B59A30950C8C0A2F87
69AF510104BFD5DAE6009EF1601E30141DB3E624205707A9108EFC9E1B8DD219
69E55D2E3207E29D9EFC806FF36F13CD49FB92F7C12F0145F867674B559734A3
6ACF35535D64D2C2116746EE4F0837CF59710B912B1F100FEDEC5B1520C957AA
6CE42F0EA6FE5BC909F6C656213AE474630841950D9F352CD6F1CAE2D2F8F0B4
6DAF931CC27B58EC8FA791314DBB060376305AA0BC3246322F7F20896C647940
71C7CBFC231AAB4570970FF833CE8E83511D6B925DE29721CA3171381631BEF1
746566D92E062C247083E7545C97F037D054A5EE802CB73B38940F2AF96EB25A
79B057B17D55A900B1B59AF24800D553422314B030F4A9C4F9308D8FBC1DC1AF
7DEDD5AF20185FBF0542E81456E993E26830C91199ED9EF25C0807F0223940F0
8A57464C93D4F6D85E51E07748D4FFCC0B9E6B5A64642AEC859040D1606FD0F8
8D19D567B8FD80EC910ECA4CDEC85ACD1BABC9F88FB057A3686E90EC82F73FE8
8D23742B5A2362CAF1CFF76B6D1968732E1E4FF5727C85A93AEB122170653DC6
8FB81DB1FDD5C3276CA5EF1F92C24EDE368F49EF68EC168C4065A64CC2E1213A
92413232C75B939ECE77E345393A377E74448D00965DA7EBA31655926725370D
935E16F280ABD2B08A7953D608B09E9202A8345B95647770E959A2C062EE7446
95416DD64701CA61AC4543B31BC1337007D0D568CB07466C30DB2E49FDE84F99
962875288F1DA5755C23A5D2E99D8087DC2C3F5B01EA0EA509341D343B5B5291
9898A001CB5385E647CFFBF2E0DFA1C9EE0FF5416D653CB44C108700FB1C732A
9B39BB02989367497016FE58FC39B0564A947A8A298B4A58E36FA983944A33C7
A0292CC74EF005B2E5E0889D1FC1711F07688B93B16EBC3174895D7752A16A23
A345D922B87246CFAEF749514F9B36D1C8BB152A8AFDDD26AB2566F9BEA071B1

A3E28D3DCC551BE46C9BFAD01AC00C54A960DA5062164C9D30AA136CCC283976
A64A2DFE1BC22F4493C9099759D1E1B4C4D42A7F45BFAFD128A33C6C82078F97
A6C4D88B1BE008C66B4D6BC327C2316AA57E366269ED045E2D39546712AF3E9B
A83199AA78D06E76A8719CF54EF9B130E295EC0F2E15142AA306FC7AB0214D8E
A908E47E1FDEA7022AD394F1764684D7954A0FFE88F27D438FBDC4C7926745DF
AA2B322B7F44C06137859B733AC0D94DFB1E302B5BE9A0E955BF935477008CAD
ADADBAF6FAD2936EBA9D6B448AAEEC324AC7293E664D9702C23A65C40F38FF29
AE3D88D7581E0DB10B469BE2A526F6C0A12265E9FE3BE2B742C7863CE0CDA995
AF17A3B5BF4C78283B2EE338AC6D457B9F3E7B7187C7E9D8651452B78574B3D3
B070320B92AC42AF6100936FE4F4519A4237FB1104081EAB4D6602B09B10D6B7
B082F4E8EAB928C2362FCD183F3829C0608A2A4D50221AE749C344E278A02FC0
B1985D6277D3F32B06D9A32DA2A889AE7E4A3DD44BB7B6962F2F07966AF316F7
B6D0B1030CB71C27F91DC9C645AD2C5AAF81BDF47F8713A5FA5AA0F2F0680F29
BB550EF28F0B8570307341D6B0374C3F28593B058DB4FB9156889CC028A09239
BB971A4508D6CAD7A1EDCAB06F5EBD30C25B2C1C5100A8C606F44D319E2FAA5A
BC4D2D914F7F0044F085B086FFDA0CF2EB01287D0C0653665CEB1DDBC2FD3326
BE81342E8193DB504242E7AE503641F8FC7B34E99FF1E0FA1371B36B6BAED304
C0026BD9402185EEC8A1C7EF5639684A7AE0CD56112B23012225D6F07B5FF866
C5D7C5C94468BA74211E08D7C2AD9D0274011D432EDC1AF8CDF2215B2C9D9291
C67DE95EAF817DC46ACCE9A0948FA2BA91222193999F28CBDE9F1B477F665E52
C827B3A2DCCA43ECF1ECC6C2DFF45094183F6D7C5A91A1BE537B9FA048D28427
C942A9C5DD017942C27BE4440B6A0ECACB1E2E7D1C9432F31EB0C2DA568FC7E3
CB7F5DD7B0D6465A2D0B83042154F4329F6B7B2727C5ED17B95D777E43F437E1
CCB1FA5CDBC402B912B01A1838C1F13E95E9392B3AB6CC5F28277C012B0759F9
CD69EA2C146350DBC197D40213602007CD65030738E24AB7E09B90065AF814EA
CD9572AB21BAE521120A2A0F3BBFD8085512504A2AE9AA217DB03164828117C7
D2D1A19FD2CF2093DEFE42DDBAAA2B01535313848A888D4F20C40EB8C4A518BA
D3844AC08424B50C3624718665D387D0C24888685744F8EFCE217197F597483E
DA0AD540A16BE01AE1430DD2AF8F48FD28F3AC4F965FC6780D8EEE3A2DB2AD10
DAB05E284A9CBC89D263798BAE40C9633FF501E19568C2CA21ADA58E90D66891
DCAD7F5135FFA5E98067B46FEEC2563BE8C67934EB3B14EF1AAD8FF7FE0892C5
DD7639C87F4DFA99B08601CBEAD7848D9614D84FF0EFA685936B881FA27D7331
DF3A183CD356D14CA1DEE36A0376DE8ED7D8BE2451E3E191CACA004CBDBA568D
E0F6073AEE370D5E1E29DA20208FFA10E1B30F4CF7860BB1A9DDE67A83DEE332
E234782F64F67EF3F78FFFCE306EAD1ED2011AE9217275556AD14C08CD5BB04E
E38D15ADD7BB5FA7387CB9B377D549B1365386DC13FC7E5ED08468CAD5ECAFE2
E4511C9492DCBB850830E6FA6443EB95FF3E389D65EBA620D1AAA36ED29399C7
E559C65B51A874B9EBF4FAACD830223428E507A865788C2F32A820B952CCF0B4
EAC418381EA047601FAE9C92412B5DF49ED6AAC3EDD74FB5E2EB6F09A1CC3861
FA9758814E0994B972AFE305A50B7326193A3D15F603063D0B6728DCCFBD8DBF
FB00B98B44E3AA59FC2309C477EBB75774A2B5E1F300383414762BB4AB95D96A
FB97A028760CF5CEE976F9BA516891CBE784D89C07A6F110A4552FC7DBFCE5F4
FF94DED03A42857C7C534229859B99E034745177184791DF3084B6DDE66B29E6

Group-IB — one of the global leaders in providing high-fidelity Threat Intelligence and anti-fraud solutions

www.group-ib.com
info@group-ib.com
twitter.com/groupib_gib
group-ib.com/blog
+7 495 9843364
linkedin.com/organization/1382013