Bolsas
Na sexta-feira
0,24% São Paulo
0,77% Nova York

Pontuação B3
Ibovespa nos últimos dias
138.854 — 141.263
1/7 2/7 3/7 4/7

Dólar
Na sexta-feira
R$ 5,424
(+ 0,37%)

Últimos	
30/junho	5,434
1/julho	5,461
2/julho	5,420
3/julho	5,405

Salário mínimo
R$ 1.518

Euro
Comercial, venda na sexta-feira
R$ 6,388

CDI
Ao ano
14,90%

CDB
Prefixado 30 dias (ao ano)
14,91%

Inflação
IPCA do IBGE (em %)

Janeiro/2025	0,16
Fevereiro/2025	1,31
Março/2025	0,56
Abril/2025	0,43
Maio/2025	0,26

CRIME CIBERNÉTICO

O maior ataque hacker da história do país

Polícia Civil de SP prendeu um dos autores do crime, que confessou a participação no assalto bilionário feito no meio digital

» RAPHAEL PATI
» ROSANA HESSEL

Foi preso na noite de quinta-feira, em São Paulo, um suspeito de participar da invasão ao sistema da C&M Software (CMSW). João Nazareno Roque, de 48 anos, era funcionário terceirizado da empresa e prestava serviços como operador de TI e foi levado pela Polícia Civil do estado paulista (PC-SP), onde confessou que teria disponibilizado login e senha particulares do sistema a terceiros.

Nas redes sociais, ele se identifica como eletricista predial e residencial com mais de 20 anos de experiência, além de especialista em leitura e interpretação de projetos no AutoCad, quatro anos como técnico de instalação de TV a cabo e um ano como técnico de alarme de incêndio. À polícia, João revelou ter recebido R$ 15 mil pelos criminosos desde março, quando se encontrou pela primeira vez com um dos participantes da invasão.

"Ele (João) disse que foi abordado em um bar da rua, que ele frequentava, próximo da casa dele, por pessoas que já sabiam que ele trabalhava nessa empresa", disse o delegado Renato Tupan, do Departamento Estadual de Investigações Criminais (Deic) da PC-SP, em coletiva de imprensa na sede da corporação. Segundo a Polícia Civil, o suspeito recebeu R$ 5 mil no momento em que foi cooptado pela primeira vez e, posteriormente, conseguiu mais R$ 10 mil dos criminosos. No dia da fraude, ele relatou que teria conversado com o grupo que, ao todo, teria pelo menos quatro integrantes com vozes de pessoas jovens.

As conversas ocorreram por mensagens e ligação, mas sem João conhecer o rosto ou os nomes verdadeiros dos hackers. "O único que ele viu, segundo contou, foi o que fez a abordagem, e aí no dia da fraude eles falaram o seguinte para ele: 'olha, deixamos a poeira baixar, e aí a gente volta a conversar por outros valores'. E aí eles perderam o contato", acrescentou o delegado.

De acordo com as investigações, a maior vítima até o momento é o banco BMP, que contratou o software da C&M para realizar suas operações. Além disso, há outros bancos que foram prejudicados, mas não foram informados pela PC-SP, por questões de sigilo. "Plenamente, a gente não tem dúvidas que o João é um dos co-autores do crime, ele responde por associação criminosa, no mínimo, e um furto qualificado mediante fraude e abuso de confiança", disse o delegado Paulo Barbosa, diretor da 2ª Divisão de Crimes Cibernéticos do Deic.

> **Plenamente, a gente não tem dúvidas que o João é um dos coautores do crime, ele responde por associação criminosa, no mínimo, e um furto qualificado mediante fraude e abuso de confiança"**
>
> ***Paulo Barbosa,*** *diretor da 2ª Divisão de Crimes Cibernéticos do Deic*

Estimam-se que os valores desviados podem superar a casa de bilhões de reais, apesar de ainda não haver confirmação tanto por parte do Banco Central, quanto da polícia. Segundo o delegado Topan, todas as transferências ocorreram via Pix, apesar de a empresa também oferecer serviços por TED. "Em relação à estimativa, a gente não pode afirmar hoje uma cifra exata. Mas é um valor muito alto. É o maior da história do Brasil", detalhou Barbosa.

A C&M Software é uma empresa que interliga algumas instituições financeiras ao Sistema de Pagamentos Brasileiro (SPB), inclusive, o Pix. Em nota, a empresa afirmou que foi vítima de uma "ação criminosa externa", originada a partir da violação do ambiente de um cliente, cujas credenciais de integração foram indevidamente utilizadas. "Não houve invasão direta aos sistemas da CMSW. Os sistemas críticos seguem íntegros e operacionais", diz a empresa.

Ontem, o Banco Central suspendeu cautelarmente do Pix três instituições de pagamento (IP) suspeitas de terem recebido recursos desviados pelos criminosos do sistema C&M Software, que já havia sido suspensa. A nova suspensão envolve as IP Transfeera, Soffy e Nuoro Pay.

Reprodução

Funcionário terceirizado confessou ter recebido R$ 15 mil para fornecer login e senha. Roque disse que não conheceu os criminosos pessoalmente

Episódio mostra fragilidade do sistema

Mesmo com a prisão do primeiro suspeito do roubo bilionário de clientes da CMSW, que era credenciada pelo Banco Central para intermediar operações financeiras com SPB da autoridade monetária, analistas levantam preocupações sobre a fragilidade do sistema.

Para eles, o BC precisa explicar melhor o ocorrido e mostrar que o SPB é confiável para a população. Procurado, o BC reforçou que o problema não está relacionado com a instituição e que há "zero chance" de algum funcionário da autoridade monetária estar envolvido nesse roubo. A instituição informou ainda que nem a C&M "nem seus representantes e empregados, atuam como seus terceirizados ou com ele mantêm vínculo contratual de qualquer espécie". "A empresa é uma prestadora de serviços para instituições provedoras de contas transacionais", informou a nota da autoridade monetária.

Na avaliação dos especialistas, o roubo foi bem elaborado e executado por profissionais que conhecem muito bem o SPB. Para eles, essa quadrilha de criminosos deve ser nacional. Além disso, segundo os analistas, dentro desses bancos, as pessoas com credenciais para acesso a essa conta reserva são muito poucas e, geralmente, são cargos de confiança dentro da instituição.

> **O caso é diferente dos ataques mais comuns, porque mostrou uma vulnerabilidade tecnológica e os criminosos acabaram entrando pela porta da frente"**
>
> ***Rodolfo Almeida,*** *especializada em cibersegurança da ViperX*

"Esse caso mostra um direcionamento do roubo, que não foi nas contas dos clientes das instituições financeiras, e sim nas reservas dos depósitos de bancos no BC", afirmou Rodolfo Almeida, COO da ViperX, startup do grupo Dfense especializada em cibersegurança.

Anchises de Moraes, especialista da Apura Cyber Intelligence, destacou que esse ataque cibernético não é muito normal e não envolve o usuário final, que são bem investigadas pelas autoridades. "Um banco digital costuma ter um ou dois funcionários apenas com acesso a essa conta reserva no BC e, geralmente, é um executivo da área de negócios. O fato de o roubo ter ocorrido na madrugada de uma segunda-feira essas pessoas não tinham como serem avisadas. Acredito que o horário foi escolhido a dedo uma vez que o Pix funciona dia e noite e não tem interrupção", afirmou.

Moraes lembrou que esse sistema que foi atacado é muito específico e não é qualquer pessoa que tem conhecimento do SPB. "O criminoso tinha que ter um conhecimento muito específico, porque as pessoas físicas e tem algumas particularidades que precisam ser essa conta reserva é bilionária e muito mais complexa", destacou.

O fato de os desvios terem começado de madrugada mostra também a fragilidade no monitoramento de operações suspeitas, tanto no BC quanto nas instituições financeiras clientes da CMSW que acabaram sendo vítimas. "O caso é diferente dos ataques mais comuns, porque mostrou uma vulnerabilidade tecnológica e os criminosos acabaram entrando pela porta da frente, via credenciais válidas com acesso ao fundo reserva no Banco Central. Não é qualquer pessoa que consegue ter esse tipo de acesso", afirmou Rodolfo Almeida. Ele lembrou que as cifras dos desvios ainda não estão totalmente conhecidas e podem chegar a R$ 3 bilhões.

"Um ponto preocupante desse caso é que não houve monitoramento e a descoberta aconteceu porque uma corretora de criptomoedas considerou o volume de uma operação muito alto e fez o alerta a um dos clientes da CMSW", afirmou Almeida. Ele lembrou que o principal vetor do comprometimento foi via a CMSW e isso exige mais maturidade das empresas que contratam serviços de terceiros.

PF tem condições de esclarecer golpe

» ANA MARIA CAMPOS
Enviada especial

Lisboa — O diretor-geral da Polícia Federal, Andrei Rodrigues, acompanha, de Lisboa, onde passou os últimos três dias no 13º Fórum de Lisboa, o ataque hacker contra a empresa C&M Software, que presta serviços de tecnologia para instituições financeiras.

Andrei Rodrigues afirmou que a PF tem condições de esclarecer o crime — considerado o maior golpe cibernético contra instituições financeiras do país. "Não posso revelar os detalhes da investigação. O que posso dizer é que criamos uma diretoria de crimes cibernéticos exatamente com essa perspectiva do crescimento dessa modalidade delituosa", afirmou.

Andrei disse que a Polícia Federal trabalha integrada a agências e inteligência. "Temos hoje uma equipe técnica, equipamentos e estamos trabalhando sobre esse caso, sobretudo, com uma grande interação com outras agências, inclusive, do setor privado para que a gente consiga avançar", afirmou o diretor-geral após participar do painel Segurança Pública e Federalismo Cooperativo: Enfrentando as Organizações Criminosas, ao lado do governador de São Paulo, Tarcísio de Freitas (Republicanos), do procurador-geral da República, Paulo Gonet, e dos ministros do Superior Tribunal de Justiça (STJ) Raul Araújo Filho e Mauro Campbell Marques, corregedor nacional de Justiça.

Segundo Andrei Rodrigues, a PF tem obtido sucesso na elucidação de crimes em 86% das investigações. "Eu espero que essa seja uma que aumente essa estatística", afirmou.

Em sua palestra, o delegado afirmou que a PF hoje trabalha sem espetacularização e com respeito aos investigados. "Não tem mais o japonês da Federal, o hipster da Federal ou presos exibidos com algemas", disse Andrei. Ele ressaltou que a PF não trabalha mais com "achincalhamento".

Mariana Campos/CB/D.A Press

Andrei Rodrigues disse que a PF está equipada para elucidar o crime