Ataques, fama, dinheiro, o líder adolescente e as (curtas) férias. Afinal, o que se sabe sobre o grupo Lapsus$?

observador.pt/especiais/ataques-fama-dinheiro-o-lider-adolescente-e-as-curtas-ferias-afinal-o-que-se-sabe-sobre-o-grupo-lapsus

▲O grupo Lapsus$ já terá atacado grandes empresas mundiais, como a Okta, a EA e a Samsung
NurPhoto via Getty Images

O Lapsus$ tem desafiado a cibersegurança de grandes empresas. Adolescentes que "gostam de fama" anunciaram que iam de férias, mas voltaram a atacar pouco tempo depois. O que se sabe sobre o grupo?

O grupo Lapsus$ tem posto à prova os sistemas de defesa cibernéticos de grandes empresas mundiais. Desde o momento em que reivindicaram os primeiros ataques, os *hackers* ganharam notoriedade, fama e mais de 58 mil seguidores na rede social Telegram.

Começaram a ser falados após comprometerem o site do Ministério da Saúde do Brasil, mas ambicionaram mais. À medida que ficaram mais conhecidos terão atacado empresas cada vez maiores, verdadeiras gigantes mundiais como a Samsung ou a Eletronic Arts (EA). Em Portugal, reivindicaram o ataque ao grupo Impresa e ao site do Parlamento.

"O Lapsus$ é só mais um grupo, que agora apareceu mais mediaticamente", desvalorizou o especialista português em cibersegurança Bruno Castro. Da fama das empresas que foram vítimas destes piratas informáticos aos maiores ataques que conseguiram realizar. Da importância da Microsoft à prisão de um adolescente que pode ser um dos líderes. Afinal, o que já se sabe sobre o grupo Lapsus$?

Os ataques que o Lapsus$ realizou e reivindicou

Um ataque ao site do Ministério da Saúde do Brasil e à plataforma que continha os dados de vacinação contra a Covid-19 do país, em dezembro de 2021, foi o primeiro a ser reivindicado pelo grupo de *hackers*. A emissão de certificados de vacinação ficou bloqueada. Como consequência, milhões de brasileiros não conseguiram obter o certificado, que, na altura, era necessário para viajar, ir a jogos de futebol e a restaurantes.

O grupo Lapsus$ anunciou ao mundo que pretendia "vazar ou guardar" as informações que tinha recolhido — cerca de 50 *terabytes* (TB) de dados relacionados, por exemplo, com o processo de vacinação, avançou a CNN Brasil. Demorou quase duas semanas a pôr a funcionar o portal do Ministério da Saúde do Brasil com normalidade, com o organismo a garantir ter conseguido recuperar os dados.

No mesmo dia em que comprometeu o site do Ministério da Saúde, o grupo atacou a Escola Virtual brasileira, noticiou, na altura, a CNN. Na página do site comprometido, o Lapsus$ terá deixado a seguinte mensagem: "Nós voltamos, porém, com mais notícias (e com mais poderio). Vamos explicar algumas coisas: o nosso único objetivo é obter dinheiro, não ligamos para a família Bolsonaro (vulgo Bolsofakenews) de m****".

Ainda no mês de dezembro, nos dias 27 e 29 de dezembro, os canais de atendimento, os serviços de recarga de pré-pagos e os sistemas internos das lojas da operadora de telecomunicações brasileira Claro ficaram indisponíveis. Foi mais um ataque reivindicado pelo grupo Lapsus$. A operadora recusou-se a confirmar o ataque, mas os *hackers* alegavam ter acedido a 10 mil *terabytes* de dados.

O Lapsus$ parecia estar a atacar apenas no Brasil, até que foi revelado que, afinal, no mês de junho de 2021, uma empresa muito maior já tinha sido alvo dos piratas informáticos. **A Electronic Arts** (EA), considerada uma das maiores empresas de videojogos do mundo, produtora do FIFA e do The Sims, tinha sido atacada.

As informações privadas dos jogadores não terão sido divulgadas, mas evoluções do jogo FIFA2021, dados sobre novos lançamentos, código-fonte de vários jogos e ferramentas utilizadas no seu desenvolvimento foram tornadas públicas pelo Lapsus$. A empresa informou que não existiam "razões para acreditar que a privacidade dos jogadores estava em risco", mas garantiu ter melhorado a sua segurança, avançou a revista Vice aquando do ataque.

Embora a EA pareça ter desvalorizado a divulgação do código-fonte dos jogos — informação que é única — a realidade é que o roubo pode ter implicações. Segundo o CEO da Visionware, empresa portuguesa de cibersegurança, Bruno Castro, **o roubo "significa, na prática, que esse jogo pode ser replicado com outro nome".**

> Imagine, eu poderia roubar o código-fonte do seu jogo, vendê-lo na *dark web* a uma empresa que faça jogos, eles melhoram esse código-fonte e ainda fazem um jogo melhor do que o seu", explicou Bruno Castro em declarações ao Observador.

Muito ativos na rede social Telegram, onde reivindicam os ataques e enviam mensagens para as empresas cuja cibersegurança tentam comprometer, o grupo Lapsus$ começou no final de 2021 a ganhar as atenções do mundo. Em Portugal, permaneceram sem causar

impacto até ao segundo dia de 2022.

No dia 2 de janeiro de 2022, os sites do grupo Impresa, entre os quais se incluem Expresso, SIC, Blitz e Opto foram atacados e ficaram indisponíveis. Descrito pela Impresa como um "atentado nunca antes visto à liberdade de imprensa em Portugal na era digital", **o ataque foi reivindicado pelos *hackers***. Em comunicado, a empresa de comunicação social admitiu violação de alguns dados pessoais, mas disse não ter evidências que os atacantes tivessem palavras-passe ou dados bancários dos utilizadores, e que também não houve qualquer pedido de resgate.

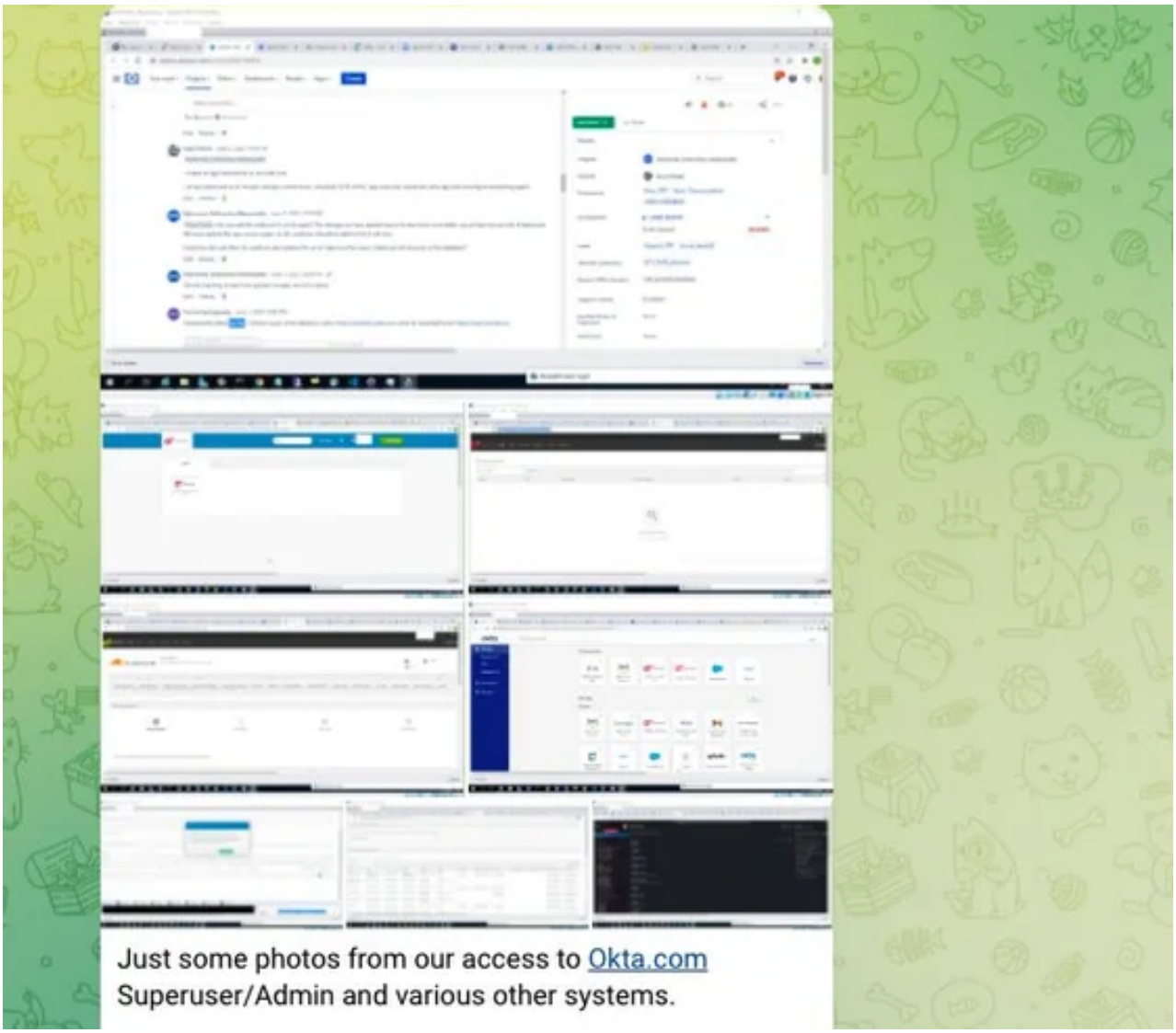
No mesmo mês, mas a dia 30, o alvo português foi outro: o grupo dizia ter conseguido entrar no site do Parlamento português. O Lapsus$ anunciava ter-se apoderado de várias informações sobre o Governo e os políticos, mas a Assembleia da República garantiu que através do site não era possível ter acesso a informações reservadas ou confidenciais.

Uns dias depois, a 7 de fevereiro, a Vodafone foi atacada. Serviços, como hospitais, ficaram afetados e milhões de portugueses deixaram de conseguir receber e enviar mensagens ou chamadas e ficaram sem acesso à internet. A empresa de telecomunicações referiu não ter indícios de que os dados dos clientes tivessem sido comprometidos. Uma mensagem deixada no Telegram a perguntar se deveriam "vazar" primeiro os dados da Impresa ou da Vodafone é única associação existente entre o ataque à operadora de telecomunicações e o Lapsus$, que não reivindicou este ataque.

No final de fevereiro, a onda de intrusões reivindicadas pelo grupo continuou, novamente fora de Portugal. Os sistemas internos da Nvidia, empresa de processadores gráficos, foram comprometidos pelo grupo Lapsus$. Os *hackers* afirmaram ter na sua posse mais de 1TB de dados e informações de mais de 71.355 funcionários juntamente com códigos-fonte da empresa. **A Nvidia acabou por assumir que foi vítima de um "incidente de cibersegurança"** que teve impacto nos seus sistemas informáticos, salientando que reforçou a segurança da sua rede e notificou as autoridades do ataque. A empresa garantiu também que os códigos-fonte a que os *hackers* tiveram acesso já não eram válidos uns desde 2014 e outros desde 2018.

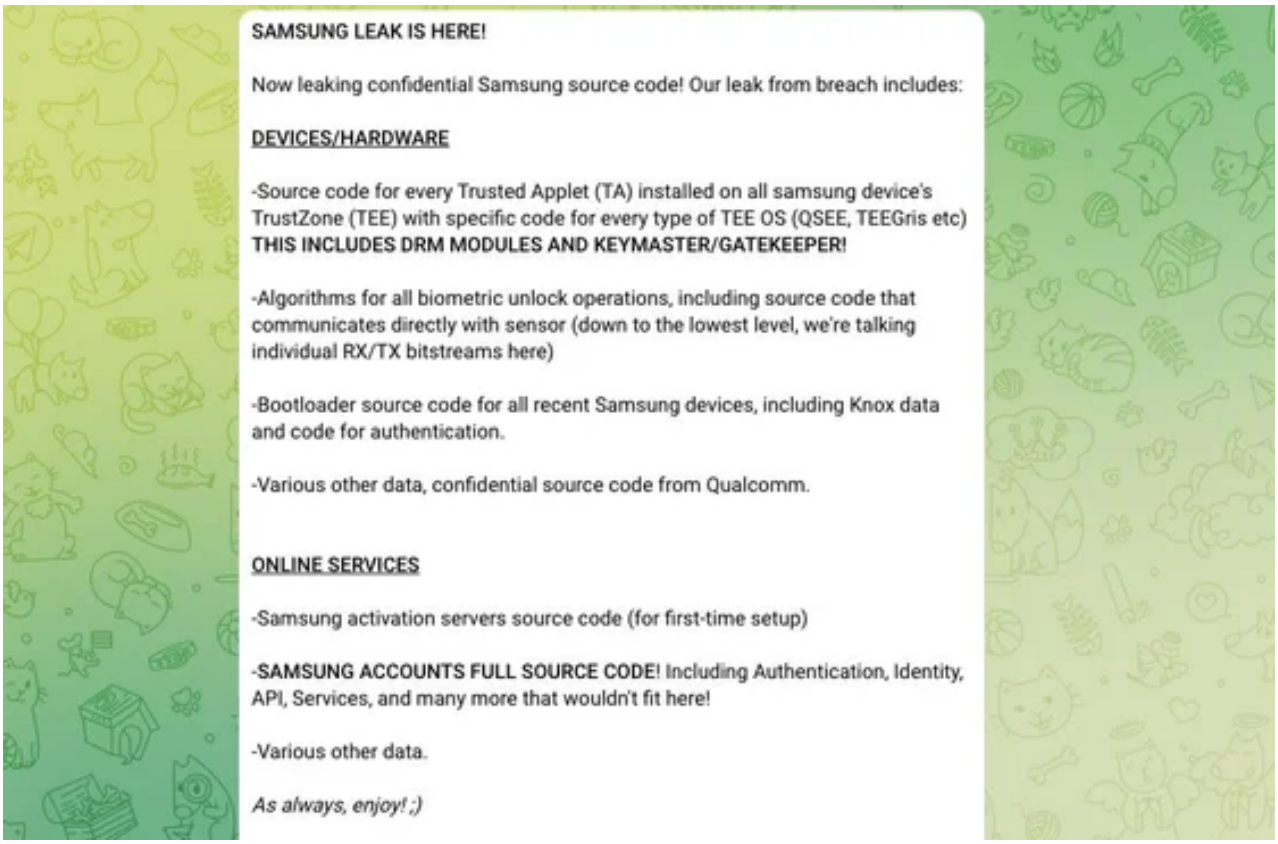
No seio das vítimas do Lapsus$ seguiu-se a Okta, que fornece a funcionários de mais de 15 mil organizações sistemas de autenticação no acesso a aplicações através de um *login* único. Até março, a Okta negou o ataque que poderá ter acontecido em janeiro. Quando finalmente admitiu que os seus serviços tinham sido comprometidos pelo Lapsus$, a empresa revelou em comunicado que os piratas informáticos poderiam ter acedido à informação de cerca de 2,5% dos seus clientes.

A empresa pediu desculpa pela incerteza que o ataque causou e afirmou levar muito a sério a responsabilidade de proteger a informação dos clientes, admitindo que cometeu um "erro" ao acreditar que o Lapsus$ não teria sido bem sucedido. Em resposta à Okta, o grupo de *hackers* revelou no Telegram diversas capturas de ecrã que comprovam o ataque e disse que tinha conseguido acesso a uma conta de administrador da empresa, o que lhe permitia redefinir palavras-passe e contas de qualquer cliente que escolhessem.



No Telegram, o Lapsus$ publicou várias capturas de ecrã para comprovar que tinha acesso a uma conta de administrador da Okta

Na segunda-feira, dia 21 de março, conheceu-se um dos mais recentes alvos do Lapsus$. A Samsung confirmou uma "violação relacionada com os dados internos da empresa", revelou a Bloomberg. O grupo de *hackers* conseguiu assim realizar mais um ataque a uma grande empresa, que confirmou que parte do código-fonte dos dispositivos Galaxy mais recentes foi comprometida, não especificando quantos modelos da linha foram afetados. A empresa sul-coreana garantiu que reforçou a sua segurança e afirmou ainda que o ataque não comprometeu informações sobre clientes e funcionários.



O anúncio do ataque à Samsung publicado pelo Lapsus$ no Telegram

Na maioria dos ciberataques, o grupo Lapsus$ utilizou o Telegram para os reivindicar, para divulgar dados e para ameaçar as vítimas. A escolha desta rede social tem uma explicação para Bruno Castro: **"É um canal de comunicação ultrasseguro, muito difícil de rastrear e muito difícil de as comunicações serem intersetadas.** Portanto, diria que é o veículo quase perfeito para fazer comunicações criminosas no seio de um grupo que tem que comunicar mundialmente, porque tem elementos a trabalhar pelo mundo inteiro." Contactado pelo Observador, o Centro Nacional de Cibersegurança não deu qualquer informação sobre o grau de conhecimento que terá sobre o Lapsus$, informando que não comenta casos concretos.

A Microsoft investigou o Lapsus$ e revelou como é que o grupo recruta novos membros

Tudo começou com uma tentativa de ataque que falhou. Foi aí que a Microsoft começou a investigar o grupo Lapsus$. Os piratas informáticos disseram ter conseguido aceder ao código-fonte de produtos da empresa, que rapidamente negou as acusações.

Admitindo que os *hackers* tentaram atacar e conseguiram comprometer uma única conta, a Microsoft sustentou que **"nenhum código ou dados dos clientes" tinham sido envolvidos na tentativa de ciberataque**. Em comunicado, a gigante tecnológica referiu que as suas equipas de segurança conseguiram bloquear o possível ataque a meio da operação. A Microsoft revelou ainda que não "depende" do "secretismo do código-fonte como uma medida de segurança".

Sofisticado, com ataques de perfil elevado e sem recorrer ao *ransomware* — um tipo de malware que permite que o atacante se apodere de ficheiros bloqueando a possibilidade da vítima conseguir aceder aos mesmos para depois pedir um resgate. Foi desta forma que a Microsoft descreveu o Lapsus$.

Porém, continua a não ser consensual que estes piratas informáticos não recorram ao *ransomware*. O especialista português Bruno Castro acredita ter havido "ataques em que utilizam *ransomware*", uma vez que, os grupos criminosos precisam "do dinheiro". Ainda assim, permanece sem ser possível confirmar que o Lapsus$ tenha conseguido lucrar com eventuais pedidos de resgate a alguma das empresas que atacou.

Os *hackers* atacaram as empresas, roubaram informações e divulgaram-nas no Telegram, arranjando sempre uma razão para não se libertarem do controlo que tinham sobre os dados. O grupo, que afirmou não ser patrocinado por nenhuma entidade estatal e não estar ligado à política, fez assim ações de "destruição e sabotagem massiva e gratuita de informações, infraestruturas e sistemas", referiu a Microsoft.

"Colocar em causa a instituição por alguma razão específica e roubar os dados para depois comercializá-los na *dark web* em fóruns específicos" é o propósito dos grupos que não pedem resgate dos dados que têm na sua posse, considerou Bruno Castro. Ou seja, estes piratas informáticos poderão entrar nas empresas apenas para mostrar que o conseguem fazer, acabando por comprometer centenas de dados confidenciais.

"Podemos dizer que a tendência não é atacar as empresas, nem as infraestruturas. Numa primeira instância, é atacar as pessoas. A tendência há-de ser cada vez mais atacar o fator humano"

Bruno Castro

Índice

Como o **fator humano é o elo mais fraco**, os *hackers* começaram a utilizar-se dele para conseguir chegar até às empresas que querem atacar. No caso do Lapsus$, para conseguirem realizar a intrusão necessária para os ataques informáticos, os emails dos colaboradores foram utilizados como alvo pelos *hackers*.

Na prática, Bruno Castro explicou como funcionam os ataques "direcionados aos elementos da informática ou ao CEO da empresa". Os emails (de *phishing*) contêm conteúdos atrativos e personalizados para aquela pessoa. "Para a informática envio emails com informação da área, para o CEO que sei que gosta de barcos envio emails sobre barcos. Conteúdos que sejam altamente permeáveis ao seu interesse. E eles clicam

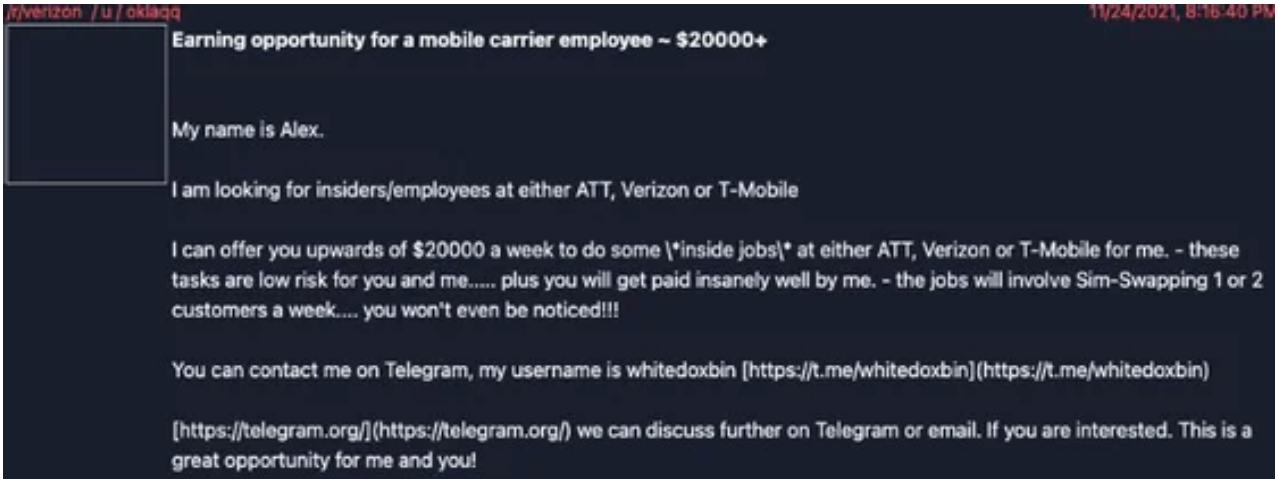
naqueles emails que são armadilhas". A partir desse momento, a pessoa que caiu na fraude dos *hackers* é uma vítima, mas também o responsável por permitir que os piratas informáticos ataquem a empresa.

A Microsoft disse ainda que o SIM Swapping é outra das técnicas utilizadas pelo grupo Lapsus$ para aceder a dados das empresas. Com esta técnica, os *hackers* conseguem clonar um cartão de telemóvel e ter acesso a informações pessoais sobre a vítima, como o seu nome completo ou dados bancários. Depois, os *hackers* deslocam-se a uma loja do operador de comunicações onde se fazem passar pela vítima para pedir a transferência de dados de um SIM para o outro. Assim, conseguem ter acesso a informações e senhas confidenciais de funcionários das empresas que vão comprometer.

Na investigação ao grupo Lapsus$, a **Microsoft descobriu também como é que os *hackers* recrutam novos membros.** Desde pelo menos novembro de 2021, os piratas informáticos terão recrutado pessoas que trabalham dentro de grandes empresas cujos sistemas querem comprometer para os ajudarem nos ataques.

Mais uma vez, Bruno Castro disse que é "muito comum" que sejam contratadas pessoas que trabalhem para as vítimas dos ataques. "A colaboração de alguém de dentro seja ela em troca de dinheiro, influência, ataque à entidade patronal, por vingança ou meramente por estar a ser pago por isso é muito normal. Há elementos internos que são utilizados como pivôs dos ataques".

Porém, também nas redes sociais apareceram indícios de que o grupo tentou contratar funcionários de dentro das empresas. No passado mês de novembro foi colocado no Reddit um anúncio de emprego, onde o Lapsus$ oferecia 20 mil dólares por semana (cerca de 18 mil euros) a quem estivesse disponível para fazer "inside jobs" ("trabalhos por dentro", em tradução livre).



O anúncio de emprego colocado no Reddit pelo Lapsus$

Lapsus$, um grupo de *hackers* movido a dinheiro e fama?

As principais razões que levam o Lapsus$ a atacar as empresas não são conhecidas, mas acredita-se que o grupo seja motivado não só pelo dinheiro, mas também pela notoriedade e fama. João Lucas Brasio, brasileiro considerado um dos maiores

especialistas em segurança digital, disse em entrevista telefónica ao Observador que o grupo Lapsus$ "tem um elemento que é raro" nos *hackers*. No entender do especialista, o grupo tem um elevado conhecimento técnico e experiência no mundo do cibercrime, mas gosta demasiado de **fama**.

"São excelentes, muito bons mesmo no que fazem. Mas gostam muito de fama. **E esse é o pior lado do cibercrime — é quando gostam de fama.** Eles espalham o nome deles em todo o lado, querem estar nos holofotes", analisou João Lucas Brasio, que acredita que os grupos de quem ninguém ouve falar e que deixam poucas pistas sobre os ataques que fazem representam as maiores ameaças à cibersegurança mundial.

Bruno Castro, em declarações ao Observador, discordou de João Lucas Brasio, já que acredita que "a fama é um mito urbano". Para o especialista português da Visionware, o "conceito de fama" serve para os *hackers* se "autopromoverem".

"O facto de serem conhecidos dá-lhes mais poder: quanto mais conhecidos forem, mais reconhecidos no mercado ficam e mais valiosos são os seus serviços criminosos"

Bruno Castro

As motivações do Lapsus$ são "a procura de angariar dinheiro", garantiu Bruno Castro. "No final do dia, o objetivo final é o dinheiro. É um modelo de negócio muito maduro, muito profissional, muito bem alinhado tecnicamente, altamente mutável, sempre em evolução, mas sempre numa ótica de crime organizado".

A Microsoft parece partilhar da opinião dos especialistas sobre o grupo ao qual denominam de DEV-0537. Para esta empresa, **os *hackers* não se preocupam em esconder "o seu rasto" e "vão mais longe** e anunciam os seus ataques nas redes sociais".

A imagem de marca do Lapsus$ é mesmo anunciar os ataques no Telegram e provocar as vítimas ao expor publicamente informações roubadas. Porém, este grupo chegou a ir mais longe ao invadir vídeochamadas Zoom de empresas que comprometeram, apenas para provocar os funcionários que tentavam resolver as consequências do ataque.

A despreocupação em esconder os ataques e as informações que foram sendo disponibilizadas publicamente ajudaram a polícia de Londres e peritos em cibersegurança a investigar o Lapsus$ e a identificar aquele que pode ser um dos líderes do grupo.

"White", o adolescente que pode ser um dos cabecilhas do grupo

Tão rápido e habilidoso a *hackear* que os investigadores pensavam que estavam a observar um programa automático. Foi assim que o adolescente de 16 anos que vive com a mãe perto de Oxford, no Reino Unido, foi descrito pelas autoridades. Com a alcunha online de **"White" ou "Breachbase", o adolescente terá uma fortuna de cerca de 14 milhões de dólares** (cerca de 12,7 milhões de euros), dinheiro que terá conseguido com ataques informáticos.

As autoridades britânicas anunciaram a 23 de março a detenção de sete jovens com idades entre os 16 e os 21 anos suspeitos de estarem ligados ao Lapsus$. O membro mais novo do grupo será "White", o rapaz com espectro de autismo grave, que foi descrito pelos investigadores como uma "mente brilhante" do crime. A polícia não confirmou a detenção do adolescente, avançando a Bloomberg que o rapaz já estava a ser investigado há um ano.

O jornal Expresso revelou que a unidade de cibercrime da Polícia Judiciária (PJ) terá ajudado na detenção de "White". Fontes próximas da investigação admitiram que o grupo Lapsus$ já fez "vários estragos pelo mundo". **O Observador contactou a PJ, mas não obteve respostas sobre o envolvimento das autoridades portuguesas** na investigação britânica.

Inicialmente, a imprensa internacional avançava que os sete adolescentes tinham sido libertados, apesar de permanecerem sob investigação. Mas, informações mais recentes davam conta que dois rapazes de 16 e 17 anos tinham sido formalmente acusados por crimes de acesso não autorizado a computadores para prejudicar o acesso a dados e um crime de fraude por representação falsa.

As autoridades não revelaram a identidade dos adolescentes investigados. Então, como é que as informações pessoais sobre "White" foram tornadas públicas? A morada dos seus pais, que estão separados, o carro da família e uma fotografia da casa da mãe foram publicadas online por rivais.

Segundo a revista The Verge, o adolescente tinha comprado o domínio de Doxbin, um site onde as pessoas podem encontrar e partilhar informação pessoal sobre outros. Mas, depois do negócio ser fechado, algo deverá ter corrido mal porque **"White" partilhou ilegalmente a base de dados do Doxbin na conta do Telegram do Lapsus$.** Como vingança, o Doxbin revelou informações pessoais sobre o adolescente.

A mãe disse à imprensa não ter conhecimento das informações que tinham sido reveladas e mostrou-se perturbada por fotografias da sua casa terem sido partilhadas. À BBC, o pai do rapaz afirmou saber que o filho "é bom com computadores", mas pensava que passava muito tempo a "jogar videojogos". "Ele nunca falou sobre *hacking*", garantiu o pai de "White".

Até ao momento, as informações apontam para que o Lapsus$ tenha colaboradores em vários países e continentes. As autoridades suspeitam que outro membro importante para o grupo possa residir no Brasil e que os piratas informáticos sejam adolescentes.

O *hacker* russo D4rk R4bbit esteve doze meses a identificar membros do Lapsus$ e diz que há entre sete a 16 pessoas envolvidas no grupo de hackers, acreditando também que sejam todos adolescentes. Os **jovens são descritos como "extremamente desleixados", "descuidados e imprudentes"**. Porém, D4rk R4bbit reconheceu em entrevista à CNN Portugal que estes piratas informáticos "trabalham tão depressa" que é "difícil acompanhá-los".

O especialista português Bruno Castro mostrou-se mais cauteloso e pediu que as pessoas não se deixassem enganar. “Estamos a falar de redes criminosas altamente maduras, um modelo de negócio muito bem sustentado. Quem trabalha neste tipo de grupos é, tipicamente, profissional da área. Haverá obviamente elementos jovens porque estamos a falar de novas tecnologias, mas não se deixe enganar pelo conceito do miúdo em casa a fazer este tipo de brincadeira. Não, não é. São perfis altamente profissionais, com muito conhecimento desta área”, salientou.

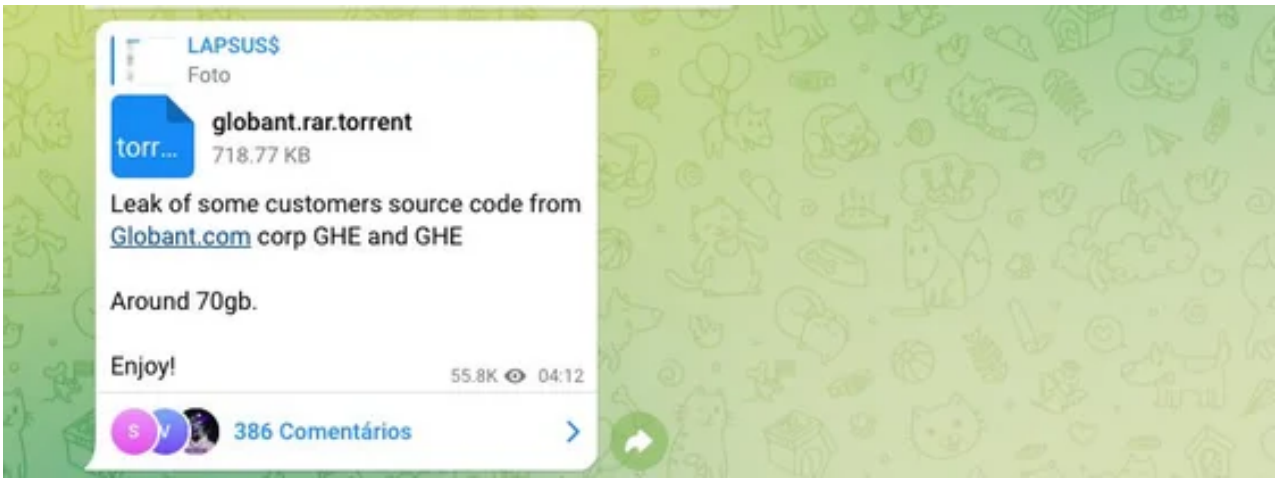
As férias anunciadas no Telegram que duraram (muito) pouco

O grupo Lapsus$ anunciou no dia 23 de março, no mesmo dia em que as autoridades realizaram as sete detenções, que alguns membros “iam entrar de férias”. O aviso foi deixado no Telegram: “Podemos ficar quietos durante algum tempo. Obrigada por nos entenderem — vamos tentar fazer *leaks* [revelar informações] o mais rápido possível”.

“Podemos ficar quietos durante algum tempo.” O anúncio das “férias” dos hackers

E as férias, realmente, não duraram muito tempo. Uma semana depois, o grupo disse estar “de volta” e fisgou como alvo a Globant, uma empresa de desenvolvimento de software com mais de 23 mil funcionários. Em comunicado, a empresa afirmou que os ***hackers* tiveram acesso a uma quantidade limitada de dados, ao código-fonte e a documentos “de um número limitado de clientes”**, num total de 70 *gigabytes* (GB) de conteúdos.

A Globant, com clientes muito conhecidos como a Google, a Meta e a Apple, afirmou estar a investigar o ataque que pode ter comprometido seriamente os seus dados confidenciais e a sua segurança. No Telegram, o Lapsus$ partilhou capturas de ecrã com mais de duas dúzias de pastas que têm o que os *hackers* dizem ser o código-fonte dos clientes da Globant.



O Lapsus$ partilhou no Telegram informações sobre a Globant

O regresso das curtas férias mostrou que a inatividade face às detenções não foi o início do fim para os *hackers*, que prometem continuar a comprometer a segurança e a privacidade de algumas das maiores empresas do mundo. Há ainda várias questões sem resposta. A verdadeira identidade e extensão do grupo é uma delas. Mas uma é de especial importância: **será que o Lapsus$ é verdadeiramente uma ameaça para a cibersegurança mundial?**