Opinião

O cibercrime e o vírus

David Silva Ramalho
7 Abril 2020

142

Se o vírus mostra uma invulgar capacidade de se adaptar a novos ambientes de propagação, o cibercrime mostra semelhantes capacidades de mutação e aproveitamento oportístico das circunstâncias.

A Europol divulgou na passada sexta-feira o seu relatório sobre cibercrime e desinformação durante a pandemia Covid-19. A principal conclusão, de resto já anunciada pela mesma entidade no mês passado, é óbvia: o maior volume de utilização de tecnologias de informação durante a quarentena criou terreno fértil para o aumento, a adaptação e a diversificação do cibercrime.

As notícias publicadas sobre a matéria ao longo das passadas semanas indicam isso mesmo. Para além das habituais burlas online – não confundir com burlas informáticas, que são crimes diferentes –, do recente *zoombombing* (a prática de entrar em reuniões alheias no Zoom, geralmente para exibir imagens de teor sexual) e da disseminação de *malware* em mapas interativos com supostas atualizações do minuto da evolução da Covid-19, têm-se multiplicado esquemas de venda ilegal de produtos médicos, em muitos casos contrafeitos, como máscaras, medicamentos antivíricais e cloroquina para a malária, ou mesmo ataques a infraestruturas críticas de saúde, como aconteceu recentemente com o hospital de Brno, na República Checa, ao ponto de levar ao adiamento de cirurgias urgentes e à necessidade de transferir pacientes em estado grave para outros hospitais.

Não foi, porém, nestes pontos – pelo menos não diretamente, embora alguns sejam referidos lateralmente no relatório – que a Europol se focou. As ameaças destacadas no relatório, seja pela sua frequência, seja pelo potencial de se virem a agravar num futuro próximo, foram cinco: *ransomware*, ataques DDoS (*distributed denial-of-service*), exploração sexual de crianças, atividade na *Dark Web* e *fake news*.

O *ransomware* corresponde a um dos cibera taques mais comuns, precisamente por ser um dos mais fáceis e lucrativos. O atacante, recorrendo a técnicas de *phishing* ou de *spear phishing* – muitas vezes através de engenharia social para se fazer passar por um conhecido do atacado, noutros casos simplesmente enviando-lhe um link malicioso disfarçado de um website legítimo –, consegue aceder ao computador do visado, ou mesmo ao servidor de uma empresa, e encriptar toda a informação que aí se encontra armazenada. Em troca da libertação da informação, o atacante exigirá ao visado o pagamento de uma quantia, geralmente em bitcoins ou ethereum, e dar-lhe-á um pequeno tutorial sobre como utilizar moedas virtuais para que possa fazer a transferência. Estes ataques, que já há muito são dirigidos a pessoas singulares e a empresas, e que, em algumas modalidades de maior ou menor sofisticação, estão centralizadas em grupos de hackers já conhecidos, têm aumentado em frequência e em intensidade, havendo inclusivamente campanhas de recrutamento, por parte destes grupos ou de outros que entretanto surgiram, de novos colaboradores tecnicamente habilitados para o efeito.

Os ataques de DDoS, ou ataques distribuídos de negação de serviço, apenas recentemente começaram a mostrar sinais de poderem vir a aumentar. O objetivo deste tipo de ataques é provocar um congestionamento no acesso a um concreto servidor, serviço ou rede, e torná-lo inoperacional. O aumento exponencial controla uma rede de computadores infetados, chamados de *bots* (que podem ser os computadores de qualquer um de nós) e, sem que os seus utilizadores saibam, dirige simultaneamente milhares de pedidos de acesso, por exemplo, a um website, de modo a esgotar a sua capacidade de resposta e levar a que deixe de estar online. Com o aumento do teletrabalho e, portanto, do número de utilizadores a aceder remotamente aos sistemas informáticos das empresas, estes ataques passaram a tornar-se mais fáceis por os recursos da rede estarem já próximos do limite. O impacto destes ataques, para além de ser economicamente significativo quando dirigido a empresas, pode levar à paralisação de infraestruturas críticas na área da saúde ou de operadores de serviços essenciais.

Em terceiro lugar, a Europol destaca que o período de isolamento tem levado igualmente ao aumento de ilícitos relacionados com a exploração sexual de crianças. Os ilícitos destacados no relatório são essencialmente dois: de um lado, a procura de ficheiros de pornografia infantil, seja através do acesso a websites ou *fóruns* na *Dark Web*, seja através de *downloads* em redes de *peer-to-peer* (só em Espanha o *download* destes ficheiros aumentou em 25% no espaço de duas semanas); de outro lado, o aliciamento de menores para fins sexuais, aproveitando a circunstância de os menores estarem agora mais tempo ligados à Internet, sem supervisão de adultos e à procura de interação social que compense o seu atual estado de isolamento.

Na *Dark Web*, o cibercrime também se adaptou rapidamente. Desde a comercialização de produtos relacionados com a Covid-19, como as já referidas máscaras e mesmo *kits* para testar a doença, até à comercialização de serviços de ataque informático para os fins já referidos, como os conhecidos *ransomware-as-a-service* ou *DDoS-as-a-service*, a *Dark Web* oferece agora um conjunto de produtos e serviços que, embora não sejam inovadores, apresentam um novo *branding* e com isso captam o interesse de outro público.

A última ameaça identificada pela Europol em Portugal não tipificada como crime, e cuja criminalização se pode considerar no mínimo problemática consiste nas conhecidas campanhas de desinformação através de *fake news*. O excesso de informação sobre o tema da Covid-19, a despreocupação dos utilizadores na confirmação da genuinidade das notícias que surgem nos seus *feeds* e a procura de fontes que corroborem um conjunto de crenças e convicções não demonstradas cientificamente, criam as condições adequadas à propagação de teses e de teorias da conspiração frequentemente utilizadas para fins lucrativos ou mesmo por entidades com apoio governamental para fins políticos.

As tendências identificadas pela Europol são pouco mais do que adaptações de práticas já amplamente difundidas no cibercrime, às quais foi dada uma nova *roupagem*. O que verdadeiramente as torna perigosas, mais do que os atacantes, são as vítimas. É a transição do trabalho de escritório para computadores pessoais sem qualquer tipo de proteção, são as redes domésticas abertas ou com palavras-passe de acesso nunca alteradas, é a confiança cega no *e-mail*, é a crendice na informação minoritária ou na cura milagrosa, são os *downloads* despreocupados, são as compras impulsivas, são as empresas que sustem a respiração até a crise pandémica acabar, ao invés de disseminarem boas práticas – já nem digo outro tipo de investimento –, é o tempo, é o

Stream
Home Discover My content + Create Search
Live event
Channel
Welcome back, Carolina
Sponsored
Prémio Inovação
Watch now
Invite your coworkers to upload videos. Everyone in your company can contribute.

Precisamos de si, caro leitor, e nunca precisamos tanto como hoje para cumprir a nossa missão. Que vive lá disso? Que leia as nossas notícias, que partilhe e comente, que sugira, que critique quando for caso disso. A contribuição dos leitores é essencial para preservar o maior dos valores, a independência, sem a qual não existe jornalismo livre, que escrutine, que informe, que seja útil.

A queda abrupta das receitas de publicidade por causa da pandemia do novo coronavírus e das suas consequências económicas torna a nossa capacidade de investimento em jornalismo de qualidade ainda mais exigente.

É por isso que vamos precisar também de si, caro leitor, para garantir que o ECO é económica e financeiramente sustentável e independente, condições para continuar a fazer jornalismo rigoroso, credível, útil à sua decisão.

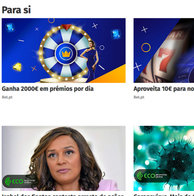
De que forma? Contribua, e integre a Comunidade ECO. A sua contribuição faz a diferença,

Ao contribuir, está a apoiar o ECO e o jornalismo económico.

António Costa
Publisher do ECO

5€ 10€ 20€ 50€

Contribua



Zurich e CYE protegem empresas ante riscos de cibersegurança

ECO Seguros, 17 Fevereiro 2020

A colaboração com a CYE "permite oferecer aos clientes uma solução cibernética de última geração", afirma Sierra Signorelli, responsável para área de subscrição em seguros comerciais na Zurich.

LMS é a solução tecnológica para sociedades de advogados

Thalassiano Medeiros, 6 Abril 2020

Assine já

ACT a travar despedimentos? Advogados dizem que é ilegal

Isabel Patrício, 6 Abril 2020

Para si

Listas personalizadas por Jetpack

Ganha 2000€ em prémios por dia
Bet.pt

Aproveita 10€ para novos registos
Bet.pt

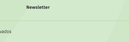
Bónus de Boas-Vindas até 1.200€
Bet.pt

Isabel dos Santos contesta arresto de ações da NOS

Coronavírus. Mais de 65 mil mortos em todo o mundo

Travão no vírus anima investidores. Bolsa ganha mais de 1,5%

Empresas estão a pedir 150 euros às farmácias por máscaras



"Estamos em negação sobre efeitos da crise no nível de vida"

De 4% a 20%. De que tamanho vai ser a recessão em Portugal?

Populares

Search the Web

4 Medidas em Portugal foram das mais rápidas da Europa
3 Abril 2020

5 Dona do Pingo Doce vai dar prémio de 500€ a cada funcionário
6 Abril 2020

6 Alunos até aos 9? ano passam a ter aulas através da televisão
4 Abril 2020

© Copyright ECO 2020 Swipe News, SA. Todos os Direitos Reservados