Economia

RICARDO GRAÇA

Empresas da região alvo de ataques informáticos com pedido de resgate

Ransomware Nas últimas semanas, várias empresas da região foram alvo de ataques informáticos com pedido de resgate. Questão da segurança informática é cada vez mais relevante

Raquel de Sousa Silva
raquel.silva@jornaldeleiria.pt

Ryuk. Será este o nome do vírus que atacou a rede da Geocam, fazendo com que a empresa de moldes da Martingança perdesse muita informação da área de projecto e de contabilidade. Como esta, várias outras empresas da região foram nas últimas semanas alvo de *ransomware*, ataques com pedido de resgate, que chegam a atingir milhares de euros.

No caso da Geocam, os *hackers* pediram cerca de 30 mil euros (em *bitcoins*) para fornecer a chave que permitiria recuperar o acesso aos dados que tinham sido encriptados com o ataque. Paulo Monteiro, gerente da empresa, contou ao JORNAL DE LEIRIA que, segundo apuraram os técnicos chamados para resolver o problema, o vírus terá estado instalado na rede (que conta já com 60 PC e seis servidores) durante algum tempo antes de a empresa deixar de conseguir aceder aos dados, o que aconteceu no passado dia 19. "Quando os funcionários chegaram às seis da manhã e quiseram começar a trabalhar não conseguiram abrir os ficheiros necessários".

Durante aquele tempo, o vírus "foi retirando informações para no momento certo correr o programa e encriptar todos os nossos dados. Onde não conseguiu entrar, pura e simplesmente formatou os nossos servidores", explicou o empresário num alerta que publicou na rede profissional Linkedin. A empresa, que participou o caso à Polícia Judiciária, ainda negociou e conseguiu baixar o valor do resgate para metade, mas acabou por não pagar qualquer verba. "Não iríamos conseguir recuperar os dados formatados, de qualquer forma", justifica o gerente.

Quando falou com o JORNAL DE LEIRIA, esta segunda-feira, ainda não se sabia exactamente como é que o vírus tinha entrado na rede da empresa, já que a prioridade foi recuperar o máximo de dados possível. Como tem servidores de *backup*, a Geocam conseguiu recuperar muita da informação, mas houve dados que se perderam. Agora vai reforçar ainda mais a segurança, divindo a informação por mais servidores e desligando da rede os que armazenam *backup*. Serão ligados apenas uma vez por semana para actualizar dados.

Segundo foi possível apurar, às empresas alvo deste tipo de ataques são quase sempre pedidos resgates de 30 mil euros. A maioria não paga. Quando percebem que foram atacadas, as empresas começam por verificar os sistemas de *backup* e se estes estiverem operacionais iniciam por aí a reposição dos ficheiros danificados. Mesmo não havendo cópias, acabam por tentar juntar toda a informação que não tenha sido en-

Os números

30

mil euros (em *bitcoins*) é o valor de resgate que tem sido pedido às empresas atacadas

3,7

milhões de dólares terão sido extorquidos desde Agosto de 2018 a empresas de todo o mundo, segundo estimativas da CrowdStrike e da FireEye

criptada e começam daí a tentar repor os dados, explicam alguns dos profissionais de informática ouvidos.

"São muito raros os que pagam o dito resgate. Na nossa opinião, não convém fazer o pagamento dos resgates, sendo que se o fizer a empresa poderá ser considerada propicia a um novo ataque, visto que quem paga a primeira vez talvez pague a segunda", acrescentam.

"Pagar é sempre um risco", diz igualmente Mário Afonso, director técnico da Lansys, empresa da Marinha Grande que actua na área das soluções de infra-estruturas, *backups* e segurança informática. Aponta o caso de uma empresa que pagou e a quem foi fornecida a chave para desencriptar os dados, mas diz que nem sempre isso acontece. A mesma sorte não teve uma outra empresa da região. "Pagou, mas isso não lhes resolveu o problema", conta por sua vez Paulo Monteiro.

O *mail* é uma das principais vias de entrada deste tipo de vírus nas redes das empresas. "Mas há também os chamados ataques brutos", diz Mário Afonso. Com estes, "os *hackers* testam a vulnerabilidade dos sistemas, até encontrarem uma brecha que possa ser decifrada por uma *password*. Fazem constantes ataques para a descobrir, acabando por conseguir: pode demorar horas ou dias. Depois é só entrar na rede".

Nenhuma empresa está imune, frisa o técnico. "Não é uma questão de saber se vai acontecer. É quando vai acontecer. Dificilmente alguém estará livre. São atacadas grandes empresas mundiais, com bons sistemas de segurança informática. Logo, empresas sem grandes cuidados nesta matéria mais facilmente são atacadas", frisa o director técnico da Lansys.

Como podem as empresas precaver-se? "Apostar na segurança de perímetro, em *firewalls*, em sistemas anti-vírus, na protecção de mails", enumera. "Muito importante é igualmente a formação das pessoas, porque muitas vezes, por falta de conhecimento, abrem *mails* que não são fidedignos". Depois, "e muito importante, há que apostar também em boas cópias de informação, em *backups*. Mas não apenas os do dia-a-dia. Deve haver a preocupação de ter fora da rede da empresa cópias de segurança, para o caso de haver um ataque generalizado", diz o responsável da Lansys.

"Mas isto é algo com que as empresas não têm estado muito preocupadas, porque têm a percepção de que é um custo não produtivo", constata Mário Afonso, dizendo que estes *backups* devem ser encarados na mesma óptica do seguro do carro: temos de o ter, mas esperamos que nunca seja preciso accioná-lo.

"Este tipo de ataque é recorrente. Ninguém está imune", diz igualmente António Poças. Para o administrador da inCentea, grupo de Leiria que presta serviços nas áreas da tecnologias de informação, comunicação e gestão, há que apostar fortemente na protecção das redes. "Não se investe o que se devia na protecção de perímetro. Ainda se encara este aspecto como um custo e não como um verdadeiro investimento em segurança informática", constata.

"Quanto mais os colaboradores estiverem familiarizados com este tipos de ataques, e mais informação tiverem sobre os mesmos, menor a possibilidade de clicarem em *links* fraudulentos", alertam por sua vez David Barata e Ricardo Romeiro, respectivamente técnico de informática e comercial da Norma 6 - Tecnologias de Informação, de Leiria.

Por outro lado, para se precaverem deste tipo de ataques, as empresas devem apostar num "sistema completo de *backups* interno". Além disso, recomendam estes profissionais, "é necessário um segundo *backup* externo às instalações da empresa, para proteger a informação (sempre com chaves de encriptação), para prevenir *ransomware*". Segundo explicam, existem soluções como *firewalls* (que conseguem filtrar toda a informação que entra e sai da rede informática), antivírus e aplicações anti-*ransomware* instaladas em todos os postos de trabalho da empresa. "Com estes sistemas a funcionar em conjunto, conseguimos detectar o início de um ataque, sendo de imediato bloqueados os equipamentos onde se detecte o *ransomware* em execução", explanam.