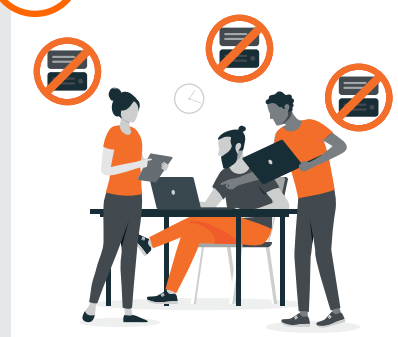
# Vulnerabilidades de software negligenciadas

Podem ser evitadas muitas perdas através da correção de software vulnerável antes que os cibercriminosos tenham a oportunidade de o explorar. Os exemplos de perdas abaixo destacam a importância de manter o software atualizado e detalham o processo de investigação para avaliar como as vulnerabilidades conhecidas são exploradas e as perdas resultantes ajustadas.

## - Alerta para a vulnerabilidade dos servidores

1



**1. O evento**

A 16 de julho, a equipa de TI da empresa Exemplo foi contactada por vendedores externos para indicar que não conseguiam utilizar quaisquer sistemas. As estatísticas do servidor monitorizado mostraram que vários sistemas estavam offline. Durante uma investigação inicial, a equipa de TI descobriu uma mensagem que indicava que os servidores estavam encriptados. Concluiu que a empresa tinha sido vítima de um ataque de ransomware. A equipa de TI da empresa Exemplo contactou o Centro de Resposta a Incidentes Cibernéticos da Chubb, tendo sido contratados um gestor de incidentes e especialistas forenses em TI para apoiar a investigação.

A inspeção inicial dos sistemas revelou que o autor da ameaça tinha comprometido grandes partes da rede e da infraestrutura.

2

**2. O problema**

Em resposta, a empresa Exemplo conteve rapidamente o ataque, desligando os servidores. No entanto, nessa altura, o autor da ameaça já tinha encriptado os servidores virtualizados e os hipervisores nos centros de dados da empresa. Aquando da avaliação das opções de recuperação, descobriu-se que era possível restaurar totalmente o ambiente informático com cópias de segurança, pois o autor da ameaça não tinha conseguido encriptar ou danificar as mesmas. A estratégia de cópia de segurança da empresa Exemplo foi atualizada nos 12 meses anteriores para proteger melhor o seu ambiente informático de ataques de ransomware, mantendo cópias de segurança em armazenamento a frio e a autenticação em servidores de cópia de segurança separados do Active Directory.

A partir do dia seguinte, os investigadores de TI e os especialistas forenses ajudaram a empresa Exemplo a avaliar a situação e a comunicar com o autor da ameaça, dando prioridade à recuperação de ativos. Ao mesmo tempo, investigaram em termos forenses a causa e o impacto do incidente para favorecer uma recuperação segura e protegida. Esta investigação consistiu em verificar se o autor da ameaça tinha exfiltrado dados para fins de extorsão, incluindo o controlo da natureza e da quantidade de dados declaradas no pedido de resgate.

A análise dos dados de registo das cópias de segurança demonstrou que, a 19 de junho, cerca de um mês antes, o autor da ameaça tinha iniciado sessão a partir de 6X.XXX.XX.232 num servidor VPN SSL alojado na Europa com credenciais pertencentes à conta “Fred.Bloggs”. O servidor VPN era gerido localmente e executava a versão 6.2.0-vr, uma versão desatualizada. Este início de sessão teve origem num IP conhecido por ser um nó de saída TOR, o que era suspeito, pois, normalmente, um utilizador não iniciaria sessão com a rede TOR. O autor da ameaça autenticou-se novamente cerca de 25 minutos depois, utilizando, desta vez, um IP geolocalizado num país em que a empresa Exemplo não operava.

O autor da ameaça aumentou os seus privilégios de acesso em menos de uma hora, acedendo a uma conta de administrador do domínio. Conseguiu fazê-lo porque as credenciais desta conta estavam armazenadas num ficheiro de configuração em todos os dispositivos Windows ligados ao domínio. Isto permitiu que o autor da ameaça se movesse lateralmente entre os servidores e hipervisores localizados no Reino Unido e na Alemanha que suportavam as operações europeias da empresa Exemplo.

Em julho, o autor da ameaça criou persistência ao instalar um software de acesso remoto e uma ferramenta de distribuição de software. Isto permitiu-lhe implementar e disseminar o ransomware em todos os servidores do domínio. Felizmente, os terminais, nomeadamente os portáteis e as estações de trabalho, conseguiram bloquear o ransomware através de um agente antivírus avançado que não era executado nos servidores.

Nenhum registo apresentava tentativas de início de sessão falhadas a partir da conta “Fred.Bloggs”, pelo que se determinou que o autor da ameaça tinha credenciais válidas, não tendo efetuado um ataque por força bruta. Os registos mostram também a atividade do código do autor da ameaça que explora uma vulnerabilidade conhecida - CVE-2022-123XXX - na versão 6.2.0-vr do software VPN. Quando explorada, a vulnerabilidade permite a um utilizador obter credenciais válidas utilizadas recentemente. O autor da ameaça confirmou este método de entrada no pedido de resgate e durante as negociações.

3

**3. A solução**

Após confirmar que as cópias de segurança não tinham sido afetadas por malware, os esforços de recuperação de dados e sistemas, bem como o trabalho de atualização da configuração continuaram durante os cinco dias seguintes. Estes esforços foram bem-sucedidos, pelo que não foi necessário continuar a negociar com o autor da ameaça e não foi pago qualquer resgate.

Conforme indicado na Base de Dados Nacional de Vulnerabilidades e no website de assistência do fornecedor de software VPN, foi descoberta uma vulnerabilidade crítica na versão 6 do software. Esta situação permitiu o roubo de credenciais e a entrada no sistema, tendo sido identificada pela primeira vez em janeiro deste ano. O Common Vulnerability Scoring System (CVSS) atribuiu-lhe uma classificação de criticidade de 9,8 e o identificador CVE-2022-123XXX. O fornecedor de software criou uma correção para estas vulnerabilidades a 2 de fevereiro (versão 6.2.1-vr) e, no mesmo dia, enviou um e-mail aos seus clientes, incluindo a empresa Exemplo, aconselhando os utilizadores a aplicarem a correção o mais rapidamente possível.

4

**4. O resultado**

Decorreram 137 dias entre o lançamento da correção e o momento em que a vulnerabilidade foi explorada. As cláusulas de seguro de resposta a incidentes, custos de recuperação de dados e sistemas, extorsão cibernética e perdas por interrupção da atividade foram todas inicialmente acionadas em resposta ao incidente cibernético, sujeitas aos limites, franquia e cosseguro aplicáveis a eventos de software negligenciado indicados no programa da apólice durante 137 dias.

A Chubb tramitou então o sinistro de acordo com o método padrão, revendo os custos de resposta a incidentes para o Gestor de Resposta a Incidentes, os especialistas forenses em TI, os advogados e os especialistas em relações públicas, as perdas por interrupção da atividade, os custos de recuperação de dados e sistemas, bem como as despesas por extorsão cibernética.

# Vulnerabilidades de software negligenciadas

## - Vulnerabilidade conhecida, sem correção

1

### 1. O evento

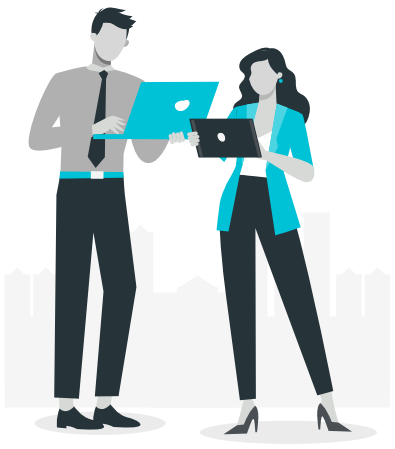
Num fim-de-semana, a empresa Exemplo detetou um acesso não autorizado aos seus sistemas informáticos e servidores. O acesso foi obtido através de uma vulnerabilidade conhecida, grave e comum que permitiu aos piratas informáticos acederem aos sistemas informáticos, servidores e dados da empresa Exemplo. Os piratas informáticos encriptaram ambos os sistemas e exfiltraram os dados.

2

### 2. O problema

Com os seus servidores inativos, a empresa Exemplo não conseguiu processar nem satisfazer as encomendas dos clientes. Os funcionários estimaram que, por cada 24 horas de inatividade dos servidores, a empresa perderia 750 000 euros de lucro. O pirata informático exigiu um resgate de 2 milhões de dólares para fornecer as chaves de desencriptação e não publicar os dados exfiltrados, ameaçando aumentar periodicamente o pedido se não recebesse o pagamento.

3



### 3. A solução

A empresa Exemplo comunicou o incidente assim que o descobriu, recorrendo rapidamente a um Gestor de Resposta a Incidentes que conseguiu efetuar a triagem do incidente com base nos factos iniciais. O Gestor de Resposta a Incidentes recorreu imediatamente a uma empresa forense especializada em TI para ajudar a empresa Exemplo na investigação e contenção.

A equipa de resposta a incidentes também prestou assistência à empresa Exemplo. Recorreu rapidamente a advogados, profissionais de relações públicas e especialistas em extorsão. A equipa implementou então uma estratégia de mitigação que incluíu a identificação de servidores que pudessem ser restaurados a partir de cópias de segurança.

Em última análise, não foi pago qualquer resgate após a equipa de TI e os especialistas em extorsão terem determinado que os dados exfiltrados não eram sensíveis. Descobriram que os sistemas podiam, em grande parte, ser restaurados a partir de cópias de segurança separadas de forma segura que não foram afetadas pelo incidente.

A equipa de resposta a incidentes contribuiu para a eliminação do ransomware dos servidores afetados e para a restauração dos sistemas, incluindo a correção que terá impedido a exploração da vulnerabilidade conhecida. A equipa de relações públicas ajudou a comunicar com os clientes e os advogados apoiaram a empresa Exemplo na notificação dos organismos legais e regulamentares necessários.

4

### 4. O resultado

As operações acabaram por ser totalmente restabelecidas. A equipa forense de TI forneceu um relatório 10 dias após o incidente que explicava o método pelo qual o acesso foi obtido, a CVE específica relacionada com a vulnerabilidade e a atenuação recomendada, incluindo a data em que as correções estavam disponíveis, mas não foram implementadas.

As cláusulas de seguro de resposta a incidentes, custos de recuperação de dados e sistemas, extorsão cibernética e perdas por interrupção da atividade foram todas inicialmente acionadas em resposta ao incidente cibernético. No entanto, o incidente teve origem numa vulnerabilidade conhecida que foi explorada. Isto foi confirmado pelo relatório forense de TI que estabeleceu que estava disponível uma correção na altura do incidente, mas que não foi aplicada. O relatório detalhava exatamente quando é que o pirata informático obteve acesso ao sistema e destacava o período em que os sistemas da empresa Exemplo não estavam corrigidos. Isto permitiu-lhe aplicar o cosseguro e o sublimite corretos no âmbito dos limites de eventos de software negligenciados.