

Este tipo de ameaças aumentou 500% no primeiro trimestre do ano, comparado com o mesmo período de 2018

Ransomware

Novas estratégias de defesa?

Pagar ou não pagar, eis a questão

O ransomware continua a aumentar, afectando não só indivíduos e empresas mas também organizações públicas. Um retrato do que está a acontecer numa "crise" cada vez mais sofisticada.

PEDRO FONSECA

No primeiro semestre deste ano, 22 cidades norte-americanas foram afectadas por uma "epidemia" de ransomware. É um pico pouco usual mas que reflecte um crescimento nestas operações.

O ransomware - contração dos termos em inglês resgate e software - cifra os dados inseridos nos computadores ou pode evitar o acesso ao ecrã do utilizador. O objectivo é obter um pagamento do utilizador ou da organização afectados por este tipo de ataque, normalmente efectuado por transacções em moedas virtuais como os bitcoins, por serem difíceis de rastrear.

Não há qualquer garantia que, após o pagamento, o computador seja desbloqueado. Mas não o fazer significa a possibilidade de nunca mais aceder aos dados actualizados, especialmente se não se efectuou cópias de segurança ("*backups*") recentes.

Ao pagar, pode não receber nada mas também pode ser que o atacante resolva o problema. Mas um pagamento não significa que os ataques parem: um computador infectado com ransomware pode ser posteriormente atacado pelo mesmo atacante ou outro que descobriu a falha.

Apesar dos constrangimentos que possa provocar às organizações, o conselho generalizado é para não pagar aos atacantes, recorda Daniel Castro na revista *Government Technology* (edição de Setembro).

O vice-presidente da *Information Technology and Innovation Foundation* (ITIF) realça que este foi "*o ano dos ataques ransomware*": este tipo de ameaças aumentou 500% no primeiro trimestre do ano, comparado com o mesmo período de 2018, e "*uma série recente de incidentes mostrou que a governação estatal e local foram alvos particularmente lucrativos*".



Encryption Ransomware:
cifra pastas e ficheiros pessoais

Neste cenário, começa a existir uma linha de acção que defende o não pagamento especialmente por entidades públicas. Com as organizações concertadas nesse sentido, os atacantes irão procurar outros alvos.

O global WannaCry

O estado de emergência relativamente ao ransomware surgiu em Maio de 2017, com os ataques globais do software *WannaCry*.

Naquela que foi considerada uma "*epidemia global*", o *WannaCry* (conhecido também por *Wanna Decryptor*, *Wanna Crypt* ou *WannaCrypt0r*) afectou equipamentos com o sistema operativo Windows - apesar da Microsoft já ter solucionado o problema.



Mobile Ransomware:
afecta dispositivos móveis, sobretudo com o Android

A severidade do problema foi enorme e levou a empresa a criar uma solução para as versões antigas do XP, Windows 8 e Windows Server 2003 .

A *Europol* calculou foram afectados 200 mil computadores em 150 países. Terão sido mais de 250 mil equipamentos, com perdas financeiras a atingirem os quatro mil milhões de dólares, segundo o vice-presidente da ITIF. A revista *ZDNet* contabilizou "*300 mil vítimas*".

Foram divulgados problemas no Serviço Nacional de Saúde britânico e também do Irão ou Egipto, no ministério russo do Interior, numa operadora telefónica em Espanha e noutra de energia no Cazaquistão, em quase 30 mil entidades na China e em fabricantes automóveis na França, na Roménia ou na Eslovénia.

Portugal não escapou mas como o ataque se iniciou a 12 de Maio, a tolerância de ponto na Administração Pública antes das tradicionais comemorações em Fátima mitigaram o problema.

A vulnerabilidade terá sido desenvolvida pela *National Security Agency* (NSA) norte-americana e disseminada pelo grupo de *hacking Shadow Brokers*. Pouco depois, foi revelado o *NotPetya*, alegadamente criado pelas autoridades russas para causar problemas na Ucrânia.

Tudo isto levou o presidente da *Microsoft*, Brad Smith, a criticar os governos que "*armazenavam*" este tipo de vulnerabilidades. Por seu lado, os *Shadow Brokers* anunciaram ter uma solução para resolver o problema - a quem pagasse...

Castro declara que "*poucas organizações pagaram o resgate*" e, quatro dias depois do início do ataque, os atacantes apenas tinham recebido 72 mil dólares. "*Meses mais tarde, aparentemente lucraram menos de 150 mil dólares*", afirmou.

A razão para este insucesso - do ponto de vista dos atacantes, obviamente - deve-se a que, mesmo após o pagamento, os ficheiros não foram desbloqueados e isso foi divulgado, desincentivando potenciais pagantes.

Novas estratégias

Algo mudou após os ataques com o *WannaCry*. Em vez de atirar em todas as direcções para ver quem era atacado com sucesso e depois pedir o resgate, os ataques passaram a ter alvos específicos. As entidades públicas passaram assim a merecer a atenção des criminosos. Os casos sucederam-se, com maior impacto, mas é bom recordar que eles já vinham de trás.



Master Boot Record Ransomware: alteração à parte do disco rígido do computador que permite ao sistema operativo arrancar

Em 2015, um inspector da Polícia Judiciária alertou para o problema em Portugal. Em Fevereiro desse ano, um ataque de ransomware a um hotel na Áustria bloqueou o funcionamento das portas dos quartos. Os atacantes receberam um pagamento de 1.800 dólares e o hotel considerou substituir as chaves electrónicas por manuais para evitar este tipo de incidentes no futuro.

O lançamento dos televisores com ligação à Internet também captou o interesse dos ciberbandidos, como sucedeu nesse ano com *Darren Cauthon*. Ele recebeu um aviso no ecrã bloqueado da sua "*smart TV*" para pagar 500 dólares e assim poder desactivar o *ransomware Cyber.Police*, também denominado de *FLocker*, *Dogspectus* ou *Frantic Locker*.



Lock Screen Ransomware: bloqueia o ecrã do computador

Após a vaga *WannaCry*, o *Georgia Department of Agriculture* foi atacado com ransomware em Dezembro de 2017 mas não pagou, optando por accionar um seguro de protecção informática para ter técnicos a cuidar do sistema até este ficar a funcionar, o que conseguiu.

No ano seguinte, a cidade de Atlanta pagou "*milhões de dólares*" para recuperar os ficheiros atacados num ataque semelhante.

Este ano, algumas cidades norte-americanas também optaram por pagar neste tipo de ataques. Depois de, em Março, a cidade de *Jackson County* dispender 400 mil dólares, dois meses depois foi a vez de Baltimore ter os seus servidores informáticos atacados. O resgate pedido foi de três bitcoins - cerca de 18 mil dólares - por cada servidor ou, em alternativa, um pagamento total de 13 bitcoins para limpar o sistema.

Segundo Daniel Castro, o FBI pediu ao executivo camarário para não pagar, o que este cumpriu mas revelou-se uma estratégia dispendiosa: o director financeiro camarário "*estimou que o ataque custou a Baltimore pelo menos 10 milhões de dólares, a somar a mais oito milhões em receitas perdidas*".

Em Junho de 2019, três cidades (*Riviera Beach, Lake City e La Porte County*) pagaram cerca de 1,1 milhões de dólares em resgates - a primeira cerca de 600 mil dólares, *Lake City* quase 500 mil dólares (por bloqueio aos sistemas telefónico e de correio electrónico, e ao portal de pagamentos online), enquanto a última pagou cerca de 130 mil dólares para recuperar os dados camarários.

A 3 de Julho, diversas clínicas dentárias foram alvo de ataques semelhantes, embora através do seu fornecedor de serviços de cibersegurança *PM Consultants*.

A *Arbor Dental*, em *Longview*, ficou com os sistemas bloqueados e sem acesso aos registos dos pacientes. A PM não conseguiu resolver o problema e solicitou aos clientes que procurassem ajuda externa, após o que encerrou a sua actividade.

problema pagando aos autores do ataque, enquanto a primeira reportou o caso ao FBI.

A porta-voz da autoridade, *Melinda Urbina*, reconheceu que "*estes são os alvos que [os atacantes] procuram porque sabem que estarão mais predispostos a pagar para terem os seus serviços a funcionar*" para os seus clientes.

A situação em Portugal

Há vários casos reportados de ransomware ou de ataques a infra-estruturas sensíveis no nosso país.

Em Abril de 2015, Rogério Bravo, da brigada de cibercriminalidade informática da Polícia Judiciária, alertou como o ransomware era um dos ataques mais frequentes em Portugal. 80% das vítimas eram técnicos e revisores oficiais de contas (TOC e ROC, respectivamente), advogados e os programas de vencimentos nos agrupamentos escolares.

Um ataque informático às Forças Armadas em Novembro de 2018 visou "a rede de correio electrónico administrativo utilizado pelos militares e funcionários civis do EMGFA [Estado-Maior General das Forças Armadas], num total de cerca de 3,5 Gb de informação de emails exfiltrados".

A "*Advanced Persistent Threat*" (APT) ou ameaça avançada persistente foi o ataque "mais complexo e grave até ao momento" mas "não [houve] informação sensível afectada", assegurou o porta-voz das Forças Armadas à agência Lusa, em Abril passado.

A Fundação *Champalimaud* queixou-se em Julho de um "ataque informático sem precedentes, mas conseguiu ultrapassar a situação sem ceder a qualquer exigência dos atacantes". Em comunicado, a organização garantiu que ficou sem acessos mas "a privacidade dos doentes da fundação não foi violada".

Cerca de um ano antes, a José de Mello Saúde notificou a Comissão Nacional de Proteção de Dados (CNPS) de um ataque de ransomware às suas unidades, como o Hospital CUF Descobertas. O programa informático *SamSam* terá bloqueado o sistema informático da organização, sem afectar os dados dos pacientes, requerendo um pagamento que não terá sido feito.

A situação no país é "assustadora", sintetizou em Abril passado José Tribolet. Segundo este presidente do Departamento de Engenharia Informática do IST, "a fragilidade dos nossos sistemas vitais, os sistemas críticos que fazem a sociedade funcionar, é assustadora" em termos de cibersegurança, área em que o país sofre de uma "falta de pensamento".

O que este tipo de ataque revelou foi uma alteração no modo de ataque, passando de visar alvos directos para atingir gestoras de serviços para entidades externas.

Este ano, um ataque ao fornecedor *TSM Consulting Services* afectou 22 cidades, enquanto um ataque à *PerCSoft* afectou 400 clínicas dentárias nos EUA. Alegadamente, esta empresa terá resolvido o

A par com a carga de enorme trabalho que é limpar todo um parque bloqueado de máquinas externas, existe igualmente a questão da credibilidade que estas empresas pretendem assegurar em público. Mas, ao pagarem - como também sucedeu com

empresas de recuperação de dados e até seguradoras -, estão a incentivar os ataques.

Estas situações levaram a *Conference of Mayors* norte-americanos a pedir aos seus membros para não pagarem por ransomware, embora se desconheçam os efeitos da medida. A *Conference of Mayors* é uma organização apartidária de cidades com 30 mil ou mais habitantes, num total de mais de 1.400 municípios.

De irritação a sofisticada ameaça

Em meados de Setembro, a "crise" do ransomware estava a aumentar e a ter contornos mais sofisticados. Passou de "*uma irritação menor para os utilizadores de PCs para ser uma ameaça significativa a grandes empresas e até países*", segundo um artigo na revista *ZDNet*.

O cenário não está sequer a ser equacionado porque já aconteceu na África do Sul este ano. Um ataque de ransomware deixou Joanesburgo às escuras e a empresa *City Power* revelou que o ataque cifrou todas as suas bases de dados, aplicações e acesso à rede.

A *ZDNet* nota como "*a verdadeira surpresa não é que haja tantos ataques de ransomware mas que não existam mais, muitos mais*". Isto quando, a acreditar nos criadores de um programa de ransomware, o negócio é tão lucrativo que eles resolveram reformar-se no início do ano, após terem arrecadado dois mil milhões de dólares.

O que nos leva à questão essencial: perante um ataque, deve-se pagar o resgate? "Nunca é recomendado, principalmente porque não garante que seja a solução do problema", defende a *Europol*.

"A melhor forma de evitar este tipo de ataques é proteger os sistemas informáticos, dar formação adequada aos funcionários e ter planos de recuperação dos dados actualizados."

***Daniel Castro**, Vice-presidente do Information Technology and Innovation Foundation (ITIF) e Diretor do Center for Data Innovation*

As ameaças agravaram-se e se situações como a do hotel ou da "*smart TV*" podem parecer caricatas, outras há mais perigosas. Por exemplo, há receios de que ataques de ransomware possam afectar as mesas de voto electrónico nas eleições presidenciais de 2020 nos EUA.

Os ataques podem igualmente atingir infra-estruturas críticas como as redes de fornecimento de electricidade.

No início de Setembro, a *North American Electric Reliability Corp. (NERC)* revelou ter registado uma ciberagressão à rede eléctrica do país. A publicação *Environment & Energy News* não fala de ransomware mas note-se que este foi o primeiro "ciberevento" do género no país, cuja ocorrência foi detectada em Março passado.

Antes, o director de *National Intelligence* já tinha alertado que a Rússia podia tentar algo semelhante nos EUA ao ocorrido há cerca de três anos com a interrupção do serviço na rede eléctrica da Ucrânia.

"*Um número considerável de problemas podem surgir depois de pagar o resgate, por exemplo, a componente de recuperação do malware pode ter um 'bug' que faça com que os dados cifrados fiquem irremediavelmente perdidos, mesmo com a chave de decifragem correcta*".

Daniel Castro tem uma visão dividida: colectivamente, as cidades não devem pagar quaisquer resgates, por forma a desincentivar os atacantes; no entanto, de forma casuística, a tendência será para o fazer.

Ele e outros especialistas salientam que a melhor forma de evitar este tipo de ataques é proteger os sistemas informáticos, dar formação adequada aos funcionários e ter planos de recuperação dos dados actualizados.

Comentários e Sugestões:

www.afcea.pt

secretariado@afcea.pt