ALERTA CIBERCRIME

14 de abril de 2020

Mensagens Eletrónicas Fraudulentas:

- mensagens contendo *malware*;

- mensagens de *phishing* e

- extorsão por correio eletrónico.

1. No decurso do tempo de pandemia que se vive tem sido crescentemente sinalizado, embora de forma que não permite ainda quantificá-lo com rigor, um aumento dos fenómenos de cibercriminalidade. Este aumento assume ainda maior dimensão por haver milhões de pessoas em casa, em teletrabalho (ou a estudar em casa), utilizando meios de comunicação à distância e acesso remoto a sistemas informáticos, sem que tenha havido tempo ou possibilidade para cabal preparação, de pessoas e de sistemas, para esta nova realidade.

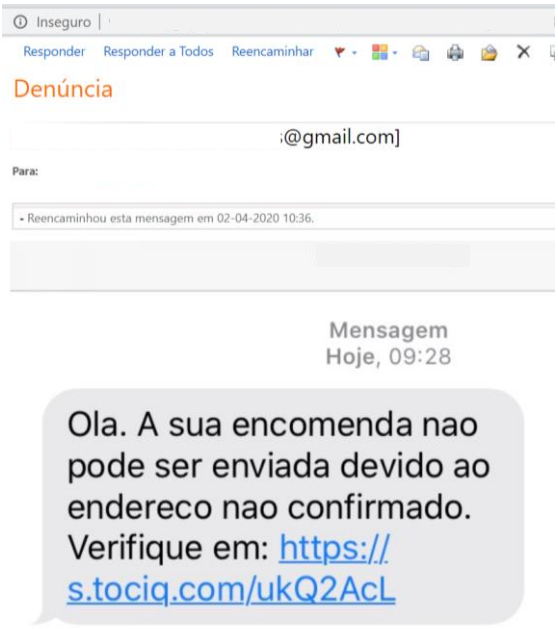
2. Tem sido detetado um número muito significativo de mensagens fraudulentas que veiculam a prática de cibercrimes. Designadamente, assim acontece com mensagens de *email* e SMS contendo *malware* (por exemplo *software* de *ransomware*). Noutros casos, igualmente muito numerosos (também *email* ou SMS), as mensagens contêm *links* para páginas de *phishing*. Tem sido também muitíssimo crescente o número de mensagens cujo propósito é a extorsão (estas apenas de *email*).

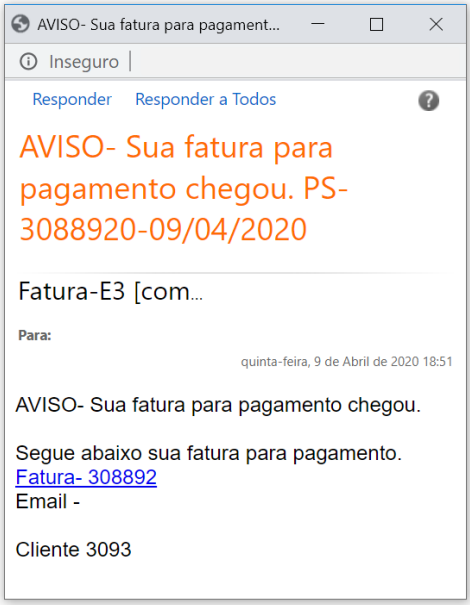
3. Como se disse, o aspeto comum a estas práticas criminosas é o de todas elas chegarem sob a forma de mensagem, seja de *email*, seja de SMS. Estas mensagens são remetidas por desconhecidos das vítimas, que obtêm os respetivos endereços de *email* ou números de telefone em bases de dados ilegítimas, à venda na Internet.
Trata-se de ações provenientes de múltiplos agentes, independentes uns dos outros que, replicando os vários modos de atuar prosseguem, cada um deles, interesses individuais, de lucro ilegítimo.

MENSAGENS CONTENDO *MALWARE*

4. Em geral, este tipo de ataques informático é perpetrado por via da difusão de *emails*, aos quais são anexados ficheiros dissimulados, contendo *malware*. No caso específico do *ransomware*, muito frequente, caracteriza-se pelo bloqueio total do computador da vítima, cujos dados ficam inacessíveis e, normalmente, são irremediavelmente perdidos – a menos que se pague um resgate ao atacante, o qual, em muito bom número de casos, é inconsequente (e portanto, a vítima fica sem os dados e sem a quantia que pagou…).
Mas são também possíveis opções diversas de *malware*.

Têm ocorrido casos deste tipo com mensagens de *email*, mas também com mensagens de SMS.

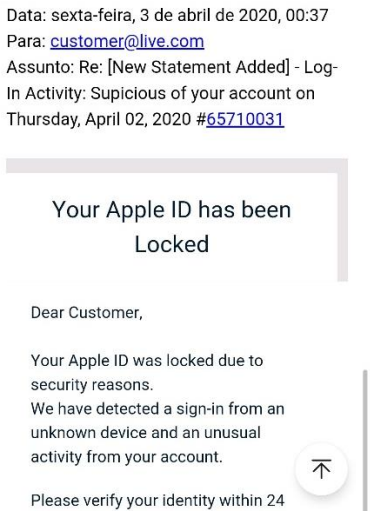




5. Recomenda-se particular cuidado com este tipo de mensagens, sempre que provenham de origem desconhecida e o destinatário ignore a que se referem. Frequentemente, contêm erros de ortografia ou de gramática, sendo incorreto o português utilizado. Os eventuais anexos ou *links* que contenham **não devem ser abertos** ou acedidos. A mensagem deve ser apagada.

MENSAGENS DE *PHISHING*

6. Têm igualmente sido sinalizadas de forma crescente mensagens fraudulentas de *phishing* – mensagens de *email,* mas também de SMS. Tais mensagens, expedidas sempre para inúmeros destinatários, anunciam provir de bancos ou outras instituições que suponham pagamentos (Apple, Netflix, Paypal, entre muitas outras). Os respetivos textos, imprimindo urgência, anunciam que o destinatário deve aceder a um *link*, que supostamente dá acesso à legítima página do banco ou outra instituição. No caso das mensagens de *email*, normalmente vem associada à mensagem o logotipo da instituição em causa.

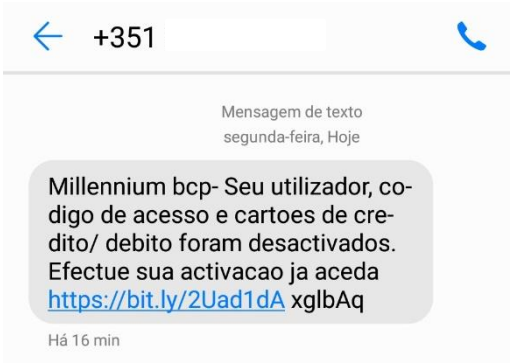

Data: sexta-feira, 3 de abril de 2020, 00:37
Para: customer@live.com
Assunto: Re: [New Statement Added] - Log-In Activity: Supicious of your account on Thursday, April 02, 2020 #65710031

Your Apple ID has been Locked

Dear Customer,

Your Apple ID was locked due to security reasons.
We have detected a sign-in from an unknown device and an unusual activity from your account.

Please verify your identity within 24



7. Estas mensagens são fraudulentas. Não foram emitidas pelo banco ou pela instituição referida: por razões de boas práticas de segurança, os bancos e outras instituições não pedem aos seus clientes ou utilizadores, por correio eletrónico, informação pessoal ou confidencial. Normalmente, os *links* incorporados nas mensagens fraudulentas conduzem a *sites* Internet onde se reproduzem, de forma muito fiel, os conteúdos disponibilizados nos autênticos *sites* daquelas instituições. Porém, tais *sites* não são geridos pelas mesmas nem por elas foram criadas: são páginas *web* falsas, que fraudulentamente pretendem captar as credenciais de acesso dos utilizadores.

8. Se a vítima aceder à página *web* correspondente ao *link* fornecido e ali introduzir os seus códigos, estará a fornecer aos autores destes factos os dados de acesso à sua conta, no legítimo *site* do banco ou outra instituição. E assim, permitirá que terceiros procedam a movimentos bancários ou outros, por esta via. Por isso, **este tipo de mensagens deve ser apagado**, sem lhe ser dada qualquer resposta.
Caso seja necessário aceder à página *web* do banco, tal acesso não deve ser feito com uso do *link* incorporado na mensagem, mas a partir do endereço URL habitualmente utilizado pelo utilizador.
Às vítimas destes crimes recomenda-se que contactem de imediato o banco (ou outra instituição em causa) e, por outro lado, que façam, logo que possível, queixa junto das autoridades policiais ou do Ministério Público.

EXTORSÃO POR VIA DE CORREIO ELETRÓNICO

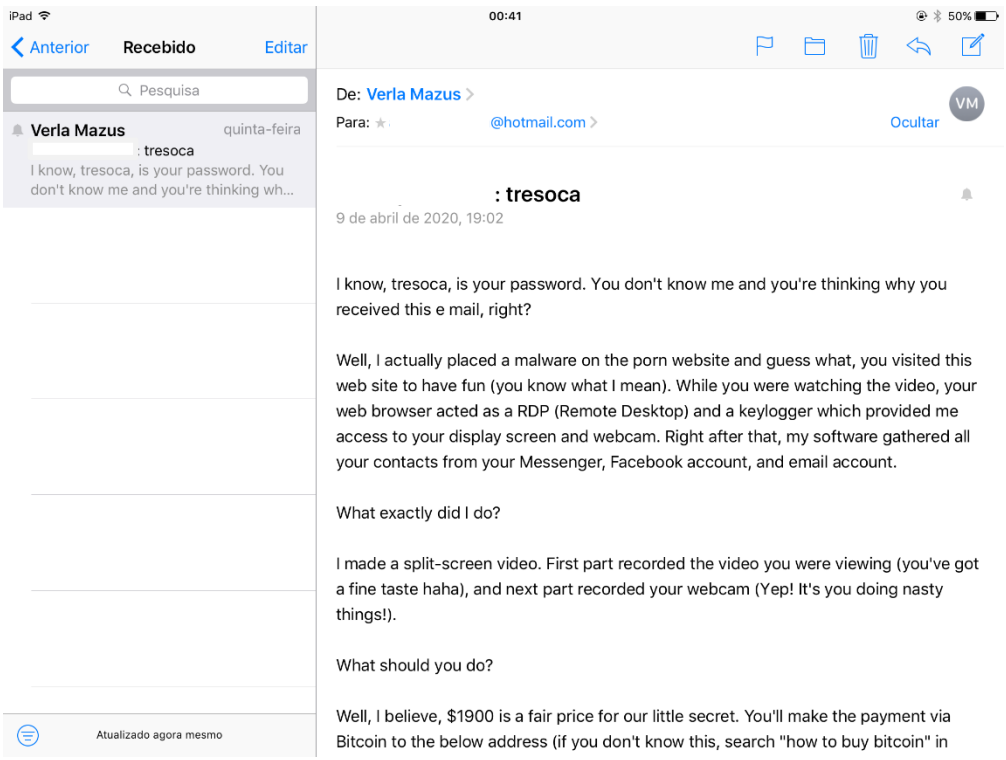
9. De igual modo, têm sido identificadas muitas mensagens de extorsão por via de correio eletrónico, cujo propósito é o de convencer as vítimas a pagar quantias monetárias, em *bitcoins*, sob a ameaça de divulgação pública de dados, imagens ou informações pessoais das mesmas.

10. Como nos casos anteriores, o processo fraudulento passa pela expedição de mensagens de correio eletrónico para inúmeros destinatários, de forma indiscriminada. Nessas mensagens, o

remetente diz ser conhecedor da senha (*password*) de correio eletrónico da vítima. Adianta que, por essa mesma razão, logrou aceder ao computador da mesma.
Em regra, os remetentes destas mensagens obtiveram os endereços de correio eletrónico das vítimas, e as correspondentes *password*, em listagens ilegalmente disponíveis na Internet. Tais listagens são resultantes de dados conseguidos em diversos ataques informáticos realizados no passado – nalguns casos, há já vários anos. Por isso, muitas vezes, as *passwords* em causa são já antigas e não estão a ser utilizadas. Porém, o mero conhecimento das mesmas pelos agentes criminosos tem provocado inquietação nas vítimas.

11. As mensagens costumam referir explicitamente provir de um *hacker*, que logrou introduzir no computador da vítima, ou *smartphone*, programas informáticos maliciosos ("*malware*"). Com esta alusão, os autores das mensagens pretendem convencer as vítimas de que, efetivamente, tiveram acesso aos conteúdos guardados nos seus dispositivos – frequentemente, conteúdos de natureza íntima, sexual, e o registo de acesso a páginas na Internet dessa mesma natureza.

12. As mensagens referem sempre, ainda, que o seu autor revelará o conteúdo da informação íntima a que teve acesso a pessoas incluídas na lista de contactos da vítima, caso não lhe seja efetuado um pagamento. Esta ameaça vem acompanhada de muita urgência, sendo concedido à vítima um curto prazo para o fazer (24 ou 48 horas).
Quanto aos pagamentos solicitados, os respetivos montantes têm rondado os 1000 a 2000 euros.



13. Sublinha-se que as concretas mensagens deste tipo a que o Gabinete Cibercrime teve acesso terão, todas elas, sido expedidas para endereços de correio eletrónico disponíveis na Internet, em resultado de ataques informáticos ocorridos no passado – alguns deles há já vários anos.

14. Por outro lado, não se apurou, em caso algum, que os remetentes das mensagens tivessem efetivamente instalado "*malware*" nos computadores das vítimas. Ou seja, os remetentes destas mensagens procuram explorar o *desconhecimento informático* das vítimas, invocando *intrusões* técnicas que efetivamente não realizaram – que são, portanto, falsas.

15. Sem prejuízo da recomendação de alteração da *password* de acesso à conta de correio eletrónico (que aliás deve fazer-se regularmente, por rotina), não há outras recomendações significativas de segurança para estes casos: apenas **ignorar a ameaça transmitida pela mensagem**, não respondendo ao seu remetente.
Como já acima se disse, nos casos identificados, estas mensagens foram sucessivamente remetidas para muitos destinatários, não tendo o seu autor qualquer conhecimento das suas potenciais vítimas, nem qualquer acesso ao seu computador ou *smartphone*. Apenas tenta persuadir o destinatário, com ameaças vagas que não conseguirá concretizar, procurando explorar o menor *conhecimento informático* das vítimas. Igualmente, na generalidade dos casos, quando a vítima não responde, nada acontece: o remetente percebe que a vítima não acreditou no seu "bluff" e procura outras vítimas. Nos casos registados, embora fosse *concedido* às vítimas um prazo muito curto para pagar o *resgate*, decorrido esse prazo nada aconteceu.