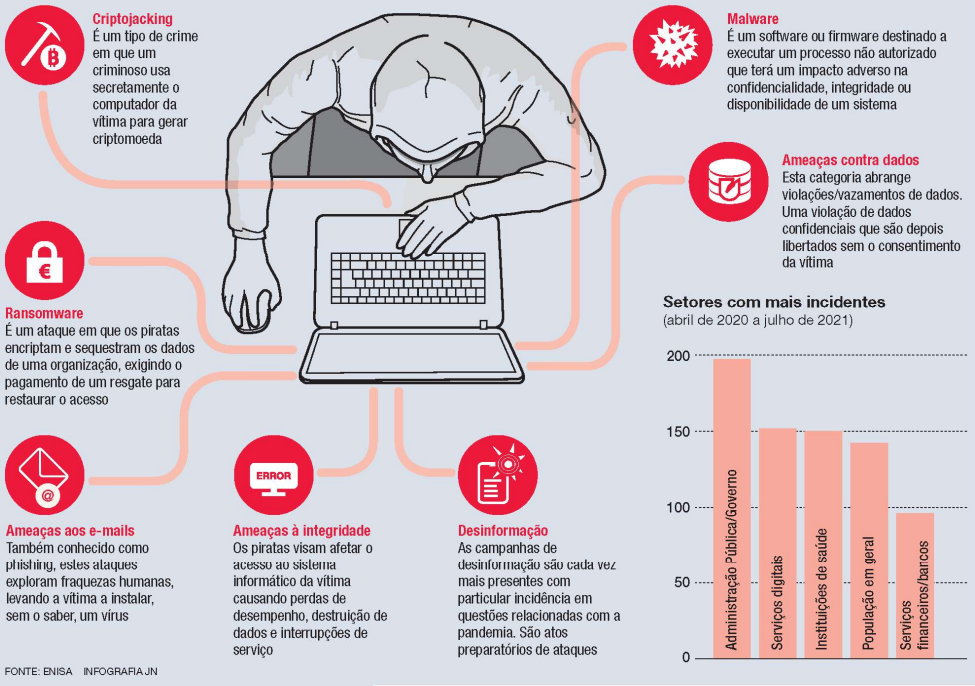
Piratas informáticos aproveitam medo da covid para ataques

Inquéritos a casos de cibercrime duplicam em 12 meses **P. 4 e 5**

Jornal de Notícias
13.01.2022
P. 04

PRIMEIRO PLANO

Principais ataques e setores afetados em 2021



FONTE: ENISA INFOGRAFIA JN

Conselhos úteis

① **Senhas fortes**
Usar credenciais de acesso fortes, com números e letras maiúsculas. Não repetir senhas em sites diferentes e mudar regularmente as senhas pode dificultar a vida aos piratas informáticos. Evitar usar nomes de familiares ou datas de nascimento.

② **Atualizações**
A atualização regular do software é importante na prevenção da cibercriminalidade. Para obter acesso aos sistemas os piratas usam padrões que podem ser detetados com as atualizações. Usar um antivírus é fortemente recomendado.

③ **Backups blindados**
A implementação de estratégias de backups (cópia de segurança dos dados) seguros e recorrentes que estejam desligados da rede permite evitar a encriptação ou destruição de dados.

④ **Formação**
É importante manter-se atualizado sobre os perigos e os cuidados a ter com a utilização da Internet.

Hackers usam novas variantes da covid como isco nos ataques

Estruturas do Estado e organismos públicos têm sofrido mais pirataria informática. PJ regista aumento exponencial de inquéritos sobre cibercriminalidade e quase duplicou o número de detidos em 2021

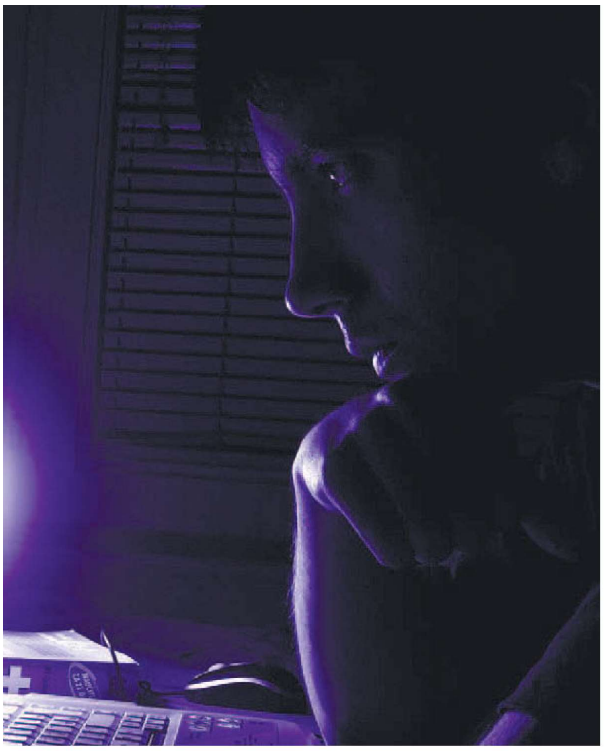
Alexandre Panda
alexandre.panda@jn.pt

PIRATARIA As novas variantes da covid-19 são a grande aposta dos piratas informáticos, que aproveitam o medo e a curiosidade das pessoas para lhes roubarem credenciais ou dados pessoais sigilosos e os usarem em lucrativos ataques informáticos. De 2020 para 2021, verificou-se um aumento exponencial de casos de pirataria e as instituições do Estado, como hospitais ou autarquias, foram alvos preferenciais dos hackers.

Cuidado e vigilância. Estas são as palavras de ordem para quem usa a Internet. O perigo está em todo o lado e os números não enganam. Em janeiro de 2021, a Polícia Judiciária tinha pendentes cerca de 13 900 inquéritos relacionados com a cibercriminalidade. Já este ano, são 17 800 casos, o que representa um aumento de 27% em relação a 2021.

De acordo com o mais recente relatório da Agência da União Europeia para a Cibersegurança (ENISA), desde o início da pandemia que a covid-19 é o isco favorito dos grupos criminosos para perpetrar ataques. E, dentro do tema covid-19, os piratas estão agora a explorar o interesse pelas novas variantes.

"Durante a pandemia, os cibercriminosos têm explorado o interesse, a preocupação, a curiosidade e o medo das pessoas usando iscos de phishing relacionados com a covid-19 para obter ganhos financeiros", explica o relatório. Além das novas variantes, os criminosos também orientam as suas campanhas na exploração da curiosidade sobre rastreamento, teste e tratamento de doenças e ainda sobre vacinação. Os ataques são cada vez mais personalizados e dirigidos a funcionários colocados em teletrabalho e sobre quem os piratas fizeram um trabalho de



engenharia social (pesquisa sobre os interesses específicos de cada pessoa). Muitos deles serão funcionários públicos.

"Os piratas usam temas sobre a saúde para aproveitar a curiosidade. Quanto mais o tema for apelativo, mais eficaz é o processo de phishing ou ransomware (pedido de resgate). Num primeiro tempo, os piratas querem chegar às credenciais de acesso para depois lucrarem com os ataques", explicou ao JN uma fonte da Unidade Nacional de Combate ao Cibercrime e à Criminalidade de Tecnológica (UNC3T) da PJ. Em 2020, esta Unidade deteve 45 suspeitos de crimes informáticos, tendo esse número disparado para 79 em 2021.

MAIORES RESGATES

"O aumento reflete também mais ataques contra estruturas do Estado, como os hospitais. O objetivo é sempre obter credenciais, para usá-las depois para ter acesso ao banco online ou outro objetivo monetário, mas também pode ser motivado por vingança ou pelo ego. Há também os pedidos de resgate", precisou a mesma fonte.

De acordo com a ENISA, no passado os cibercriminosos especializados em pedidos de resgate (após encriptação dos dados) visavam principalmente pequenas e médias empresas com programas de segurança menos eficientes. Mas, atualmente, a tendência é para direcionar os ataques para organizações maiores, capazes de pagar maiores resgates. ●

PROTEÇÃO

Seguros para proteger do cibercrime

Durante a pandemia, várias seguradoras portuguesas lançaram apólices para as vítimas da cibercriminalidade. Os seguros oferecem indemnizações por danos provocados a terceiros, devido a ataques à própria rede informática, com capitais que podem chegar a 1,2 milhões de euros, mas também o pagamento de despesas de recuperação de dados e limpeza de vírus. As seguradoras impõem geralmente avaliações básicas de risco, incluindo testes de segurança e verificação de vulnerabilidades para assegurar os clientes contra ataques informáticos. Porém, a iniciativa pode ter efeitos perversos. Segundo a Agência Europeia de Cibersegurança, as empresas vítimas de ransomware poderão sentir-se tentadas a pagar de imediato os resgates, alimentando toda a economia deste tipo de ataques.

Piratas de aluguer contratados como mercenários

Hackers remunerados para roubar e guardar informação sensível

SERVIÇOS Os piratas informáticos são cada vez mais profissionais do crime. As autoridades acreditam que os cibercriminosos estão a organizar-se para trabalhar em conjunto e assim obter mais lucro. Alguns são mesmo contratados para perpetrar ataques direcionados.

Entre as motivações que explicam os ataques informáticos está o roubo de informações sensíveis e sigilosas. Um pouco à semelhanças dos casos de espionagem entre estados, uma empresa ou organização que queira obter informação de concorrentes pode recorrer aos serviços de piratas. Os hackers podem ser contratados na chamada Dark Web e são pagos em moeda virtual.

ATRÁS DO DINHEIRO

No relatório da Agência Europeia contra da Cibercriminalidade, explica-se que "os cibercriminosos vão onde o dinheiro está". Verificou que em 2021 "muitos dos grupos de crimes cibernéticos fornecem serviços que suportam operações de ransomware direcionadas". São piratas "que desenvolveram serviços especializados em crimes cibernéticos e cibercriminosos que construíram relacionamentos dentro do ecossistema", explica o relatório.

As autoridades também reconhecem a existência de mercenários digitais. São piratas mais orientados para ações de roubo de informação específica, que vai ser útil e é valiosa para quem os contrata.

Estes cibercriminosos também podem ser contratados para causar dano direto em determinadas organizações públicas ou privadas. ●

ENTREVISTA

"A informação dos hospitais é valiosa para piratas"

Bruno Castro
Especialista em cibersegurança e líder da empresa Visionware

Quais são os setores mais atacados?
Todos os setores que envolvam dinheiro ou informação que valha dinheiro. Num segundo plano, há o patamar político, social ou institucional, de forma a colocar em causa a sua credibilidade. Este tipo de ataque é orientado a motivações políticas ou sociais.

Quais os novos ataques visando empresas e entidades portuguesas?
Há um esforço por parte da comunidade cibercriminosa no sentido de gerar conteúdos mais eficazes que permitam criar mais "tentação e apetências" das pessoas a cair nas armadilhas para concretizar a intrusão que depois irá gerar outras ações maliciosas, como roubo de credenciais, usurpação de identidade, acesso e roubo de dados, etc. A maior novidade prende-se com resgates de "não divulgação" de informação e ataques de destruição completa.

A segurança dos hospitais e tribunais podem estar em risco?
A informação existente num hospital é focada em dados pessoais e é altamente confidencial e sensível. Por inerência, será valiosa para ser "comercializada" no mercado negro. Face à criticidade do serviço que prestam, os hospitais são também potencialmente interessantes para um ataque que se foque na disrupção de serviço, com o intuito de colocar em causa a instituição. Também pode levar a possíveis pedidos de resgate, para "não divulgação" de informação roubada.

Como ganham dinheiro com ataques?
Apontaria três típicos vetores de proveitos: um pedido de resgate para acesso à informação encriptada (via chave de desencriptação); um pedido de resgate de não divulgação de dados roubados; e, por fim, a comercialização nos fóruns de cibercrime da informação roubada a outros grupos criminosos ou a organizações que assim tenham interesse. São criminosos profissionais. O "hacktivismo" já foi uma tendência, hoje não é.

Ataques recentes

Janeiro 2022
Telefonemas Microsoft
Houve um aumento de telefonemas fraudulentos, em nome da empresa Microsoft, que incentivam as vítimas a instalarem programas maliciosos no seu computador, com a intenção de roubar ou encriptar informações.

Dezembro 2021
SIC e Expresso
O grupo Impresa foi alvo de um ataque sem precedentes em Portugal, envolvendo a destruição de dados. O mesmo foi qualificado de ataque à liberdade de imprensa. O caso está a ser investigado pela Polícia Judiciária.

Setembro 2021
Novo Banco
Criminosos lançaram uma campanha de phishing dirigida a clientes do Novo Banco. Como é habitual nestes casos, o processo começou com a expedição, para muitos destinatários, de mensagens fraudulentas de correio eletrónico.

Setembro 2021
Caixa Geral de Depósitos
Também através de phishing, foi lançada uma campanha dirigida a clientes da Caixa Geral de Depósitos que fossem titulares de cartões de crédito. Nesta campanha, os criminosos pretendiam convencer as vítimas a facultarem-lhes dados dos seus cartões de crédito.

Abril 2020
EDP
A elétrica foi alvo de um ataque em que os piratas conseguiram penetrar num servidor interno onde terão sacado dez terabytes de informação sensível. Reclamaram dez milhões de euros de resgate para não divulgar a informação.

