FraudGPT e Worm GPT representam “salto quântico” no cibercrime

jornaleconomico.pt/noticias/edicao-diaria-3a-caso-rui-pinto-cibercrime-nao-e-uma-coisa-estranha-que-aparece-em-hollywood-afirma-partner-da-visionware

8 de agosto de 2023

O cibercrime continua a aperfeiçoar as suas técnicas para gerar cada vez mais atividades maliciosas. As mais recentes ferramentas à disposição dos *hackers* são o FraudGPT e WormGPT, descobertas recentemente na *darkweb* e no Telegram pela equipa de Strategic Intelligence da VisionWare.

Com preços que variam entre os 200 e 1.700 dólares qualquer cidadão pode aprender entre outras técnicas maliciosas, como lançar esquemas de *phishing*, desenvolver software perigoso ou escrever cartas e *e-mails* para burlas.

Em entrevista ao Jornal Económico, Filipe Custódio, Partner da VisionWare, fala dos perigos das duas recentes ferramentas e analisa também o facto de como o caso Rui Pinto serviu para despertar os portugueses para a realidade do cibercrime.

Como descobriram estes *malwares*?

No início deste ano dissemos que mais tarde ou mais cedo isto ia acontecer. Ou seja, iam começar a aparecer ferramentas mais especializadas para um determinado tipo de ciberataque. Sobre o WormGPT e o FraudGPT ainda se sabe pouco, porque apareceram

há cerca de duas semanas. O que se sabe é por interposta pessoa e pela publicidade feita pelas ferramentas na *darkweb* e no Telegram, por alguns comentários que já surgiram de especialistas em segurança sobre elas.

Estes dois *malwares* propõem um modelo de subscrição, onde se paga para utilizá-los. A comunidade internacional de segurança não está particularmente, digamos, surpreendida com estas capacidades.

Hoje em dia já existem ataques cibernéticos feitos pelo ChatGPT. Um dos ataques mais simples de fazer os ataques de *spear-phishing*, onde se envia um email para uma determinada vítima a fingir que é um *e-mail* de uma determinada empresa e onde se leva a vítima a clicar no *link*, a fornecer informações confidenciais e a pessoa faz porque viu um *e-mail* que parece legítimo e tem todo o aspeto de ser da sua empresa.

Se for só uma questão de *e-mails* e roubo de credenciais, parece muito pouco em termos do que o WormGPT e FraudGPT propõem, face à capacidade daquilo que podem fazer, o que nos leva a crer que estas ferramentas estão a ser usadas como publicidade para depois vender algo mais poderoso.

Algo mais poderoso. Como por exemplo?

Temos aqui duas vias de ataque que podem ser feitas com a inteligência artificial. A primeira via será uma automatização dos ataques. Imagine que, em vez de estar a pedir ao WormGPT para criar um *e-mail* com uma determinada característica, tenho uma plataforma *online* que automaticamente me faz os emails de *pishing*, cria os *sites* de captura de credenciais e faz todo o processo de forma semi-automática.

Isto é um passo quântico em termos de efetividade dos ataques. Hoje em dia um atacante ainda tem que estar a estudar site a site, empresa a empresa, banco a banco. Se tiver um WormGPT, que vai identificar as ameaças e customizar as ameaças para aquele ataque, fazer o ataque com sucesso sem intervenção humana, isto faz com que o número de ataques possa subir repentinamente. Este parece o cenário mais provável e possível de acontecer nos próximos meses, que é aparecer uma ferramenta a fazer ataques em massa.

Mas estamos a falar de ataques em massas a qualquer tipo de estruturas ou vocacionadas para algum sector em específico da sociedade?

Há aqui três vítimas que são sempre visadas. Uma é o *homebanking*, que é muito fácil de ir buscar credenciais e depois fazer roubo direto de dinheiro das pessoas. Os bancos são os alvos iniciais, mas os finais são os seus clientes

O segundo serão os cartões de crédito e o *e-commerce*. O terceiro serão os ataques às contas corporativas, ou seja, as contas de Office365, as contas que usamos no dia a dia e através disso consegue-se fazer ou potenciar ataques de *ransomware* às empresas.

Podemos ter este tipo de ataques diariamente?

Sim, e travar não vai ser fácil. A comunidade de *intelligence* está a fazer o seu papel e a tentar identificar este tipo de ameaças o mais cedo possível, para que depois consiga tomar as medidas de proteção possíveis para estes ataques.

Enquanto Visionware em Portugal que ataques já detetaram? Têm algum tipo de colaboração, nomeadamente com a Polícia Judiciária?

Não de forma muito direta, porque trabalhamos em campos um pouco diferentes. A Visionware trabalha com os seus clientes na prevenção dos ataques e na deteção dos mesmos e a Polícia Judiciária trabalha após o ataque. As autoridades judiciais, até que haja um ataque concreto ou um crime que tenha sido cometido, não podem fazer nada. Nós podemos pelo menos alertar os nossos clientes de que algo está a ser preparado.

Quais são os ataques mais utilizados atualmente em Portugal?

Vemos um pouco tudo. Continua a existir muito acesso a contas cooperativas para depois fazer um *ransomware* e colocar as empresas fora de ação e pedir um resgate. Existe alguma prevalência também de um crime que já vem de alguns anos, que é o ataque às financeiras das empresas, onde se enviam *e-mails* a tentar convencer os fornecedores de determinadas empresas a fazer os seus pagamentos numa conta que é falsa. Este tipo de fraude está bem enraizada e tem até aumentado.

Os ataques de *homebanking* continuam também. Temos visto alguma passagem do *phishing* simples para o *smishing*, ou seja, a utilização cada vez mais dos SMS's como forma de ultrapassar as defesas *antiphishing* que a maior parte das empresas já tem.

O cidadão comum que não esteja familiarizado com estas práticas do cibercrime o que pode fazer para se defender?

Passa muito pela consciencialização e aprendizagem comum que temos de ter em sociedade. É uma aprendizagem constante, o meu receio é que possa não ser suficientemente rápida para evitar muitos ataques com sucesso.

A banca, em particular, tem responsabilidades porque quando é um cidadão comum, a maior parte dos ataques tem como alvo as suas credenciais de *homebanking* ou o seu cartão de crédito e a banca tem a responsabilidade de manter os seus canais cada vez mais seguros, ainda que possa ser à custa de alguma comodidade para o seu cliente.

O caso Rui Pinto serviu de alguma forma para alertar os portugueses para o cibercrime?

Foi um dos aspetos mais positivos que veio desse caso criminal. Por um lado, o cibercrime não é uma coisa estranha que aparece em Hollywood. É algo que está aqui connosco no dia a dia.

Em segundo lugar abriu espaço para discutir um pouco a ética dos ciberataques, onde havia pessoas, por vezes até ligadas à sua preferência clubística que achavam muito bem aquele ciberataque. As vítimas de ciberataques, ou mesmo aqueles que não tinham

nada a ver com isto, achavam mal porque já foram vítimas e sabem o que custa. Foi interessante ver essa discussão.

Ficou surpreendido pelo facto de uma só pessoa conseguir aceder a tanta informação?

Sim, mas atenção. O que nós já sabemos hoje dos ataques é que foi uma pessoa, a muitas empresas, mas usando sempre o mesmo método. No *hacking* existe muitas vezes esta questão, que é quando um *hacker* descobre uma chave que lhe permite entrar numa determinada marca de porta, ele vai testar todas as portas onde essa chave funciona.

Este é um aspeto onde a Inteligência Artificial pode ser um perigo, porque hoje em dia essas chaves únicas, neste caso era uma falha num *software* VPN, eram raríssimas. É raríssimo haver uma vulnerabilidade que afeta muitas empresas ao mesmo tempo e que alguém a descobre antes de ser feita a respetiva conexão. Acredito que este tipo de ataques também vai crescer nos próximos tempos.

Ataques como aqueles que aconteceram à Vodafone, Altice ou Impresa podem voltar a acontecer?

Os ciberataques com muito sucesso, que aconteceram nos últimos dois, três anos, causaram uma mudança também na ciberdefesa. Mesmo as empresas que investem muito dinheiro em cibersegurança sabem que mais cedo ou mais tarde vão ser vítimas de um ataque com sucesso. Mesmo que consigam proteger 99% dos dados dos seus ativos, basta 1% que não ficou protegido para conseguir comprometer a empresa.

A pandemia também proporcionou o desenvolvimento destes ataques?

A pandemia foi o catalisador para o aumento dos ciberataques, quer pelo facto de muita gente estar em casa e, portanto, haver as fronteiras das empresas que antigamente eram feitas pela *firewall*. Essa fronteira teve de se esbater por razões de emergência e, portanto, os colaboradores passaram a estar em casa no seu computador, onde não há segurança física.

Estão numa reunião e se calhar ao lado está alguém a ouvir a informação. Onde o mesmo computador que é usado para o teletrabalho pode ser usado para os filhos jogarem. Grande parte dos ataques de *ransomware* de grande dimensão começam com o ataque a um funcionário.

Portugal hoje em dia está bem preparado para responder ao cibercrime?

Temos dos melhores cérebros nesta área da cibersegurança e os investimentos que no passado eram difíceis, hoje em dia já estão mais presentes nos orçamentos das várias empresas. Temos uma vantagem em relação a outros países que é uma grande interconectividade. Ou seja, temos empresas muito tecnológicas e com muita capacidade de trabalho nesta área.

A desvantagem é que por vezes temos pouca cultura de risco. Esse é o ponto onde e como sociedade nós poderíamos evoluir mais. Acho que Portugal tem a capacidade, as empresas têm os cérebros e meios para o fazer. Há aqui alguma mudança de atitude face ao risco que está a vir por via dos ataques e não tanto por via da prevenção.

Portugal tem também meios financeiros para responder a estes ataques?

Depende. Temos capacidade para responder há maior parte dos ciberataques que estão presentes hoje, mas já há ciberataques muito evoluídos e sofisticados.

Digamos que para a maior parte dos ciberataques que se verificam hoje em dia, nós enquanto sociedade e as nossas empresas estão preparadas para os enfrentar, estando sempre alerta, já que é uma realidade em constante mudança.