Ataques baseados em memória estão em ascensão: proteja-se!

Josh Fu (*)

Ultimamente, você pode ter ouvido falar sobre ataques baseados em memória, ataques sem arquivos e ataques de subsistência (living-off-the-land attacks)

Se assim for, é excelente que você se mantenha atualizado. Todos esses termos se referem à mesma coisa. Como sugerem os nomes, trata-se de um ataque à memória do sistema, tanto à ROM quanto à RAM.

Por que agora?

Os atacantes estão usando cada vez mais esse tipo de ataque porque funciona. É menos detectável pelos mecanismos antivírus (AV) e até mesmo por algumas soluções AV de última geração. Por causa disso, os cibercriminosos que usam essa técnica têm mais chance de ter sucesso em sua missão, que é roubar seus dados – sejam credenciais, segredos corporativos ou recursos de computação.

Como esse ataque funciona

Esse tipo de ataque se concentra em obter instruções ou dados fora da memória, em vez de nas áreas de foco tradicionais, como os diretórios do disco ou chaves do registro. A maneira como esse ataque é normalmente executado é a seguinte:

Etapa 1: um script ou arquivo chega ao endpoint. Ele evita a detecção porque parece um conjunto de instruções, em vez de ter recursos típicos de arquivo.

Passo 2: essas instruções são carregadas na máquina (vamos explicar onde e como mais tarde).

Etapa 3: depois de executadas, elas trabalham usando as próprias ferramentas e recursos do sistema para realizar o ataque.

Exemplos de ataque

Um exemplo comum desse ataque usa uma combinação de macros do Word: Powershell, Meterpreter e Mimikatz. Essas ferramentas nativas, bem como aplicativos da Web, são executadas na memória e possuem alto nível de direitos de execução.

Acontece da seguinte maneira: um usuário recebe por e-mail um documento do Word contendo macros que solicitam ativação após a abertura do documento. As orientações das macros entram em contato com um servidor Command and Control (C2) para baixar um script, que permite que o Powershell faça um segundo download do Meterpreter e do Mimikatz (ambos aplicativos com usos legítimos) para começar a localizar e enviar credenciais ao servidor C2. Uma carga do malware também pode ser baixada, o que pode ser capturada por uma boa solução antivírus de próxima geração.

Talvez o usuário acesse um site e seja solicitado a executar o Flash, que geralmente apresenta algum tipo de vulnerabilidade. Depois que o usuário o habilitar, o Flash comprometido poderá enviar o código de shell ou as instruções para o endpoint do usuário, para ser executado na linha de comando e na memória sem o conhecimento da vítima.

Como esses ataques são baseados em orientações da própria máquina e no uso de aplicativos locais, fica mais fácil entender de onde vêm os nomes "sem arquivo" e "de memória".

Como deter esses ataques hoje

É possível, no entanto, evitar esses ataques, sendo vigilante:

- Manter-se atualizado sobre patches.
- Bloquear sites que executam Flash, Silverlight ou Javascript, ou bloquear a exibição desses softwares em sites que solicitem sua ativação.
- Restringir o uso de macros em documentos.

Infelizmente, alguns desses métodos não são realistas para seus usuários, principalmente quando estão tentando trabalhar, mas são opções legítimas.

Você também pode detectar manualmente esses tipos de ataques, se notar um tráfego estranho usando seu software de SIEM (security information and event management, ou gerenciamento e correlação de eventos de segurança, em português) – supondo que você tenha um. Você pode ainda usar seus firewalls para inspecionar o tráfego. A utilização de ambos os métodos como sua estratégia de detecção envolve a integração de inteligência de ameaças externas de alta qualidade e regras para detectar a execução interna de aplicativos.

Você também pode investigar os eventos manualmente ou realizar varreduras diárias com uma ferramenta de análise da memória. Como sugestão, a Volatility Foundation tem software de código aberto altamente renomado.

Como deter esses ataques amanhã

Se você acha que isso parece um monte de trabalho que exige vigilância constante e talento, você tem razão. E discutimos apenas dois exemplos de técnicas de ataque de toda a matriz Mitra ATT&CK, que possui dezenas de técnicas diferentes. É importante, no entanto, entender a grande quantidade de esforço manual necessário para comparar com o que acontece quando essas ações podem se tornar automatizadas e mais eficientes.

Outra opção para detectar e interromper esses ataques é obter um produto de detecção e resposta de endpoint (EDR) com ações automatizadas em um mercado muito concorrido neste momento, com palavras que soam muito semelhantes. É por isso que é muito importante informar-se sobre o que sua organização precisa e se um fornecedor pode atender a essas necessidades com rapidez, facilidade e eficácia.

Independentemente de como você implementar sua estratégia de segurança, é importante que tenha consciência desse tipo de ameaça e informe-se sobre suas possíveis opções para interrompê-la.

Ao pesquisar suas opções, não deixe de fazer perguntas detalhadas sobre como cada solução funciona, incluindo quais ações automatizadas elas oferecem e quão avançadas são suas detecções e ações. E lembre-se: o objetivo das soluções de um fornecedor é melhorar o tempo de resposta de um analista e de sua equipe, não aumentar a quantidade de trabalho deles.

(*) É CISM (Certified Information Security Manager) e CISSP (Certified Information Systems Security Professional), é engenheiro de segurança da Cylance. Tem experiência como gerente de canal, consultor em infraestrutura de nuvem e engenheiro de vendas em segurança cibernética. Josh fundou o capítulo da Costa Oeste do Consórcio Internacional de Profissionais de Cibersegurança e apresenta-se para audiências do setor em todos os EUA.

Gamificação e o mundo corporativo

Gamificação (ou em inglês gamification) é o termo utilizado para representar o uso de elementos de jogos para atingir diversos objetivos que aprimoram a experiência e o engajamento do usuário em qualquer serviço, processo ou aplicação que não esteja diretamente relacionado ao universo dos jogos

Marcelo Henrique dos Santos (*)

Marins (2013) afirma em sua obra que gamificação é o uso de elementos de jogos e técnicas de game design em contextos não relacionados a jogos.

Podemos observar, por exemplo, o sucesso de aplicações que empregam esses princípios, como o Foursquare, cuja proposta seria promover a motivação dos usuários através de elementos de jogos, fato que atraia o interesse de todos os envolvidos (empresa e consumidores).

Por incrível que pareça a ideia de utilizar os princípios e mecânicas de jogos para resolver problemas é antiga. Há mais de trezentos anos, o filósofo escocês David Hume lançou as bases para a compreensão das motivações do jogador. A partir desses estudos, podemos observar que durante uma partida, as capacidades mental e emocional do usuário são totalmente ativadas, despertando estímulos visíveis em sua feição, como senso de urgência, medo, dentre outras sensações. Além disso, o jogo consegue manter a concentração intensa e o foco profundo ao lidar com o problema que está sendo resolvido na partida.

A partir desse viés temos o desafio de aplicar os conceitos dos jogos em áreas distintas para promover essa mesma sensação no usuário.

Nos últimos anos, o mercado econômico começou a utilizar os princípios da gamificação de forma simplificada, por meio de um sistema de recompensas que serviu de base para programas de fidelidade. Tais estratégias incentivam o consumo por diversos motivos. Por exemplo, os programas das operadoras de cartão de crédito e as companhias aéreas, permitem a troca de pontos por produtos e serviços, oferecendo diversas vantagens para o consumidor.

Conforme Zichermann (2011), o principal problema de utilizar essas estratégias no mundo coorporativo é que podemos gerar uma dependência excessiva em relação à distribuição da recompensa, podendo a venda ser afetada de forma negativa se houver a retirada do benefício, além disso esse tipo de estratégia não garante que conseguiremos obter novos clientes.

A proposta de aplicar a gamificação não se resume simplesmente em inserir elementos de jogo, como distribuição de recompensas e medalhas para um determinado produto, pois exige uma abordagem aprofundada para decidir quais elementos serão incorporados e a conformidade deles com contexto do objetivo proposto pelo projeto.

Em meu livro, A utilização de games para atrair audiência em veículos de comunicação, produzido em 2018, falo sobre o processo de construção de jogos digitais com o objetivo de servir como um veículo de comunicação da marca das empresas, fortalecendo as estratégias de marketing digital com o processo de promoção e interação com o público alvo.

O engajamento fornece um diferencial competitivo a diversas empresas, através de um empenho maior dos funcionários ou então a partir do engajamento de seus clientes. Por esse motivo quando utilizamos de forma correta esses elementos transformamos a experiência em jogo, gerando uma mudança comportamental.

Diante desse cenário podemos observar que a gamificação pode ser utilizada em diversas áreas como: treinamento, saúde, educação, no meio empresarial, tanto na fidelização de clientes como no aumento de produtividade dos empregados.

REFERÊNCIAS BIBLIOGRÁFICAS

Zichermann, G. e Cunningham, C. (2011), Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps, O'Reilly Media.

McGonigal, J. (2010) "Gaming Can Make a Better World", TED.

Marins, D. R. (2013), Um Processo de Gamificação Baseado na Teoria da Autodeterminação, Dissertação (Mestrado em Engenharia de Sistemas e Computação) – Universidade Federal do Rio de Janeiro/COPPE, Rio de Janeiro.

(*) É bacharel em Sistemas de Informação, especialista em Games, Marketing e Vendas e em Negócios em Mídias Digitais, mestrando em Educação e professor do curso de Jogos Digitais do Complexo Educacional FMU | FIAM-FAAM.

Quatro elementos chave de um programa anti-phishing

Semanalmente, nos deparamos com manchetes de um novo ataque ou de uma outra grande violação. Por exemplo, recentemente milhões de clientes nas lojas Saks e Lord & Taylor foram afetados por uma violação. Embora ainda esteja sob investigação, os relatórios iniciais apontam que é o resultado de um ataque de phishing.

Não é nenhuma surpresa que os hackers usem essa abordagem - as pessoas ainda são o elo mais fraco de qualquer programa de segurança. Isso torna o phishing uma das maiores ameaças enfrentadas atualmente pelas pequenas e médias empresas. De acordo com o Relatório de Investigações de Violações de Dados da Verizon, mais de 90% dos ataques começam com um phishing.

Um dos principais fundamentos para prevenir o phishing é a educação dos colaboradores. Ao capacitar a equipe em relação a diferentes tipos de ataques, ela pode se transformar de um dos elos de segurança mais fracos, em um dos maiores aliados de uma companhia. É possível fazer isso ao criar um programa abrangente de proteção contra phishing em toda a empresa.

Quatro componentes de um Programa de Prevenção de Phishing

Programas abrangentes de proteção contra phishing incluem quatro componentes - proteção, educação, avaliação e relatórios. Compreender o porquê e como ajuda a concentrar os seus recursos limitados de segurança no que é importante.

- **Proteção:** O ciclo começa com a proteção, pois as taxas de cliques continuam altas.É de extrema importância complementar a ligação entre proteção e educação com uma solução eficiente que forneça uma camada adicional de segurança para identificar e impedir infecções por malware. Assim, os funcionários que clicam nos e-mails de phishing são protegidos e recebem uma dose de treinamento depois da ação.
- **Educação:** Essa proteção precisa estar em sinergia com a educação. Os usuários precisam entender quando cometeram um erro e como se manter seguros no futuro. Certifique-se de treinar seus usuários sobre os perigos de clicar em arquivos suspeitos de anexos de e-mail e hiperlinks e links da Web incorporados. Eles são muito fáceis de detectar, uma vez que a maioria tende a não ser personalizada para destinatários individuais. Os e-mails de phishing geralmente têm gramática ruim, links que não correspondem a domínios da Web com marca ou outros problemas de aumento de sinalização.
- **Avaliação:** Os gerentes de TI precisam entender suas taxas de cliques e onde direcionar a educação. O treinamento é o primeiro passo, mas não descarta a necessidade de exercícios práticos e avaliações periódicas da equipe. Colocar e-mails de phishing para testar a sua força de trabalho demonstra e reitera a necessidade de revisão. O objetivo é mantê-los desconfiados ao interagir com anexos de arquivos ou links em emails não solicitados.
- **Relatório:** Os participantes de um programa de treinamento se beneficiam ao falar sobre os casos que presenciam. Isso esclarece o que os atacantes estão fazendo e reforça a necessidade de estar vigilante contra esses ataques.

Além disso, certifique-se de revisar e atualizar suas políticas de segurança anti-spam e firewall. As ameaças de segurança surgem e evoluem rapidamente. É preciso estar sempre alerta e atualizado sobre os últimos vazamentos, correções e patches.

(Fonte: Todd O'Boyle é Director of Product Management da WatchGuard Technologies).

News @TI

Embratel lança solução Omnichannel

@A Embratel anuncia o lançamento da solução Omnichannel Embratel. A nova oferta consiste em uma central inteligente de atendimento baseada em Nuvem (Cloud). A solução conecta múltiplos canais de atendimento, como serviços de voz, e-mail, chat de texto e formulários da web, com o objetivo de transformar a experiência dos clientes da área financeira. O Omnichannel é uma evolução do conceito de Contact Center que acompanha e atende às expectativas das empresas que estão em busca constante de avanços tecnológicos. O Omnichannel Embratel by Genesys é indicado para empresas de diversos tamanhos e de todos os segmentos de mercado, principalmente instituições financeiras que realizam e recebem milhares de ligações diariamente em seus call centers. A nova oferta foi desenvolvida também para organizações que possuem múltiplos canais de contato, como central de relacionamento, suporte técnico, áreas de crédito e cobrança e telemarketing para vendas, entre outros (www.embratel.com.br/omnichannel).

Startup cria app para otimizar reembolsos e evitar fraudes

@A cidade de São Paulo é o destino mais procurado pelos brasileiros para viagens corporativas, seguida por Salvador e Manaus, de acordo com pesquisa da agência ViajaNet. O levantamento aponta ainda que o volume de viagens a negócios permaneceu estável no País. Viajar para fazer negócios está na rotina de muitos empreendedores, e por isso, quando as viagens corporativas não são bem planejadas, podem pesar no orçamento das empresas - independentemente de seu tamanho. O VExpenses, por exemplo, é um aplicativo brasileiro que automatiza os processos de reembolso, evitando dor de cabeça para os colaboradores e economizando tempo e dinheiro das empresas. Além de facilitar o reembolso, o app ainda colabora com a gestão das despesas, como deslocamentos, custos e pagamentos em geral (www.vexpenses.com)