O SILENCIOSO CLIQUE ZERO

Gabriel Varela Centeno Hulsendeger [1]
Anderson santos da silva [2]
Jader Ligório Rodrigues [3]
João Padilha Moreira [4]

RESUMO

Normalmente ataques maliciosos dependem de algum tipo de interação do usuário para se dar início, abrir um link, executar um arquivo entre outros. No Ataque Clique Zero (*Zero Click Attack*) nenhuma interação do usuário é necessária, pois se dá ao se conectar ao com pacotes de dados externos, como um telefone ao receber um SMS. Como a conexão é realizada de maneira automática pelo sistema é muito difícil de detectar-se, fazendo com que se tenha pouquíssimos registros comprovados tornando-o pouco conhecido pelo público geral.

Palavras-chave: Interação, clique zero, ataque.

ABSTRACT

Usually malicious attacks depend on some type of user interaction to initiate, open a link, execute a file, among others. In Zero Click Attack, no user interaction is required, as it occurs when connecting to external data packets, such as a phone when receiving an SMS. As the connection is made automatically by the system, it is very difficult to detect, causing very few proven records, making it little known to the general public.

Keywords: Interaction, zero click, attack.

[1] Acadêmico do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. gabriel.hulsendeger@alcidesmaya.edu.br
[2] Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. anderson_silva@alcidesmaya.edu.br
[3] Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. jader_rodrigues@alcidesmaya.edu.br
[4] Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. joao_moreira@alcidesmaya.edu.br

Pode-se dizer que o ataque Clique Zero ocorre em três etapas: enviar arquivo de dados, exploração de uma vulnerabilidade e inserção do código malicioso. O primeiro passo consiste em enviar para o dispositivo alvo um pacote de dados (email, mensagem de voz, sms, entre outros) com códigos bem trabalhados. Realizada a conexão, a qual é automática, ela servirá como porta de entrada para o código que irá desencadear alguma vulnerabilidade desconhecida, que fornecerá as permissões necessárias para iniciar a inserção do código malicioso. Em alguns casos pode ser um processo semelhante ao de *buffer overflow*, contudo, é apenas uma maneira possível de se realizar o ataque, pois o objetivo, como dito anteriormente, é explorar vulnerabilidades desconhecidas. Tendo sucesso se inicia o terceiro passo que consiste em inserir o código malicioso desejado pelo atacante no sistema.

Esse ataque é muito difícil de ser realizado, pois o atacante não tem como saber onde, e nem se o ataque pode ser feito necessitando de várias tentativas para se ter a chance de sucesso. Entretanto, mesmo apresentando alto nível de dificuldade e baixas chances de sucesso, possui uma grande vantagem: falhando o ataque, é muito difícil saber que ele ocorreu. Isso, pois, como dito anteriormente, o ataque inicia com a chegada de um e-mail, mensagem de texto ou ligação, que possui um código inserido que irá procurar pela vulnerabilidade, caso não consiga encontrá-la o arquivo se apaga sem deixar vestígios e sem o usuário perceber. Dessa maneira, o atacante pode realizar inúmeros ataques no mesmo sistema e não se terá registros de uma tentativa de invasão.

Sabe-se muito pouco sobre esse tipo de ataque, pelos motivos mencionados anteriormente, dificultando encontrar uma maneira de impedi-los de forma eficiente. Os casos mais famosos que se tem confirmação foram a instalação de um spyware em um celular de um ativista via WhatsApp e dos dispositivos IOS onde os aplicativos de E-mail apresentavam vulnerabilidades que permitiam esse tipo de ataque. Há um caso confirmado no Linux, que possuía em seus protocolos Bluetooth um meio de acesso por ele, que permitiria o acesso total à máquina atacada e, por consequência, qualquer outro dispositivo nele conectado.

Para se proteger desse ataque o sistema precisa ter algum software que verifique e monitore em tempo real todas as conexões realizadas ou achar a vulnerabilidade e repara-la. Em sistemas ditos “sensíveis” (bancos, empresas grandes, etc) é comum, mas em celulares é

mais difícil do usuário ter essas proteções, muitos não possuem nenhuma. Por isso, como já mostrado, os dispositivos móveis são mais vulneráveis a esse ataque. Mesmo assim, não se pode dizer que computadores são pouco afetados, pois não há como garantir que um nunca foi atacado, pela dificuldade, já mencionada, de se fazer um registro. Assim, é muito provável que centenas de milhares de ataques de Clique Zero aconteçam, mas ninguém fique ciente e já pode ter seu sistema comprometido. Isso torna esse ataque extremamente perigoso, reforçando a grande necessidade de aumentar a proteção, principalmente em dispositivos moveis, até que se obtenha um melhor entendimento dessa ameaça para poder combatê-la com eficácia.

REFERÊNCIAS

BALABAN, David. Demystifying zero-click attacks. 2020. Disponível em: < https://www.itgovernanceusa.com/blog/demystifying-zero-click-attacks > Acesso em: 23 outubro 2020.

KIGHTLINGER, Diana. Why Zero-Click Cyberthreats Should Be on Your Radar. 2020. Disponível em < https://securityintelligence.com/articles/why-zero-click-cyberthreats-should-be-on-your-radar/ > Acesso em: 23 outubro 2020.

LILY, Hay Newman. Sneaky Zero-Click Attacks Are a Hidden Menace. 2020. < https://www.wired.com/story/sneaky-zero-click-attacks-hidden-menace/ > Acesso em: 23 outubro 2020.

Zero-click infection and WhatsApp's latest breach. 2019. Disponível em: < https://thedefenceworks.com/blog/zero-click-infection-and-whatsapps-latest-breach/ > Acesso em: 23 outubro 2020.