A Publicação Mensal de Sensibilização de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Spear Phishing

O que é Spear Phishing?

Você pode estar familiarizado com ataques de phishing, que são e-mails enviados por criminosos cibernéticos para milhões de potenciais vítimas ao redor do mundo concebidos para enganar, ludibriar ou atacá-los. Normalmente, essas mensagens parecem vir de uma fonte confiável, como o seu banco ou de alguém que você conheça. Os e-mails muitas vezes têm uma mensagem urgente ou um negócio para você que é simplesmente bom demais para deixar passar. Se você clicar no link em um e-mail phishing, poderá ser levado a um site malicioso que tenta invadir seu computador ou capturar seu nome de usuário e senha. Ou talvez o e-mail de phishing pode ter um anexo infectado, que se aberto, tenta infectar e assumir o controle de seu computador. Cyber criminosos enviam esses e-mails para o maior número de pessoas possível, sabendo que quanto mais pessoas receberem o e-mail, mais pessoas vão provavelmente ser vítimas.

Editor Convidado

Lenny Zeltser é o editor convidado para esta edição do OUCH! Lenny se dedica a proteger operações de TI de clientes no NCR Corp e ensina combate a código malicioso no SANS Institute. Lenny pode ser encontrado no twitter como **@lennyzeltser** e em seu blog de segurança, **blog.zeltser.com**.

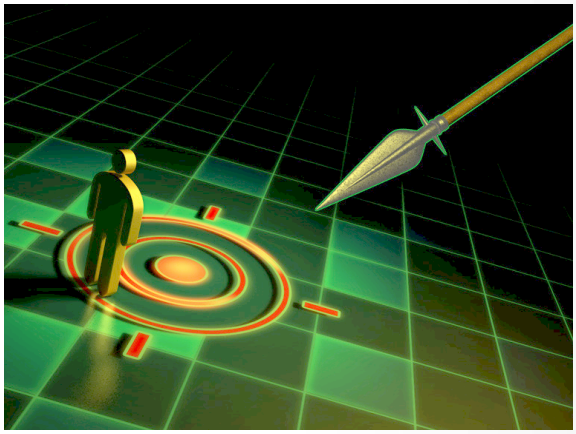
Embora phishing tenha sua eficácia, um tipo relativamente novo de ataque apareceu, chamado spear phishing. O conceito é o mesmo, os atacantes cibernéticos enviam e-mails para a vítima, fingindo ser uma organização ou uma pessoa de confiança da vítima. No entanto, ao contrário de e-mails de phishing tradicional, as mensagens de spear phishing são altamente direcionadas. Em vez de enviar um e-mail a milhões de vítimas potenciais, os atacantes cibernéticos enviam mensagens de phishing para alguns poucos indivíduos selecionados, talvez cinco ou dez pessoas visadas. Ao contrário de phishing geral, com spear phishing os atacantes cibernéticos pesquisam seus alvos, com a leitura das contas da vitima no LinkedIn ou Facebook ou quaisquer mensagens que eles postaram em blogs ou fóruns públicos. Com base nesta pesquisa, os agressores, então, criam um e-mail altamente personalizado que parece relevante para os destinatários. Desta forma, os indivíduos são muito mais propensos a se tornarem vítimas do ataque.

Eficácia do Spear Phishing

Spear phishing é usado quando o atacante cibernético quer especificamente atacar você ou sua organização. Em vez de simples criminosos que querem roubar dinheiro, os atacantes que usam spear phishing têm objetivos muito específicos, geralmente acesso a informações altamente confidenciais, como segredos corporativos de negócios, planos de uma tecnologia secreta, ou comunicações confidenciais

Spear Phishing

do governo. Ou, talvez, sua organização pode ser um alvo trampolim para possibilitar acesso a uma outra organização. Esses agressores tem muito a ganhar, e estão dispostos a investir tempo e esforço para pesquisar seus alvos.



A melhor maneira de se proteger contra spear phishing é estar ciente de que você pode ser um alvo, limitar as informações que publica sobre si mesmo, e reportar e-mails suspeitos.

Por exemplo, um governo estrangeiro pode decidir que a sua organização desenvolve um produto ou tecnologia que é fundamental para o seu sucesso econômico e começar a visá-lo. Eles pesquisam o site de sua organização e identificam três indivíduos-chave. Estes atacantes então pesquisam as páginas desses três indivíduos no LinkedIn, Twitter e Facebook para criar um dossiê completo sobre eles. Depois de analisar estes indivíduos, os atacantes criam um mail de spear phishing fingindo ser um fornecedor que sua organização utiliza. O e-mail tem um anexo que finge ser uma fatura, quando na realidade ele está infectado. Dois dos três indivíduos-alvo são enganados pelos e-mails de phishing e abrem o anexo infectado, dando ao governo estrangeiro total acesso aos seus computadores e, em última instância, a todos os segredos de produtos da sua organização, que agora poderá ser desenvolvido por eles.

Spear phishing é uma ameaça muito mais perigosa do que os ataques de phishing comuns, pois os atacantes estão construindo um ataque específico para você ou sua organização. Isso não só aumenta as chances de sucesso dos atacantes, mas torna os ataques muito mais difíceis de detectar.

Protegendo-se

O primeiro passo para se proteger contra esses ataques direcionados é entender que você pode ser um alvo. Afinal, você e sua organização provavelmente possuem informações confidenciais que alguém pode querer, ou você pode ser usado para acessar outra organização que é o objetivo final dos atacantes. Depois de entender que você pode ser alvo, tome as seguintes precauções para proteger a si mesmo e sua organização:

- Limitar as informações que você publica sobre si mesmo, tais como fóruns e-mail, Facebook ou LinkedIn. Quanto “mais” informações pessoais você compartilha, mais fácil é para os atacantes cibernéticos para criarem um e-mail phishing que parece relevante e verdadeiro;
- Se você desconfiar de um email pedindo para abrir um anexo ou clicar em um link ou ainda pedindo informações pessoais, verifique a mensagem. Se a mensagem parecer vir de uma empresa ou

Spear Phishing

pessoa que conhece, use os contatos que você já tem para retornar a mensagem e verificar se eles realmente a enviaram para você;
- Apoie os esforços de segurança da sua organização, seguindo as políticas de segurança adequadas e fazendo uso das ferramentas de segurança, como antivírus, criptografia e correções de segurança que estiverem disponíveis para você;
- Lembre-se, a tecnologia não pode filtrar e parar todos os ataques de e-mail, especialmente e-mails de spear phishing. Se um e-mail parece um pouco estranho no começo, continue lendo com cuidado. Se você está preocupado que pode ter recebido um e-mail de spear phishing ou mesmo ter sido vítima de ataque de spear phishing, entre em contato com o helpdesk ou equipe de segurança da informação imediatamente.

Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em http://www.securingthehuman.org.

Versão Brasileira

Traduzida por: **Homero Palheta Michelini**, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte
Katia Lucia da Silva, Arquiteta de T/I, Tradutora - twitter.com/kl_silva

Recursos

Como evitar Spear Phishing (em Inglês): http://www.theatlanticwire.com/technology/2013/02/spear-phishing-security-advice/62304/

Evitando Engenharia Social e ataques de Phishing (em Inglês): http://www.us-cert.gov/ncas/tips/st04-014

Phishing: http://www.securingthehuman.org/resources/newsletters/ouch/2013#february2013

Como Reclamar: http://antispam.br/reclamar/

Termos e Definições de Segurança: http://cartilha.cert.br/glossario/

Termos Comuns de Segurança (em Inglês): http://www.securingthehuman.org/resources/security-terms

Delegacia de cyber crimes, por estado: http://www.safernet.org.br/site/prevencao/orientacao/delegacias

Dica SANS de Segurança do dia (em Inglês): https://www.sans.org/tip_of_the_day.php

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traduzida por: Homero Palheta Michelini, Michel Girardias, Katia Lucia da Silva, Rodrigo Gularte, Marta Visser