Relatório de incidente de segurança cibernética

Aplicar técnicas de proteção do sistema operacional

Introdução

Objetivo desse projeto trabalhar em cima do cenário apresentado as causas e soluções, e exemplificar os **logs de tráfego TCPDump**. Trabalhando em cima do **modelo** dado pela Coursera, o projeto será dividido em 3 sessões.

Cenário

Analise o cenário abaixo. Em seguida, conclua as instruções passo a passo.
Você é analista de segurança cibernética do yummyrecipesforme.com, site que vende receitas e livros de receitas. Um ex-funcionário decidiu atrair usuários para um site falso com malware.
O padeiro executou um ataque de força bruta para obter acesso ao host. Eles repetidamente inseriram várias senhas padrão conhecidas para a conta administrativa até adivinharem corretamente a correta. Depois de obter as credenciais de login, eles puderam acessar o painel de administração e alterar o código-fonte do site. Eles incorporaram uma função javascript no código-fonte que levava os visitantes a baixar e executar um arquivo ao visitar o site. Depois de incorporar o malware, o padeiro alterou a senha para a conta administrativa. Quando os clientes baixam o arquivo, eles são redirecionados para uma versão falsa do site que contém o malware.
Várias horas após o ataque, vários clientes enviaram um e-mail para o helpdesk da yummyrecipesforme. Eles reclamaram que o site da empresa os levou a baixar um arquivo para acessar receitas gratuitas. Os clientes alegaram que, depois de executar o arquivo, o endereço do site mudou e seus computadores pessoais começaram a funcionar mais lentamente.
Em resposta a esse incidente, o proprietário do site tenta fazer login no painel de administração, mas não consegue, então eles entram em contato com o provedor de hospedagem do site. Você e outros analistas de segurança cibernética são encarregados de investigar esse evento de segurança.
Para resolver o incidente, crie um ambiente de área restrita para observar o comportamento suspeito do site. Execute o analisador de protocolo de rede tcpdump e, em seguida, digite a URL do site yummyrecipesforme.com. Assim que o site for carregado, você será solicitado a baixar um arquivo executável para atualizar

Mateus Breno Soares Silva

Relatório de incidente de segurança cibernética

Aplicar técnicas de proteção do sistema operacional

seu navegador. Você aceita o download e permite que o arquivo seja executado. Em seguida, você observa que seu navegador redireciona você para uma URL diferente, greatrecipesforme.com, que contém o malware.

Os logs mostram o seguinte processo:

- O navegador inicia uma solicitação DNS: ele solicita o endereço IP da URL do yummyrecipesforme.com do servidor DNS.
- O DNS responde com o endereço IP correto.
- O navegador inicia uma solicitação HTTP: ele solicita a página da Web yummyrecipesforme.com usando o endereço IP enviado pelo servidor DNS.
- O navegador inicia o download do malware.
- O navegador inicia uma solicitação DNS para greatrecipesforme.com.
- O servidor DNS responde com o endereço IP do greatrecipesforme.com.
- O navegador inicia uma solicitação HTTP para o endereço IP do greatrecipesforme.com.

Um analista sênior confirma que o site foi comprometido. O analista verifica o código-fonte do site. Eles notam que o código javascript foi adicionado para solicitar que os visitantes do site baixem um arquivo executável. A análise do arquivo baixado encontrou um script que redireciona os navegadores dos visitantes de yummyrecipesforme.com para greatrecipesforme.com.

A equipe de segurança cibernética relata que o servidor web foi afetado por um ataque de força bruta. O padeiro descontente foi capaz de adivinhar a senha facilmente porque a senha de administrador ainda estava definida para a senha padrão. Além disso, não havia controles para evitar um ataque de força bruta.

Seu trabalho é documentar o incidente em detalhes, incluindo a identificação dos protocolos de rede usados para estabelecer a conexão entre o usuário e o site. Você também deve recomendar uma ação de segurança a ser tomada para evitar ataques de força bruta no futuro.

Mateus Breno Soares Silva

Relatório de incidente de segurança cibernética

Aplicar técnicas de proteção do sistema operacional

Logs TCPDump

14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A? yummyrecipesforme.com. (24)
14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A 203.0.113.22 (40)
14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859 ecr 0,nop,wscale 7], length 0
14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags [S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS val 3302576859 ecr 3302576859,nop,wscale 7], length 0
14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [.], ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0
14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1
14:18:36.786595 IP yummyrecipesforme.com.http > your.machine.36086: Flags [.], ack 74, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0
...<a lot of traffic on the port 80>...
14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. (24)
14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A 192.0.2.17 (40)
14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649 ecr 0,nop,wscale 7], length 0
14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags [S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS val 3302989649 ecr 3302989649,nop,wscale 7], length 0
14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags [.], ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 0
14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 73: HTTP: GET / HTTP/1.1
14:25:29.576597 IP greatrecipesforme.com.http > your.machine.56378: Flags [.], ack 74, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 0
...<a lot of traffic on the port 80>..

Mateus Breno Soares Silva

Relatório de incidente de segurança cibernética

Aplicar técnicas de proteção do sistema operacional

Primeira sessão

Identificar o protocolo de rede envolvido no incidente:

Nota-se nos logs que o problema é oriundo do link http, o usuário tenta acessar o yummyrecipesforme.com, mas acaba sendo direcionado para outro endereço, o greatrecipesforme.com, esse site é altamente malicioso e é o principal agente que está causando problemas aos clientes.
Ao entrar no greatrecipesforme.com, automaticamente o navegador baixa um malware infectando o dispositivo de quem acessa, os relatos são de lentidão do dispositivo e a interação de uma interface web diferente da yummyrecipesforme.com.

Segunda sessão

Documentar o incidente:

Ao obter essas informações e associar a demanda de solicitações vindas do Helpdesk sobre o problema, a equipe de segurança poderá agir para solucionar o problema o quanto antes.
Um bom método para analisar o comportamento do malware, é implementando um sandbox e estudar o arquivo malicioso. Com isso, pode-se coletar dados para que exista meios de eliminar as consequências nos dispositivos infectados dos clientes.
Outro fator crucial, é analisar o código fonte de todo o site, e identificar o local do scritpt malicioso identificado com arquivo em JavaScript. Além de analisar mais afundo para identificar todas as brechas para extinguir qualquer possibilidade de futuros ataques.
O incidente foi proposto por um ataque de brute force, dando acesso a todo codigo fonte do site para que o criminoso pudesse aplicar um script malicioso, fazendo com que o navegador ao tentar conectar com o yummyrecipesforme.com fosse direcionado ao greatrecipesforme.com, fazendo com que no navegador baixasse um arquivo malicioso.

Mateus Breno Soares Silva

Relatório de incidente de segurança cibernética

Aplicar técnicas de proteção do sistema operacional

Terceira sessão

Recomende uma solução para ataques de força bruta:

Elaborar senhas extremamente fortes, um exemplo é utilizar senhas complexas com caracteres que não existam comumente no teclado. Uma boa prática é utilizar um gerador de senhas específico para isso, e um gerenciador de senhas atribuído somente para pessoas da equipe que o líder do setor tenha alta confiança.
Caso haja qualquer desligamento, para evitar o mínimo risco, é necessário gerar uma nova senha. Lembrando-que, a melhor senha é a que o próprio usuário não sabe.

Mateus Breno Soares Silva