# Relatório de incidentes de segurança

|  |
| --- |
| **Seção 1: Identificar o protocolo de rede envolvido no incidente** |
| Os seguintes protocolos de rede foram identificados como envolvidos no incidente, com base na análise do tráfego de log e na descrição do cenário:   * **DNS (Domain Name System):** Utilizado para resolver os nomes de domínio yummyrecipesforme.com e greatrecipesforme.com para os seus respetivos endereços IP.   + Exemplo do log: 14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A? yummyrecipesforme.com.   + Exemplo do log: 14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. * **TCP (Transmission Control Protocol):** Utilizado para estabelecer ligações fiáveis antes da transmissão de dados HTTP entre a máquina do utilizador e os servidores web.   + Exemplo do log (início do handshake para yummyrecipesforme.com): 14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [S], ...   + Exemplo do log (início do handshake para greatrecipesforme.com): 14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S], ... * **HTTP (Hypertext Transfer Protocol):** Como o problema estava no acesso ao servidor web do site yummyrecipesforme.com, sabemos que as solicitações de páginas web aos servidores web envolvem tráfego http. Além disso, quando executamos o tcpdump e acessamos o site yummyrecipesforme.com, o arquivo de log tcpdump correspondente mostrou o uso do protocolo http ao contatar o. O arquivo malicioso é observado sendo transportado para os computadores dos usuários usando o protocolo HTTP na camada de aplicação. * Utilizado para o pedido e a transferência do conteúdo das páginas web de yummyrecipesforme.com e greatrecipesforme.com.   + Exemplo do log (pedido GET para yummyrecipesforme.com): 14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, ... length 73: HTTP: GET / HTTP/1.1   + Exemplo do log (pedido GET para greatrecipesforme.com): 14:25:29.576590 IP your.machine.56378 >   + greatrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, ... length 73: HTTP: GET / HTTP/1.1 |
|

|  |
| --- |
| **Seção 2: Documente o incidente** |
| Um ex-funcionário obteve acesso não autorizado ao painel de administração do site yummyrecipesforme.com através de um ataque de força bruta, explorando uma senha de administrador padrão. Após o acesso, o atacante modificou o código-fonte do site, inserindo um script JavaScript. Este script induzia os visitantes a descarregar e executar um ficheiro malicioso, disfarçado de atualização de navegador. A execução deste ficheiro resultava no redirecionamento do navegador do utilizador para um site fraudulento, greatrecipesforme.com, que continha malware. Vários clientes contactaram o suporte técnico do yummyrecipesforme.com reportando o pedido de download suspeito e a subsequente lentidão dos seus computadores. O proprietário do site confirmou a perda de acesso ao painel de administração, uma vez que o atacante também alterou a senha de administrador. A investigação num ambiente controlado (sandbox), com recurso à ferramenta tcpdump, confirmou o fluxo de tráfego que levava ao redirecionamento para o site malicioso greatrecipesforme.com após a interação inicial com yummyrecipesforme.com. |

|  |
| --- |
| **Seção 3: Recomendar uma correção para ataques de força bruta** |
| Para prevenir e mitigar futuros ataques de força bruta, recomendam-se as seguintes medidas de segurança:   * **Implementação de Políticas de Senhas Robustas:**   + Exigir senhas complexas (combinação de letras maiúsculas, minúsculas, números e símbolos) para todas as contas, especialmente as de administrador.   + Definir um comprimento mínimo para as senhas (ex: 12 caracteres ou mais).   + Obrigar à alteração de todas as senhas padrão imediatamente após a configuração inicial de sistemas ou aplicações.   + Proibir o uso de senhas comuns ou facilmente adivinháveis.   + Implementar a expiração periódica de senhas. * **Mecanismos de Bloqueio de Contas:**   + Configurar o bloqueio automático de contas após um pequeno número de tentativas de login falhadas consecutivas (ex: 3 a 5 tentativas).   + O bloqueio deve ser temporário (ex: 15 a 30 minutos) ou exigir uma redefinição manual por um administrador. * **Autenticação Multifator (MFA):**   + Implementar e exigir MFA para todas as contas com privilégios elevados, incluindo o acesso ao painel de administração do site. A MFA adiciona uma camada de segurança ao exigir uma segunda forma de verificação para além da senha. * **Limitação de Taxa de Pedidos (Rate Limiting):**   + Implementar controlos para limitar o número de tentativas de login permitidas a partir de um único endereço IP ou para uma conta específica num curto espaço de tempo. * **Utilização de CAPTCHA:**   + Integrar mecanismos de CAPTCHA nas páginas de login para distinguir entre utilizadores humanos e bots automatizados que realizam ataques de força bruta. * **Monitorização e Alertas de Segurança:**   + Implementar um sistema de monitorização para detetar e alertar sobre atividades de login suspeitas, como múltiplas tentativas falhadas, logins de localizações geográficas atípicas ou em horários invulgares. * **Alteração de Nomes de Utilizador Padrão:**   + Evitar o uso de nomes de utilizador de administrador padrão (ex: "admin", "administrador") e utilizar nomes únicos e menos previsíveis. * **Revisão Periódica de Contas e Privilégios:**   + Auditar regularmente as contas de utilizador e os seus níveis de acesso, removendo contas inativas ou desnecessárias e aplicando o princípio do menor privilégio. * **Web Application Firewall (WAF):**   + Considerar a implementação de um WAF para ajudar a filtrar tráfego malicioso, incluindo tentativas de força bruta, antes que estas cheguem ao servidor de aplicações. * **Formação e Consciencialização em Segurança:**   + Promover formação regular para todos os funcionários, incluindo administradores, sobre as melhores práticas de segurança, com ênfase na importância de senhas fortes e na identificação de tentativas de ataque. |