29 de abril de 2020

Alerta nº 02/2020
Nova campanha de sequestro de contas de gerenciamento de domínio cadastradas no Registro.br

Atualização: 29 de abril de 2020

Por favor, entre em contato com o **CTIR Gov**, caso tenha alguma dúvida relacionada a esta publicação em sua Coordenação ou pelos contatos abaixo.

Informações:
https://www.ctir.gov.br

E-mail:
cgtir@presidencia.gov.br

Telefone:
+55 (61) 3411-3477

Notificação de Incidentes:
ctir@ctir.gov.br

INOC-DBA: 10954*810

Obs.: Os alertas, aqui disponibilizados, têm o objetivo de fornecer informações oportunas sobre problemas, vulnerabilidades e explorações de segurança atuais.

1. Descrição do Problema

Com base nas estatísticas de eventos ocorridos no espaço cibernético e nos diversos relatos que tem sido feitos pelos colaboradores durante a crise do COVID-19, o **CTIR Gov** recomenda a divulgação, em todos os órgãos de governo e entidades vinculadas, do presente alerta, sobre uma campanha nacional de Sequestro de Contas de Gerenciamento de Domínio cadastradas no Registro.br, realizada por grupos hacktivistas , a qual caracteriza-se por ações maliciosas para obtenção de acesso às contas de gerenciamento de domínio e alteração da configuração dos servidores DNS, direcionando os usuários para páginas fraudulentas.

2. Impacto

Diversos casos desse tipo de ataque foram confirmados contra órgãos de governo. Nessa espécie de abuso, um atacante que obteve acesso indevido a credenciais pode modificar o local para o qual os recursos de nome de domínio de uma organização são resolvidos. Com isso, as requisições dos usuários são direcionadas para páginas fraudulentas, as quais podem conter códigos maliciosos capazes de comprometer a máquina do usuário, com possível reflexo na rede de computadores da organização. Problemas como *phishing*, download involuntário de malwares, exposição à exploração de vulnerabilidades nos aplicativos instalados no computador e nos equipamentos da rede de computadores da organização podem afetar a segurança e, em consequência, a imagem de toda a instituição.

3. Dispositivos Afetados

Existe risco ativo que pode afetar partes fundamentais da infraestrutura do Sistema de Nomes de Domínio (DNS), que é responsável por converter nomes de domínios para endereços IP e vice-versa.

Usando as técnicas a seguir, os invasores podem redirecionar e interceptar o tráfego da *Web* e de *e-mail,* utilizando para outros fins indevidos.

1. Um atacante inicia a ação maliciosa obtendo, indevidamente, as credenciais (usuário e senha) com privilégios de alteração nos sistemas de registros de DNS.
2. Em seguida, o atacante altera registros DNS, como registros de Endereço (A), *Mail Exchanger* (MX) ou Servidor de Nomes (NS), substituindo o endereço legítimo de um serviço por um endereço por ele controlado. Esta alteração faz com que o tráfego de usuários seja direcionado para uma infraestrutura fraudulenta, com a possibilidade de manipulação ou inspeção dos dados antes de repassá-los ao destino legítimo.
3. Como o atacante pode definir valores de registro DNS, ele também pode obter certificados de criptografia válidos para os nomes de domínio de uma organização. Isso permite que o tráfego redirecionado seja descriptografado, expondo qualquer dado enviado pelo usuário. Como o certificado é válido para o domínio, os usuários finais não recebem avisos de erro.

Uma vez sequestrados, os domínios segmentados deixam de resolver seus endereços IP legítimos e começam a resolver a infraestrutura controlada por atores. Os atores também podem criar certificados para os domínios. Isso permite que os visitantes continuem a estabelecer conexões confiáveis, apesar de estarem apontando para uma infraestrutura mal-intencionada. Os dados disponíveis mostram que os domínios mais afetados são sequestrados por períodos muito curtos, às vezes um dia ou menos, com um domínio mostrando resoluções para um endereço IP malicioso por mais de um mês.

4. Recomendações

As seguintes práticas são recomendadas para ajudar a proteger as redes contra essa ameaça:

- Atualizar as senhas de todas as contas que podem alterar os registros DNS das organizações.
- Implementar autenticação multifator “2FA” em contas de registradores de domínio ou em outros sistemas usados para modificar registros DNS, conforme Art 3º da IN nº 31, de 17 de abril de 2020 do ME.
- Para ativar a autenticação 2FA, primeiramente o gestor deverá acessar a respectiva conta no site do Registro.br (https://registro.br/login/). Após o fornecimento do Código, CPF, CNPJ ou domínio e a senha, o gestor deverá clicar em segurança, no canto superior direito da tela (https://registro.br/painel/usuario/seguranca/). No próximo passo, o gestor deverá utilizar a opção de cadastrar o Token no aplicativo, fornecido pelo Google *Authenticator*. Por meio dele, o gestor receberá o código que ativará o token.
- Não utilizar e não vincular e-mails pessoais em suas contas do Registro.br e aos domínios gov.br.
- Reforçar aos gestores que atualizem suas informações junto ao Registro.br, cadastrando a conta corporativa de cada instituição a que pertence e remover quaisquer vinculações de e-mails pessoais aos domínios pelos quais são responsáveis.
- Auditar os registros DNS públicos para verificar se eles estão resolvendo o local pretendido.
- Procurar por certificados de criptografia relacionados a domínios e revogar todos os certificados solicitados de forma fraudulenta.

- Esse tipo específico de ataque não pode ser realizado se as extensões de ***Domain Name System Security Extensions (DNSSEC)*** estiverem ativas.

5. Referências

- Alerta nº 01/2019 - Campanha de Sequestro de infraestrutura de DNS. Disponível em: https://www.ctir.gov.br/arquivos/alertas/2019/alerta_2019_01_campanha_de_hijacking_de_infraestrutura_de_dns.pdf. Acesso em 27 de abril de 2020.
- *Alert (AA19-024A) - DNS Infrastructure Hijacking Campaign* - Disponível em: *https://www.us-cert.gov/ncas/alerts/AA19-024A*. Acesso em: 25 de mar 2019.
- *ICANN Calls for Full DNSSEC Deployment, Promotes Community Collaboration to Protect the Internet* - Disponível em: *https://www.icann.org/news/announcement-2019-02-22-en*. Acesso em: 25 de mar 2019.
- *Widespread DNS Hijacking Activity Targets Multiple Sectors* - Disponível em: *https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/*. Acesso em: 25 de mar 2019.
- **PADRÕES PARA NOTIFICAÇÃO DE INCIDENTES AO CTIR Gov**. (*https://www.ctir.gov.br/arquivos/publicacoes/Padronizacao_Notificacao_CTIRGov.pdf*)

Coordenação-Geral do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CGCTIR)

Informações: cgtir@presidencia.gov.br
Notificação de incidentes: ctir@ctir.gov.br