Departamento de Segurança da Informação – **DSI** *dsic.planalto.gov.br/*

25 de março de 2019

Alerta nº 01/2019
Campanha de Sequestro de infraestrutura de DNS

Atualização: 25 de março de 2019

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) 3411-2315

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

Acompanhando publicação do ***National Cybersecurity and Communications Integration Center (NCCIC)*** - https://www.us-cert.gov/ncas/alerts/AA19-024A, e ***Internet Corporation for Assigned Names and Numbers (ICANN)*** – https://www.icann.org/news/announcement-2019-02-22-en o **CTIR Gov** recomenda a divulgação, em todos os órgãos de governo e entidades vinculadas, do presente alerta, sobre uma campanha global de sequestro de infraestrutura do Sistema de Nomes de Domínio (*Domain Name System - DNS*).

Foi relatada uma série de ataques altamente complexos e generalizados envolvendo suspeitos de roubar grandes volumes de senhas de *e-mail* e outros dados confidenciais de governos e empresas privadas. Não existe ainda a confirmação sobre a atuação em infraestrutura brasileira.

2. Impacto

Usando credenciais comprometidas, um invasor pode modificar o local para o qual os recursos de nome de domínio de uma organização são resolvidos. Isso permite que o invasor redirecione o tráfego de usuários para uma infraestrutura controlada por invasores e obtenha certificados de criptografia válidos para os nomes de domínio de uma organização, permitindo ataques de intermediários (*man-in-the-middle*). Segundo a ***ICANN***, é possível, com esses ataques, se espionar dados pelo caminho e enviar tráfego para outro local, ou permitir que um invasor represente ou espie sites críticos.

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 endereços IP em nomes de domínio.

Os *links* a seguir possuem cópias dos indicadores de comprometimento (IOCs) das fontes listadas na seção **Referências**:

- IOCs (.csv) – https://www.us-cert.gov/sites/default/files/publications/AA19-024A_IOCs.csv
- IOCs (.stix) - https://www.us-cert.gov/sites/default/files/publications/AA19-024A_IOCs.stix.xml

Usando as técnicas a seguir, os invasores redirecionaram e interceptaram o tráfego da *Web* e de *e-mail,* usando para outros serviços de rede.

1. O invasor começa comprometendo as credenciais do usuário ou obtendo-as por meios alternativos de uma conta que pode fazer alterações nos registros DNS.
2. Em seguida, o invasor 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 que o invasor controla. Isso permite que eles direcionem o tráfego do usuário para sua própria infraestrutura para manipulação ou inspeção antes de passá-lo para o serviço legítimo, caso assim escolham. Isso cria um risco que persiste além do período de redirecionamento de tráfego.
3. Como o invasor 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.

A empresa de segurança ***CrowdStrike*** publicou um *post* (https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/) listando praticamente todos os endereços da Internet conhecidos abusados pela campanha de espionagem até hoje:

Linha do tempo de sequestros de Infraestrutura de DNS		
Endereços IP Maliciosos	**Período Ativo**	**País das organizações afetadas (Setor)**
142.54.179[.]69	*February 2017*	*Jordan (Government)*
89.163.206[.]26	*February 2017*	*Jordan (Government)*
185.15.247[.]140	*December 2017 and January 2018*	*Kuwait (Government)* *Albania (Government)*
146.185.143[.]158	*August 2018*	*UAE (Government)*
128.199.50[.]175	*September 2018*	*UAE (Unidentified Sector)*
185.20.187[.]8	*September 2018*	*UAE (Law Enforcement)* *UAE (Government)* *Lebanon (Government)* *Lebanon (Civil Aviation)*
82.196.8[.]43	*October 2018*	*Iraq (Government)*
188.166.119[.]57	*October 2018 and November 2018*	*Egypt (Government)* *Libya (Government)*

Endereços IP Maliciosos	Período Ativo	País das organizações afetadas (Setor)
206.221.184[.]133	*November 2018*	*Egypt (Government)*
37.139.11[.]155	*November 2018*	*UAE (Unidentified Sector)*
199.247.3[.]191	*November 2018*	*Iraq (Government)* *Albania (Government)*
185.161.209[.]147	*November 2018*	*Lebanon (Insurance)*
139.162.144[.]139	*December 2018*	*Jordan (Government)*
37.139.11[.]155	*December 2018*	*UAE (Unidentified Sector)*
178.62.218[.]244	*December 2018*	*UAE (Government)* *Cyprus (Government)*
139.59.134[.]216	*December 2018*	*Sweden (Internet Infrastructure)* *Saudi Arabia (Internet Services)* *Lebanon (Internet Services)*
82.196.11[.]127	*December 2018*	*Sweden (Internet Infrastructure)* *U.S. (Internet Infrastructure)*
46.101.250[.]202	*December 2018 and January 2019*	*Saudi Arabia (Government)*
Domínios dos invasores usados como servidores de nome para infraestrutura sequestrada		
cloudipnameserver[.]com *cloudnamedns[.]com* *lcjcomputing[.]com* *mmfasi[.]com* *interaland[.]com*		

Uma vez sequestrados, os domínios segmentados deixaram de resolver seus endereços IP normais e começaram a resolver a infraestrutura controlada por atores. Os atores também criariam certificados para os domínios, principalmente por meio do *Let's Encrypt*, autoridade de certificação que fornece certificados *X.509* gratuitos para criptografia *TLS*. Isso permitiria que os visitantes continuassem a estabelecer conexões confiáveis, apesar de estarem apontando para uma infraestrutura mal-intencionada. Os dados disponíveis mostram que os domínios mais afetados foram 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 em contas de registradores de domínio ou em outros sistemas usados para modificar registros DNS.
- 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

- *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