Atores de ameaças que exploram provedores dinâmicos de DNS para ativi

Data: 2025-09-29 06:02:37

Autor: Inteligência Against Invaders

Os pesquisadores de segurança cibernética identificaram uma tendência crescente em que os atores de ameaças estão cada vez mais explorando os provedores dinâmicos de DNS para sediar infraestrutura maliciosa, representando riscos significativos para organizações empresariais em todo o mundo.

Os fornecedores dinâmicos de DNS, também conhecidos como provedores de subdomínio alugável publicamente, tornaram -se alvos atraentes para atores maliciosos devido à sua acessibilidade e supervisão regulatória limitada.

Esses serviços funcionam essencialmente como “Mini Domain Registrars” sem o mesmo nível de escrutínio que os registradores de domínio legítimos enfrentam.

Ao contrário do registro tradicional de domínio, que requer conformidade com os processos ICANN e IANA, os provedores dinâmicos de DNS precisam apenas comprar um domínio e estabelecer sua própria infraestrutura de roteamento.

Pesquisa mais recente de Silent Push revela que mais de 70.000 domínios estão atualmente alugando subdomínios por meio desses serviços, muitos dos quais operam com controles mínimos de supervisão e segurança.

O apelo aos atores de ameaças está em vários fatores -chave. Muitos provedores aceitam pagamentos de criptomoeda e anunciam o registro anônimo sem exigir detalhes de “conhecer seu cliente”.

Essa combinação de anonimato e verificação mínima cria um ambiente ideal para atores maliciosos estabelecerem infraestrutura de comando e controle enquanto evitam a detecção.

Tipos de serviços de aluguel de subdomínio

O ecossistema dinâmico de DNS abrange vários modelos de serviço, cada um apresentando diferentes desafios de segurança:

Serviços de controle limitado: Esses provedores restringem o DNS uma configuração de registro, permitindo algum controle de conteúdo. Serviços como o BlogSpot se enquadram nessa categoria, embora existam métodos para contornar as restrições de conteúdo padrão.

Controle somente de conteúdo: Plataformas como páginas. Records DNS e endereços IP.

Serviços de controle total: Ofertas premium como o medo.org fornecem hospedagem completa e controle de conteúdo, normalmente disponíveis através de planos pagos. Esses serviços apresentam o maior risco, pois oferecem a máxima flexibilidade dos atores de ameaças para atividades maliciosas.

A equipe de inteligência de ameaças da Silent Push desenvolveu recursos sofisticados de monitoramento para rastrear o ecossistema dinâmico de DNS.

Sua metodologia de pesquisa combina várias fontes de dados para fornecer cobertura abrangente de ameaças em potencial.

O sistema de rastreamento incorpora dados da lista de sufixos públicos, concentrando-se na subseção “Domínios Privados”, que inclui serviços corporativos e fornecedores de qualidade inferior.

A equipe dedicou atenção especial ao medo, que opera dezenas de milhares de domínios alugando subdomínios, com alguns que remontam a aproximadamente 25 anos.

As pesquisas de padns para registros de ns relacionados podem ser realizadas em nossa plataforma, como o exemplo a seguir:

A complexidade do rastreamento desses serviços é ilustrada pelos domínios “furtivos” do medo, que não são listados publicamente e só podem ser identificados através da análise de registros do NameServer.

A plataforma de Silent Push identificou mais de 591.000 resultados por meio do NameServer DNS, as pesquisas por medo.org sozinhas.

Grandes campanhas de atores de ameaças

Grupos de ameaças de alto perfil alavancaram extensivamente os serviços DNS dinâmicos para operações maliciosas. O APT29 foi documentado exclusivamente usando domínios DNS dinâmicos para o comando quietexit e comunicações de controle em 2022.

O grupo Gameardon foi observado utilizando esses serviços em campanhas direcionadas às entidades ucranianas, enquanto Aranha espalhada Incorporou domínios publicamente alugáveis ??em suas operações de janeiro de 2025.

Painel de segurança cibernética da TitAnhq mostrando o tráfego da web de hoje, resumos de solicitação e estatísticas de filtragem baseadas em categorias

Apt28 (Urso Fancy) recebeu menção específica em um 2024 FBI Relatório para a utilização pesada de domínios DNS dinâmicos. A adoção generalizada desses serviços por grupos de ameaças persistentes avançados demonstra sua eficácia em fugir das medidas de segurança tradicionais.

Casos notáveis ??adicionais incluem o uso de domínios DNS personalizados e dinâmicos da APT33, a forte dependência do ator de ameaça do DDGroup nesses serviços para as comunicações C2 e o uso documentado do Galium do APT Group em 2022.

O precedente histórico se estende a 2014, quando a Microsoft liderou os esforços para assumir os

domínios DNS dinâmicos no IP que foram fortemente usados ??em ataques em andamento.

As implicações de segurança do abuso dinâmico de DNS se estendem além da simples hospedagem de domínio. Esses serviços podem aparecer inadvertidamente na Enterprise Lists, criando possíveis lacunas de segurança quando os funcionários solicitam acesso ao conteúdo bloqueado.

Quando os atores de ameaças controlam subdomínios em serviços que não respondem a queixas de abuso, a infraestrutura se torna altamente atraente para comando e controle comunicações.

Diferentemente dos domínios tradicionais, onde os registradores e os provedores de hospedagem podem ser contatados para solicitações de remoção, os serviços DNS dinâmicos geralmente apresentam opções de remediação limitadas.

A persistência de subdomínios maliciosos representa uma preocupação significativa. Mesmo quando as empresas de segurança cibernética identificam e relatam atividades maliciosas, os subdomínios podem permanecer ativos devido a fornecedores que não respondem ou procedimentos inadequados de manuseio de abuso.

Mitigações

O Silent Push recomenda que as organizações corporativas implementem estratégias proativas de monitoramento e bloqueio para domínios publicamente alugáveis. Suas exportações de dados em massa fornecem cobertura abrangente de domínios rastreados que alugam subdomínios e oferecem serviços DNS dinâmicos.

As organizações devem estabelecer políticas baseadas em riscos para lidar com conexões com esses domínios. Algumas empresas podem exigir um bloqueio completo de todas as conexões, a menos que os usuários solicitem manualmente exclusões específicas. Outros podem achar que os mecanismos de alerta fornecem visibilidade suficiente, mantendo a flexibilidade operacional.

O princípio principal para os defensores é reconhecer que subdomínios individuais nesses serviços podem variar dramaticamente em legitimidade.

Embora um subdomínio possa servir a propósitos legítimos, outro no mesmo serviço poderia hospedar infraestrutura maliciosa. Essa diversidade cria desafios defensivos únicos que exigem abordagens de segurança diferenciadas.

O cenário dinâmico de ameaças do DNS continua evoluindo à medida que esses serviços ganham popularidade entre usuários legítimos e atores de ameaças. Muitos provedores operam como empresas ou entidades com histórias documentadas de ignorar relatórios de abuso.

O setor de negócios que apoia esquemas de aluguel de subdomínio mostra mais esforços maliciosos do que os benignos, com algumas soluções corporativas experimentando uma exploração pesada por atores de ameaças sérias.

Os esforços de monitoramento em andamento de Silent Push ao longo de 2025 rastrearão novos desenvolvimentos neste espaço, incluindo a identificação de repositórios adicionais de domínios publicamente alugáveis ??e fornecedores dinâmicos de DNS emergentes.

A abordagem colaborativa da comunidade de segurança cibernética para identificar e rastrear esses serviços permanece essencial para manter posturas defensivas eficazes contra esse crescente vetor de ameaça.

Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas e definir GBH como uma fonte preferida em**Google**.**