Novo DNS Malware 'Detour Dog' usa TXT Records para entregar a Strela C

Data: 2025-10-01 12:35:32

Autor: Inteligência Against Invaders

O Detour Dog, uma campanha de malware furtiva rastreada desde agosto de 2023, evoluiu de redirecionar vítimas para golpes de apoio à tecnologia para um sofisticado sistema de distribuição de comando e controle de DNS (C2) que entrega o roubo de informações sobre a Strealer por meio de registros DNS TXT.

Dezenas de milhares de sites comprometidos em todo o mundo fazem solicitações DNS do lado do servidor que são invisíveis para os visitantes, permitindo redirecionamentos condicionais e execução remota de código.

Originalmente, o desvio de servidores de nomes controlados por cães direcionaram sites infectados para fazer um golpe de páginas de destino como Los Pollos e Help TDS.

No final de novembro de 2024, os redirecionamentos mudaram de Los Pollos para ajudar as redes afiliadas da TDS e do Monetizer TDS, mas o resultado – a monetização do tráfego agitada – permaneceu a mesma.

Iniciando a primavera 2025, apareceu um novo recurso: os servidores de nomes começaram a responder a consultas TXT DNS especialmente formatadas com comandos “Down” codificados por Base64, instruindo os sites comprometidos a buscar e executar scripts PHP dos servidores C2 remotos. Isso marca a primeira vez que o DOG DOG entregou malware diretamente aos usuários domésticos.

Em junho de 2025, pesquisadores observado Detour Dog Infrastructure Hosting The Starfish Backdoor, que instala a carga útil do ladrão de strela. A análise revelou que 69% dos hospedeiros confirmados de encenação de estrelas do mar estavam sob controle de cães de desvio.

Detendimento de cães Handcrafts Rastreando identificadores que são transportados em vários sistemas de distribuição de tráfego (TDSS).

Externamente, as estrelas do mar e a strela foram espalhadas por spam enviadas pela botnet Rem Proxy Mikrotik e da botnet da Tofsee.

Em 8 de junho, as respostas do DNS TXT começaram a fornecer URLs C2 para Terminais PHP -primeiro script.php Para entregar o downloader da estrela do mar, então file.php Para buscar o Arquivo de Zip Strela Stealer-criando uma cadeia de entrega orquestrada de DNS e várias etapas.

Dns txt como um canal secreto

Sites comprometidos geram consultas DNS TXT do formulário:

```
text....c2_domain
```

Quando corresponde a padrões como nwuuscript ou nauufileo servidor de nome autoritário retorna um registro txt prefixado com “Down” e um URL C2.

A saída de script PHP é retransmitida para a vítima, tudo por meio de solicitações de CURL do lado do servidor que evitam a detecção do lado do cliente.

Os registros passivos do DNS de 6 a 8 de agosto de 2025 mostram mais de 4 milhões de consultas, predominantemente benignas de respostas “não fazem nada”, mas os comandos ocasionais de execução remota revelam um modelo inovador de distribuição no estilo Monte.

A Fundação ShadowServer afundou o domínio C2 primário, webdmonitor[.]ioem agosto de 2025, apenas para o cão de desvio para girar aeroarrows[.]io em poucas horas. Os dados do poço capturaram mais de 39 milhões de consultas TXT em 48 horas, de 30.000 hosts infectados em 584 TLDs.

Embora o tráfego de bot dominasse – dividindo em 2 milhões de solicitações por hora – a IPS unique abrangeu 89 países, com os Estados Unidos representando 37% dos IPs de visitantes distintos.

Curiosamente, alguns IPs codificados pertenciam às sub -redes do Departamento de Defesa dos EUA, ressaltando o mistério de quem ou o que gera essas consultas.

Evolução histórica e laços de rede de afiliados

Detour Dog’s Origins Trace de volta a fevereiro de 2020, encaminhando inicialmente o tráfego para afiliados de Los Pollos identificados por IDs como bt1k60t e a integração posterior Ajuda os IDs de afiliados do TDS.

O link Los Pollos também inclui o Afiliate ID BT1K60T e o site é redirecionado para outro domínio, BraRaraildye[.]Live, hospedado em Hetzner, que acreditamos fazer parte do Taco Loco.

Cadeias de redirecionamento detalhadas documentadas em novembro de 2024 e 20 de novembro de 2024 ilustram transições de Ajuda TDS para TDS Monetizer com parâmetros de rastreamento consistentes (cid:11005).

Os cronogramas compostos revelam fluxos contínuos de afiliados que abrangem cinco anos e meio.

Esse Dns txt O modelo C2 representa uma nova arquitetura de distribuição de malware resiliente que disfarça a verdadeira infraestrutura C2 por trás de uma rede global de sites comprometidos.

Ao entrelaçar os fluxos de tráfego de marketing de afiliados com a execução remota baseada em DNS, o cão de desvio ofusca ofusca as correntes de ataque e desperta os defensores.

À medida que o Detour Dog continua refinando seu sistema – com testes passivos de DNS, indicando a expansão contínua dos recursos – organizações e caçadores de ameaças devem

incorporar estratégias de monitoramento e afundamento de TXT DNS para detectar e mitigar essas ameaças secretas.

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