Pesquisa alerta para aumento de risco cibernético em mecanismos de buscas

Pesquisadores revelaram que os hackers melhoraram suas estratégias de engenharia social e estão agora burlando as barreiras de detecção no tráfego comum de redes por meio de HTTP e HTTPS.

10/05/2023

A Netskope, líder em Secure Access Service Edge (SASE), divulgou hoje uma pesquisa que confirma que os hackers encontraram novos meios de burlar a detecção e se misturar ao tráfego normal de redes usando os protocolos HTTP e HTTPS para distribuir malwares.

O mais recente *Cloud & Threat Report: Global Cloud and Web Malware Trends* da Netskope identificou que, em média, cinco em cada mil usuários corporativos tentaram baixar malwares no primeiro trimestre de 2023 e 72% desses downloads continham novas famílias e variantes de malwares.

A evolução da engenharia social e do *data void* em mecanismos de buscas

Na pesquisa, a Netskope descobriu que cerca de 10% de todos os downloads de malwares no primeiro trimestre foram realizados a partir de mecanismos de buscas. Esses downloads resultaram, em sua maioria, de *data voids* – termo que se refere às informações irrelevantes ou inexistentes ao realizar buscas – ou combinações de termos de pesquisa que trazem pouquíssimos resultados aos usuários. Isso significa que qualquer conteúdo que corresponda a esses termos provavelmente aparecerá em uma posição muito alta nos resultados de buscas e terá mais potencial de atrair vítimas. Isso representa apenas uma das muitas técnicas de engenharia social que estão em ascensão no cibercrime.

A engenharia social como um todo continua a dominar como uma das principais técnicas de infiltração de malwares. Além dos mecanismos de pesquisa, os invasores continuam investindo em e-mail, aplicações de

colaboração e de bate-papo para enganar suas vítimas. Os dois principais tipos de malwares no primeiro trimestre deste ano foram os cavalos de Troia (trojans), responsáveis por 60% dos downloads, e os de phishing, representando 13%.

Avaliação dos canais de comunicação primários para atacantes

Pela primeira vez em seu relatório trimestral, a Netskope analisou os canais de comunicação utilizados pelos invasores. Esta análise revelou que, para evitar a detecção de forma consistente, os hackers usaram HTTP e HTTPS nas portas 80 e 443 como principal canal de comunicação. De fato, dos novos executáveis de malware analisados pela Netskope que se comunicaram com hosts externos, 85% o fizeram pela porta 80 (HTTP) e 67% o fizeram pela porta 443 (HTTPS). Essa abordagem permite que os atacantes passem facilmente despercebidos e se misturem ao volume de tráfego HTTP e HTTPS já existente nas redes.

Além disso, para burlar os controles de segurança baseados em DNS, algumas amostras de malware ignoram as pesquisas de DNS e, em vez disso, entram em contato diretamente com hosts remotos usando seus endereços IP. No primeiro trimestre de 2023, a maioria das amostras de malware iniciou comunicações externas usando uma combinação de endereços IP e nomes de host, com 61% se comunicando diretamente com pelo menos um endereço IP e 91% se comunicando com pelo menos um host por meio de uma pesquisa de DNS.

"A tarefa número um dos invasores é encontrar novas maneiras de encobrir seus rastros, à medida que as empresas colocam mais recursos na detecção de ameaças, mas essas descobertas indicam como ainda é fácil para eles realizarem isso à vista de todos", diz **Ray Canzanese**, diretor de Pesquisa de Ameaças do Netskope Threat Labs. "Então, conforme os invasores se movimentam em torno de serviços em nuvem que são amplamente utilizados nas empresas e aproveitam os canais populares para se comunicar, a mitigação de riscos multifuncionais se torna mais necessária do que nunca."

Visão ampliada das tendências globais de malware na nuvem e na Web

Outros destaques da pesquisa incluem:

- **55% dos downloads de malware HTTP/HTTPS vieram de aplicações em nuvem**, contra 35% no mesmo período do ano anterior. O principal fator é o aumento nos downloads de malware das aplicações de nuvem corporativas

mais populares, com **Microsoft OneDrive, rastreado como a mais popular por uma ampla margem**.

- O número de aplicações com downloads de malware também continuou a aumentar, **atingindo um máximo de 261 apps distintas no primeiro trimestre de 2023.**
- **Apenas uma pequena fração do total de downloads de malware da Web foi entregue em categorias da Web tradicionalmente consideradas arriscadas.** Em vez disso, os downloads estão espalhados por uma grande variedade de sites, sendo que os servidores de conteúdo (CDNs) são responsáveis pela maior fatia, com 7,7%.

Os esforços das empresas para se defender contra o ataque de malware precisa incluir a colaboração multifuncional entre várias equipes, como redes, operações de segurança, resposta a incidentes, liderança e até mesmo colaboradores individuais. Algumas das etapas adicionais que podem ser adotadas para reduzir os riscos incluem:

- Inspecionar todos os downloads HTTP e HTTPS, incluindo todo o tráfego da Web e da nuvem, para evitar que o malware se infiltre em suas redes;
- Garantir que os controles de segurança inspecionem recursivamente o conteúdo de arquivos populares e que os tipos de arquivos de alto risco sejam completamente inspecionados.
- Configurar políticas para bloquear downloads de aplicações que não são usadas em sua empresa para reduzir a superfície de riscos.

Fonte: *Netskope*