Microsoft

O Jogo da Confiança:

Mudanças de tática impulsionam o comprometimento de e-mails corporativos

Microsoft Threat intelligence

Cyber Signals

Maio 2023

Entre 2019 e 2022, a Unidade de Crimes Digitais da Microsoft observou um **aumento de 38%** no Cybercrime-as-a-Service que tem e-mails corporativos como alvo

Introdução

A fraude em e-mails corporativos continua a aumentar, de acordo com dados do Federal Bureau of Investigation (FBI), que relatou mais de 21 mil reclamações com perdas acima de US$ 2,7 bilhões. A Microsoft observou um crescimento na sofisticação e nas táticas dos especialistas em ameaças voltadas ao comprometimento de e-mails corporativos (BEC), incluindo o aproveitamento de endereços IP (protocolos de internet residencial) para fazer com que os ataques pareçam gerados localmente.

Essa nova tática está ajudando os cibercriminosos a monetizarem ainda mais o Cybercrime-as-a-Service (CaaS) e chamou a atenção das autoridades federais porque permite que eles interrompam alertas de "viagens impossíveis" (também conhecidos como alerta de atividades suspeitas), usados para identificar e bloquear tentativas de login incomuns.

Somos todos defensores da cibersegurança

Recorte de Segurança

O recorte de dados representa tentativas de **BEC detectadas e investigadas** pela Unidade de Crimes Digitais (DCU) da Microsoft Threat Intelligence de abril de 2022 a abril de 2023. As remoções exclusivas de URL de phishing direcionadas pela DCU ocorreram entre maio de 2022 e abril de 2023.[1]

35 Milhões
Anual

156.000
Diário

417.678
Remoção de URL de phishing

Por dentro da ascensão do serviço BEC em escala industrial da BulletProftLink

A atividade cibercriminosa que compromete e-mails corporativos tem aumentado. A Microsoft observa uma tendência significativa no uso de plataformas como a BulletProftLink, um serviço popular para criar iniciativas maliciosas utilizando e-mail em escala industrial. A ferramenta vende um serviço de ponta a ponta, incluindo modelos, hospedagem e serviços automatizados para BEC. Os cibercriminosos que usam esse CaaS recebem as credenciais e o endereço IP da vítima.

Neste momento, eles compram endereços IP de serviços de protocolo residenciais correspondentes à localização da vítima, criando "proxies" IP residenciais que permitam que eles possam mascarar sua origem. Assim, contando com um endereço para que possam executar suas atividades maliciosas, além de nomes de usuário e senhas, os invasores podem ocultar movimentos, contornar alertas de atividade suspeita e abrir um gateway para realizar novos ataques.

A Microsoft observou criminosos cibernéticos na Ásia e em um país do Leste Europeu que estão implantando essa tática com mais frequência. O alerta de atividade suspeita é uma detecção usada para indicar que uma conta de usuário pode estar comprometida, sinalizando, por exemplo, restrições físicas que indicam que uma tarefa está sendo executada em dois locais, sem a quantidade apropriada de tempo para "viajar" de um local para o outro.

A especialização e a consolidação desse setor da economia do cibercrime podem escalar o uso de endereços IP residenciais para mascarar os dados e tornar a detecção dos ataques mais complexa. Endereços IP residenciais de vítimas mapeados em escala fornecem as ferramentas e a oportunidade para que os cibercriminosos possam reunir grandes volumes de credenciais e contas comprometidas. Os invasores estão usando serviços de IP/proxy que os profissionais de marketing e de outras áreas possam usar para pesquisa e utilizá-los para dimensionar esses ataques.

Resumo das ameaças

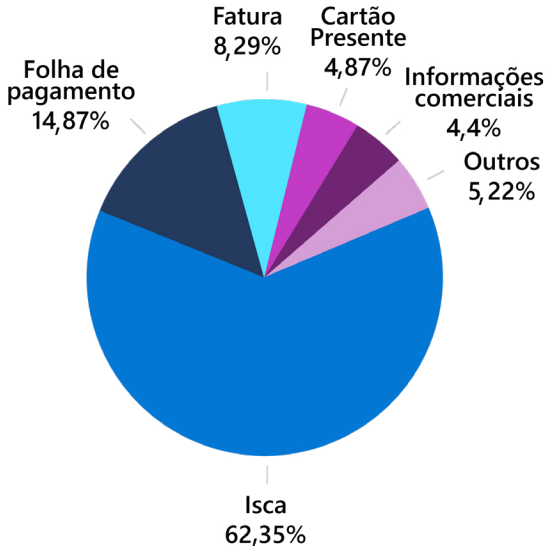
Um provedor de serviços IP, por exemplo, tem 100 milhões de endereços IP que podem ser rotacionados ou alterados a cada segundo.

Enquanto os cibercriminosos usam phishing em serviços como Evil Proxy, Naked Pages e Caffeine para implantar campanhas de phishing e obter credenciais comprometidas, a BulletProftLink oferece um design de gateway descentralizado, que inclui nós de blockchain públicos para hospedar sites de phishing e BEC, criando estrutura descentralizada da web e ainda mais sofisticada e difícil de interromper. Distribuir a infraestrutura desses sites pela complexidade e crescimento em evolução das blockchains públicas torna a identificação e remoção deles ainda mais complexos. Embora você possa remover um link de phishing, o conteúdo permanece online e os cibercriminosos retornam para criar um link para o conteúdo CaaS existente.

Ataques BEC bem-sucedidos custam às organizações, anualmente, centenas de milhões de dólares. Em 2022, a Equipe de Recuperação de Ativos do FBI iniciou a Cadeia de Destruição de Fraudes Financeiras, com 2.838 reclamações de fraudes BEC e envolvendo transações domésticas com perdas potenciais de mais de US$ 590 milhões.

Tipo de Email de Phishing de Comprometimento de Negócio

Os dados representam um instantâneo do phishing BEC por tipo de janeiro de 2023 a abril de 2023



Resumo das ameaças

Embora as implicações financeiras sejam significativas, danos mais amplos a longo prazo podem incluir roubo de identidade se as informações de identificação pessoal (PII) forem comprometidas, ou perda de dados confidenciais se a correspondência sensível ou propriedade intelectual forem expostas em e-mails mal-intencionados e tráfego de mensagens.

Os principais alvos da BEC são executivos e outros líderes seniores, como gerentes financeiros e equipes de recursos humanos com acesso a registros de funcionários que incluem, por exemplo, números, digitais, CPF, declarações fiscais, entre outras.Novos funcionários, talvez menos propensos a verificar solicitações de e-mail desconhecidas, também estão entre os alvos. Quase todas as formas de ataques BEC estão aumentando. As principais tendências para ataques BEC direcionados incluem isca, folha de pagamento, fatura, cartão-presente e informações comerciais.

Os ataques deste tipo se destacam na indústria do crime cibernético por sua ênfase na engenharia social e na arte de enganar. Em vez de explorar vulnerabilidades em sistemas ou dispositivos sem correções, os operadores desse cibercrime procuram explorar o grande tráfego diário de e-mail e outras mensagens para atrair as vítimas a fornecer informações financeiras, ou tomar uma ação direta, como enviar fundos, sem saber, para contas de "mulas de dinheiro", que recebem valores de terceiros em sua conta e ajudam os cibercriminosos a realizar transferências fraudulentas.

Ao contrário de um ataque de ransomware "barulhento" com mensagens de extorsão fortes e pertubadoras, estes cibercriminosos jogam um jogo de confiança silencioso, usando prazos e urgência inventados para estimular os destinatários, que podem estar distraídos ou acostumados com esses tipos de solicitações de última hora. Em vez de novos malwares, estes cibercriminosos alinham suas táticas para se concentrar em ferramentas que melhorem a escala, a plausibilidade e a taxa de sucesso da caixa de entrada de mensagens maliciosas.

Embora tenha havido vários ataques de alto perfil que aproveitam endereços IP residenciais, a Microsoft compartilha a preocupação das autoridades federais e de outras organizações de que essa tendência possa ser rapidamente dimensionada, dificultando a detecção de atividades com alarmes ou notificações tradicionais.

As variações nos locais de login não são inerentemente maliciosas. Por exemplo, um usuário pode acessar aplicativos de negócios com um laptop via Wi-Fi local e, simultaneamente, estar conectado aos mesmos aplicativos de trabalho em seu smartphone por meio de uma rede celular. Por essa razão, as organizações podem adaptar limites de alertas de atividade suspeita com base em sua tolerância ao risco. No entanto, a escala industrial do espaço de endereço IP localizado para ataques BEC cria riscos para as empresas, à medida que o ataque de BEC adaptável e outros invasores tomam cada vez mais a opção de rotear e-mails maliciosos e outras atividades por meio de espaço de endereço perto de seus alvos.

Recomendações:

Maximize as configurações de segurança protegendo sua caixa de entrada: as empresas podem configurar seus sistemas de e-mail para sinalizar mensagens enviadas de terceiros. Habilite notificações para remetentes não verificados. Bloqueie remetentes com identidades que você não pode confirmar e reporte estas mensagens como phishing ou spam em aplicativos.

Configure uma autenticação forte: torne o e-mail mais difícil de ser comprometido ativando a autenticação multifator (MFA), que requer um código, PIN ou impressão digital para fazer login, bem como uma senha. As contas habilitadas para MFA são mais resistentes ao risco de credenciais comprometidas e tentativas de login de força bruta, independentemente do espaço de endereço usado pelos invasores. A tecnologia sem senha fortalece ainda mais a segurança, verificando identidades no dispositivo, em vez de passar as credenciais do usuário por meio de uma conexão online vulnerável.

Treine os funcionários para identificar sinais de alerta: instrua os funcionários a identificar e-mails fraudulentos e outras mensagens mal-intencionadas, como uma incompatibilidade no domínio e endereços de e-mail, e o risco e o custo associados a ataques BEC bem-sucedidos.

Defenda-se dos ataques

Combater o comprometimento do e-mail corporativo requer vigilância e conscientização

Embora os agentes de ameaças tenham criado ferramentas especializadas para facilitar o BEC, incluindo kits de phishing e listas de endereços de e-mail verificados direcionados a líderes de áreas como contas a pagar e outras funções específicas, as empresas podem utilizar métodos para antecipar ataques e mitigar riscos.

Por exemplo, uma política DMARC (autenticação de mensagens, relatório e conformidade) baseada em domínio de "rejeitar" fornece uma proteção mais forte contra e-mails falsificados, garantindo que mensagens não autenticadas sejam rejeitadas pelo servidor antes da entrega. Além disso, os relatórios do DMARC fornecem um mecanismo para que a organização seja informada da origem de uma aparente falsificação, informação que normalmente não receberia.

Embora as organizações estejam há alguns anos gerenciando forças de trabalho totalmente remotas ou híbridas, ainda é necessário repensar a conscientização sobre segurança na era do trabalho híbrido. Como os funcionários estão trabalhando com mais fornecedores e profissionais terceirizados, recebendo assim mais e-mails "vistos pela primeira vez", é imperativo estar ciente do que essas mudanças nos ritmos de trabalho e correspondência significam para sua superfície de ataque.

As tentativas de BEC dos agentes de ameaças podem assumir várias formas, incluindo telefonemas, mensagens de texto, e-mails ou mensagens de mídia social. Falsificar mensagens de solicitação de autenticação e se passar por indivíduos e empresas também são táticas comuns.

Um bom primeiro passo defensivo é fortalecer as políticas para colaboradores das áreas de contabilidade, controles internos, folha de pagamento ou departamentos de recursos humanos sobre como responder quando solicitações ou notificações de mudanças relacionadas a instrumentos de pagamento, transações bancárias são recebidas. Dar um passo atrás para deixar de lado solicitações suspeitas e que não seguem as políticas, ou entrar em contato com uma entidade solicitante por meio de seu site legítimo e representantes, pode salvar as organizações de perdas impressionantes.

Os ataques BEC oferecem um ótimo exemplo de porque o risco cibernético precisa ser abordado de forma multifuncional com executivos e líderes, funcionários financeiros, gerentes de recursos humanos e outros com acesso a registros de funcionários, como números de seguridade social, declarações fiscais, informações de contato e agendas, juntamente com funcionários de TI, conformidade e riscos cibernéticos.

A DCU da Microsoft trabalha para interromper redes e infraestrutura de cibercriminosos usando tecnologia, perícia, ações civis, referências criminais e parcerias públicas e privadas.

Recomendações:

Use uma solução de e-mail segura: as plataformas de nuvem de e-mail de hoje usam recursos de IA, como aprendizado de máquina, para aprimorar as defesas, adicionando proteção avançada contra phishing e detecção de encaminhamento suspeito. Os aplicativos em nuvem para e-mail e produtividade também oferecem as vantagens de atualizações contínuas e automáticas de software e gerenciamento centralizado de políticas de segurança.

Proteger identidades para proibir movimentos laterais: um pilar fundamental para combater a BEC. Controle o acesso a aplicativos e dados com Zero Trust e governança de identidade automatizada.

Adote uma plataforma de pagamento segura: considere mudar de faturas enviadas por e-mail para um sistema projetado para autenticar pagamentos.

Faça uma pausa e use um telefonema para verificar transações financeiras: uma conversa telefônica rápida para confirmar que algo é legítimo vale a pena, em vez de assumir com uma resposta rápida ou clique, o que pode levar ao roubo. Estabeleça políticas e expectativas lembrando aos funcionários que é importante entrar em contato diretamente com organizações ou indivíduos — e não usar informações fornecidas em mensagens suspeitas — para verificar novamente as solicitações financeiras e outras.

Perfil do Especialista

"Para comprometer e-mails corporativos, basta phisihng de credenciais, engenharia social e muita dedicação dos cibercriminosos."

Simeon Kakpovi

Analista Sênior de Inteligência de Ameaças, Microsoft Threat Intelligence

Simeon Kakpovi inicialmente queria ser médico, mas logo percebeu que esse não era seu chamado. "Troquei de curso algumas vezes e fui parar nos sistemas de informação. Aterrissei na cibersegurança porque os meus mentores estavam na área."

Como estudante do segundo ano na Howard University, ele teve aulas adicionais de segurança cibernética em uma faculdade comunitária local, levando-o ao Lockheed Martin Cyber Analyst Challenge. "Eles nos enviaram um pen drive com 80 gigabytes de dados. O que aconteceu a seguir é uma das melhores experiências que já vivi."

O desafio exigia que os participantes analisassem uma invasão cibernética completa usando captura de pacotes e arquivos de memória. "Por meio desse processo, percebi o panorama da segurança cibernética e pensei: 'Eu adoraria fazer isso para viver'".

Isso levou a um estágio na Lockheed Martin e à co-criação do jogo de cyber skilling KC7. "Muitas aulas de cibersegurança são ministradas com siglas e conceitos vagos porque eles não têm acesso a dados reais. Isso cria um problema circular, porque você não pode obter as habilidades até conseguir o emprego, mas não pode obter os empregos a menos que tenha as habilidades."

Hoje, Simeon lidera a equipe de analistas da Microsoft que acompanha mais de 30 grupos iranianos. Embora distintos em motivação e atividade, Simeão observa que todos os criminosos iranianos compartilham um traço comum: tenacidade.

"Descobrimos que o Irã é persistente e paciente, disposto a gastar esforço, tempo e recursos para comprometer seus alvos. Eles oferecem um bom lembrete de que você não precisa usar explorações de software de dia zero ou novas técnicas ofensivas para ser bem-sucedido. Para comprometer e-mail, phishing de credenciais, engenharia social e pura garra é tudo o que é necessário. A engenharia social nem sempre é tão simples quanto parece. Vimos agentes de ameaças aproveitarem as informações pessoais reveladas nas redes sociais para atrair vítimas durante campanhas de engenharia social."

Por exemplo, o Crimson Sandstorm usa perfis falsos de mídia social (chamados de honey pots) direcionados a indivíduos com base em empregos listados em seu perfil no LinkedIn. Então, durante um período de alguns meses, eles tentam estabelecer relacionamentos usando inteligência coletada de perfis públicos para construir confiança e relacionamento, eventualmente enviando alvos BEC, arquivos maliciosos disfarçados de vídeos ou pesquisas. No entanto, como essas relações foram desenvolvidas durante um longo período, os destinos eram mais propensos a ignorar alertas de segurança quando executavam esses arquivos.

Simeon observa que os cibercriminosos iranianos são motivados por uma ampla gama de razões. "Ao rastrear a tempestade Mint Sandstorm e os ataques a agências que trabalham com governos, às vezes a política nuclear é o fio condutor. Com 'think tanks' ou instituições acadêmicas, publicar informações críticas ao governo iraniano pode despertar a ira de um grupo de cibercriminosos do país. Isso sugere que eles podem saber como os EUA ou outros países ocidentais se posicionarão em termos de política e visarão indivíduos com informações úteis para seu governo."

[1] Metodologia: Para dados instantâneos, as plataformas Microsoft, incluindo o Microsoft Defender for Office, Microsoft Threat Intelligence e Microsoft Digital Crimes Unit (DCU), forneceram dados anônimos sobre vulnerabilidades de dispositivos e dados com atividades e tendências dos agentes de ameaças. Além disso, os pesquisadores usaram dados de fontes públicas, como o "Federal Bureau of Investigation (FBI) 2022 Internet Crime Report" and Cybersecurity & Infrastructure Security Agency (CISA). A estatística de capa é baseada nos compromissos de Cibercrime como Serviço de e-mail corporativo da Microsoft DCU de 2019 a 2022. Os dados instantâneos representam tentativas de ataques BEC anuais e médias diárias ajustadas, detectadas e investigadas.