Google Cloud

Horizonte de Ameaças Cibernéticas

Relatório Horizonte de Ameaças Cibernéticas: 2º semestre de 2024

Office of the CISO

Índice

Missão

O relatório Threat Horizons do Google Cloud fornece aos tomadores de decisão inteligência estratégica sobre ameaças não só ao Google Cloud, mas a todos os provedores. O foco do relatório são as recomendações para mitigar riscos e aumentar a segurança na nuvem para profissionais e líderes de segurança da nuvem. O relatório baseia-se nos dados do Grupo de Análise de Ameaças do Google (TAG), da Mandiant, do Office of the Cloud CISO, da Engenharia de Segurança de Produto e de várias equipes de produtos, segurança e inteligência do Google Cloud.

Resumo executivo

Equipando os defensores da nuvem com medidas de mitigação de problemas de segurança na linha de frente sem servidor

A computação sem servidor surgiu como uma abordagem transformadora para o desenvolvimento de aplicativos, prometendo escalabilidade, redução das despesas operacionais e mais agilidade no tempo de lançamento no mercado.

Os produtos sem servidor também criam oportunidades para agentes de ameaça em provedores de nuvem com possíveis erros de configuração de segurança no ambiente do cliente. O que isso significa para os profissionais de segurança da nuvem?

Com base nas recentes ameaças à nuvem sem servidor que nossas equipes de segurança e inteligência encontraram, ao desenvolver uma estratégia de segurança na nuvem, você deve priorizar estas três considerações:

- **Credenciais comprometidas:** os agentes de ameaça continuam explorando as senhas fracas para ganhar acesso não autorizado a projetos do Google Cloud. Ao mesmo tempo, a computação sem servidor pode tornar a mineração de criptomoedas uma atividade ainda mais atraente para alguns agentes de ameaça, reforçando a importância dos esforços para identificar atividades suspeitas em ambientes na nuvem.
- **Exploração de erros de configuração:** nossa investigação sobre detecção e resposta mostra que é necessário garantir que as práticas recomendadas de segurança em ambientes sem servidor sejam aplicadas para evitar que os agentes de ameaça tirem proveito de erros de configuração.
- **Disseminação de malware:** os agentes de ameaça estão usando a tecnologia sem servidor e adaptando as táticas em resposta às detecções anteriores dos defensores da rede.

O relatório sobre a previsão para a segurança cibernética do Google Cloud de 2024 indicou que "tanto os criminosos cibernéticos quanto os operadores de segurança cibernética que trabalham para o governo vão usar ainda mais as tecnologias sem servidor na nuvem, porque elas fornecem mais escalabilidade e flexibilidade, e podem ser implantadas usando ferramentas automatizadas".

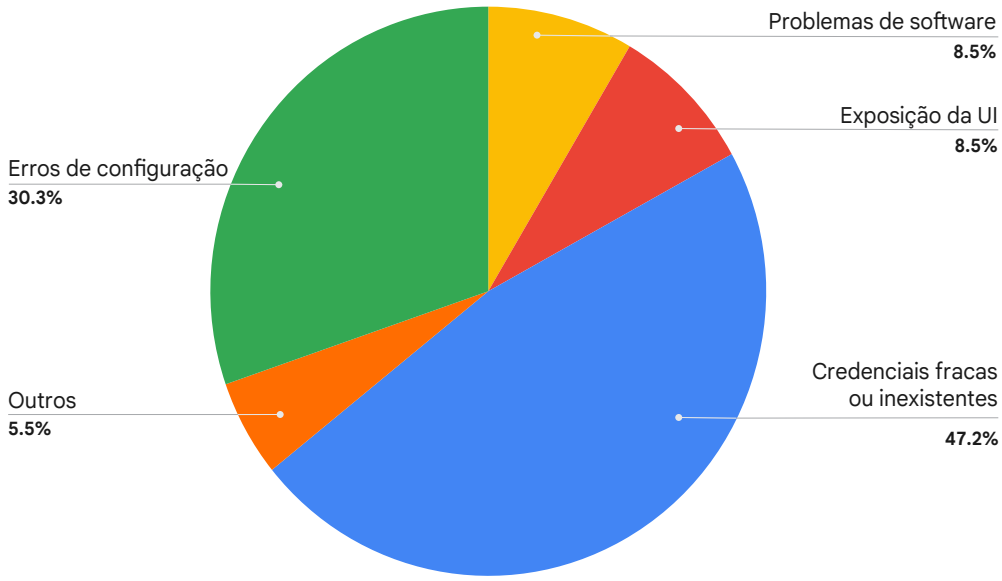
Vimos agentes de ameaça cumprirem essa previsão ao explorar vulnerabilidades da higiene de segurança da computação sem servidor. As seções a seguir vão mostrar em mais detalhes as principais lições aprendidas com essas ameaças à computação sem servidor para aumentar a defesa da segurança na nuvem.

De acordo com os dados: desafios relacionados à identidade continuam apresentando riscos aos ambientes sem servidor

Como parte do compromisso contínuo do Google Cloud com a segurança, o departamento Office of the Cloud CISO monitora atividades sobre incidentes e tendências associadas à forma como os agentes de ameaça estão obtendo acesso não autorizado aos ambientes na nuvem e seus objetivos quando conseguem entrar. Esses dados, junto com os novos insights obtidos na plataforma de Operações de Segurança do Google (antigo Chronicle), são apresentados a seguir.

O Google Cloud investigou os vetores de acesso inicial em diversas fontes no 1º semestre de 2024, analisando tanto as invasões bem-sucedidas no ambiente dos clientes quanto possíveis vulnerabilidades ou falhas encontradas em dados anonimizados das Operações de Segurança do Google em uma grande base de clientes. Com essa abordagem, nós conseguimos não só avaliar como esses agentes de ameaça invadiram os ambientes de nuvem dos clientes no 1º semestre, mas também determinar quais áreas das organizações têm o maior potencial para o aumento da segurança no 2º semestre.

Vetores de acesso inicial considerados (1º semestre de 2024)



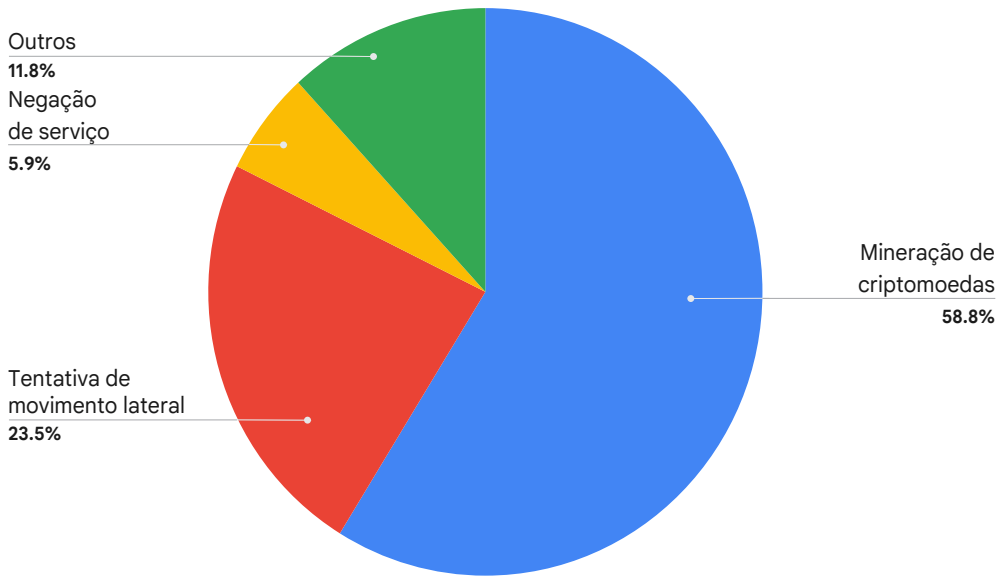
Credenciais fracas ou inexistentes é um fator importante para conseguir o acesso inicial, sendo o vetor mais bem-sucedido e o segundo gatilho mais comum das regras de detecção. Os erros de configuração, no entanto, subiram para mais de 30%, em grande parte devido ao elevado volume de detecções de fatores de ambientes pouco ou mal configurados.

Embora nem sempre sejam explorados pelos agentes de ameaça, esses erros de configuração continuam sendo uma porta aberta para uma possível atividade maliciosa. Um exemplo de problema de erro de configuração comum são chaves de contas de serviço com permissões excessivas ou controles de prevenção insuficientes contra o uso mal-intencionado. O risco imposto por erros de configuração revela um benefício importante da computação sem servidor que é minimizar a supervisão de configuração necessária para a manutenção dos processos críticos do servidor.

Além disso, essas descobertas justificam a importância da arquitetura sem servidor como parte de uma estratégia avançada de defesa mais ampla, como um controle de prevenção junto com outros controles de detecção em toda a extensão de uma possível invasão, para localizar e deter os invasores em vários pontos do processo. A categoria "Outros" inclui uma série de detecções suspeitas, como ferramentas de teste de invasão que conseguiram se infiltrar nas instâncias e tentativas de tunelamento DNS.

O objetivo final das invasões, em geral, foi o mesmo no 1º semestre de 2024, já que quase 59% das invasões foram motivadas por esforços de mineração de criptomoedas, um número um pouco menor do que o observado no 2º semestre de 2023 (65%).

Impacto observado das invasões (1º semestre de 2024)



Mitigações

- Muitos cenários que usam chaves de contas de serviço podem ser alcançados com métodos de autenticação mais seguros que não dependem do download e da distribuição dos principais arquivos. Além disso, o Google Cloud usa as configurações padrão da política organizacional para reduzir o risco imposto por ameaças à chave da conta de serviço como parte de sua arquitetura de segurança por padrão. Nós recomendamos avaliar e reduzir o uso de chaves de contas de serviço desnecessárias nas orientações que você encontra aqui.
- Garantir a adoção completa da autenticação multifatorial (MFA) para acesso administrativo a apps web sem servidor, bem como outras instâncias do Google Cloud.
- O teste de invasão é necessário para impedir que os agentes de ameaça usem ferramentas de segurança ofensivas básicas para acessar seu ambiente.
- Use a Detecção de ameaças a eventos do Security Command Center (SCC) do Google para identificar atividades suspeitas no ambiente de nuvem da sua organização, como a geração indevida de tokens ou observações de geolocalização anômalas. As organizações elegíveis podem usar o programa de proteção contra mineração de criptomoedas do SCC do Google.

Ameaças a funções sem servidor e serviços de back-end

A computação sem servidor oferece vantagens indiscutíveis, mas a segurança precisa estar integrada desde o início. Ao compreender o cenário de ameaças específico e implementar mitigações robustas, as organizações podem aproveitar os pontos fortes do ambiente sem servidor e proteger aplicativos, dados e sua infraestrutura na nuvem.

Durante as interações proativas e de resposta a incidentes nos últimos dois anos, a Mandiant observou diversas ameaças à arquitetura sem servidor em todos os provedores de nuvem. As seguintes ameaças deve ser consideradas ao implantar e operar uma arquitetura sem servidor:

- Informações confidenciais no código e de texto sem criptografia
- Invasores que usam a infraestrutura sem servidor para fins maliciosos
- Práticas de desenvolvimento e arquitetura inseguras
- Serviços de back-end mal-configurados

Informações confidenciais no código e de texto sem criptografia

A prática de incorporar informações confidenciais, como chaves API e credenciais de banco de dados, diretamente no código da função sem servidor ou nas variáveis do ambiente deve ser evitada a todo custo. Infelizmente, essa prática ainda é muito disseminada em todas as plataformas de nuvem e as informações confidenciais em texto não criptografado são comumente identificadas pela Mandiant nas interações proativas e de resposta a incidentes com clientes. Os principais riscos incluem:

- **Exposição:** se o seu código for exposto (vazamento de repositório, erro de configuração de permissões, ambiente de hospedagem comprometido etc.), os invasores poderão obter acesso a credenciais em texto não criptografado. Além disso, se conseguir acesso para somente leitura de recursos da nuvem, o invasor poderá acessar credenciais de texto sem criptografia armazenadas em variáveis ou código de função. Em ambos os casos, isso pode permitir a escalada de privilégios dentro do ambiente de nuvem ou a capacidade de fazer o movimento lateral para outras plataformas ou serviços.
- **Controle de versões:** as informações confidenciais no código ou em variáveis do ambiente geralmente contam com o controle de versão, o que cria um risco de longo prazo mesmo se a exposição inicial for resolvida.
- **Rotação de credenciais:** informações confidenciais dentro do código dificultam a tarefa de mudar as credenciais com regularidade. A rotação de credenciais ajuda a limitar um possível dano em caso de comprometimento das informações confidenciais. No entanto, para fazer a rotação de credenciais com informações confidenciais no código, é necessário modificar e reimplantar a função inteira, o que cria despesas operacionais e aumenta o risco de erros.

Mitigações e práticas recomendadas

- **Secret Manager:** use o Secret Manager do Google Cloud para armazenar e gerenciar suas informações confidenciais com segurança. O Cloud Run se integra ao Secret Manager para permitir que você monte informações confidenciais como variáveis do ambiente ou arquivos.
- **Nunca armazene informações confidenciais diretamente nas variáveis do ambiente:** as informações confidenciais armazenadas diretamente em variáveis no ambiente não são criptografadas e podem ser facilmente acessadas. O Cloud Run cria proativamente recomendações se detectar variáveis do ambiente que possam ser senhas, chaves de API ou credenciais de aplicativos do Google.
- **Princípio do privilégio mínimo:** siga o princípio do privilégio mínimo ao conceder aos serviços do Cloud Functions ou Cloud Run as permissões necessárias para acessar os devidos recursos. Isso minimiza um possível dano caso seu código ou suas credenciais fiquem comprometidos.
- **Varredura de segurança:** Rverifique regularmente seu código, as dependências e os recursos da nuvem em busca de possíveis exposições de informações confidenciais e credenciais. Essas verificações podem ser feitas usando ferramentas de código aberto, como trufflehog e detect-secrets, ou usando ferramentas de provedores de nuvem como a Proteção de dados confidenciais no Security Command Center.

Invasores que usam a infraestrutura sem servidor para fins maliciosos

Nos últimos anos, a Mandiant observou agentes de ameaça, como UNC2465, UNC4713 e APT41, que usam a infraestrutura sem servidor para disseminar malware ou comunicação de Comando e Controle (C2). Os agentes de ameaça usam ambientes de tempo de execução sem servidor como um proxy para tráfego destinado a uma infraestrutura controlada por agentes mal-intencionados ou ao direcionar o tráfego diretamente para a máquina comprometida1. A comunicação que está sendo transmitida de e para subdomínios do provedor de nuvem torna mais fácil para os agentes maliciosos ocultar seu tráfego malicioso.

Os agentes de ameaça conseguem manipular funções de forma que elas aceitem apenas as solicitações que atendam a critérios específicos, como usuário-agente, caminhos de URI, cabeçalhos ou parâmetros de consulta. Se uma solicitação não atender um ou mais desses requisitos, os agentes de ameaça conseguem redirecionar o tráfego para um site seguro ou, se uma função existente estiver sendo utilizada, eles conseguem permitir que a função seja executada conforme pretendido originalmente. A próxima seção deste relatório fala mais sobre esse tópico e explica em detalhes como os agentes de ameaça estão usando os serviços de nuvem sem servidor para propagar malware.

Mitigações e práticas recomendadas

- Restrinja o tráfego de saída de todos os recursos (nuvem e on-prem), salvo quando explicitamente necessário. Monitore o tráfego em busca de comunicação com serviços de nuvem não autorizados. Se for necessária uma conexão de saída, o Google Cloud Secure Web Proxy pode ajudar a monitorar e proteger o tráfego de saída de VMs, contêineres e ambientes sem servidor.
- Certifique-se de que as funções e serviços sem servidor estejam atrás de um Gateway de API e de um balanceador de carga de aplicativos, permitindo segurança adicional, como:
  - Integração com **firewall de aplicativos web (WAF)** para filtrar e excluir tráfego malicioso com base em ataques comuns na web.
  - **Integração de identidade ou chaves de API** para controlar o acesso por meio de autenticação e autorização.
  - **Imposição de HTTPS** em todas as solicitações recebidas para garantir que a criptografia seja implementada em trânsito de e para funções sem servidor.
  - **Registro em log e monitoramento aprimorados** para fornecer logs detalhados de chamadas de API, erros, monitorar o desempenho da API e anomalias.
- Examine e remova as permissões desnecessárias concedidas a usuários ou funções IAM e que permitam criar, modificar ou executar recursos sem servidor. O IAM recommender pode ajudar a identificar e remover permissões excessivas dos usuários no Google Cloud.
- Certifique-se de que o princípio do privilégio mínimo está sendo implementado para a função ou serviço. Consulte a próxima seção para obter uma orientação mais precisa.

Leia o design de segurança do Cloud Run, para entender como ele funciona, que também se aplica ao Cloud Functions. O Cloud Run e o Cloud Functions são executados, por padrão, em um ambiente de sandbox isolado.

Arquitetura e práticas de desenvolvimento inseguras

Em uma arquitetura sem servidor, o código é executado em contêineres de curta duração. Isso significa que não existe uma infraestrutura permanente para atacar, o que torna difícil para os agentes de ameaça ganhar acesso ao ambiente de nuvem. No entanto, como o próprio código é a base de uma função sem servidor, qualquer funcionalidade dentro dele pode ser explorada. Isso inclui falhas de injeção (como injeção de SQL, XSS), dependências inseguras e erros de lógica. O risco está no fato de um invasor usar os pontos fracos de recursos sem servidor para fazer o movimento lateral para outra infraestrutura da nuvem, onde ele pode ganhar mais acesso ou obter dados.

Por exemplo, um invasor pode conseguir usar uma função vulnerável para acessar as credenciais da conta de serviço. O Cloud Functions do Google Cloud usa uma conta de serviço padrão para executar funções, que é configurada com a função de editor. Se o token da conta de serviço for comprometido, o invasor terá amplas permissões no projeto, inclusive de listar todos os buckets de armazenamento na nuvem e de recuperar objetos dentro deles.

Mitigações e práticas recomendadas

- **Código seguro:** siga os princípios de código seguro, use ferramentas de análise dinâmica e estática e mantenha as dependências atualizadas para minimizar as vulnerabilidades. Além de seguir os princípios, use a checklist da OWASP (como validação de entrada, codificação de saída, tratamento de erros) para ver orientações específicas. No Google Cloud, a análise de artefatos pode fornecer informações sobre vulnerabilidades de imagens de contêineres armazenadas no Artifact Registry.
- **Princípio do privilégio mínimo:** conceda às cargas de trabalho sem servidor apenas as permissões que forem absolutamente necessárias para as operações. No Google Cloud, recomendamos criar uma conta de serviço exclusiva para cada recurso sem servidor e conceder a ela a função IAM mínima necessária. As políticas da organização devem ser usadas para impedir a concessão automática da função de Editor para contas de serviço padrão em novos projetos. Essa política agora é aplicada por padrão em todas as novas organizações do cliente.
- **Registro em log e detecção:** use os logs de auditoria das atividades do admin para identificar um uso da conta de serviço diferente da atividade esperada. Por exemplo, desenvolva uma detecção que alerte sobre o uso da conta de serviço de uma função em intervalos de IP inesperados ou o acesso de recursos inesperados.

Erros de configuração em serviços de back-end

As organizações que usam provedores de back-end como serviço (BaaS) sem servidor confiam neles para fazer o armazenamento e o gerenciamento de dados de seus aplicativos. No entanto, medidas de segurança mal configuradas ao implementar o recurso BaaS podem expor os dados a vazamento ou acesso não autorizado.

- **Endpoints de API acessíveis ao público:** quando os endpoints de API podem ser acessados sem autenticação ou autorização adequada, eles se tornam vulneráveis à exploração. Por exemplo, com acesso não autenticado a esses endpoints, os invasores podem buscar vulnerabilidades, extrair dados sigilosos e manipular a funcionalidade do aplicativo.
- **APIs não seguras:** mesmo com autenticação, as APIs podem continuar vulneráveis se não seguirem as práticas recomendadas de segurança. Por exemplo, uma validação de entrada insuficiente expõe o aplicativo a ataques de injeção, um tratamento de erro indevido pode causar o vazamento de informações e um limite de taxa inadequado facilita os ataques de força bruta.
- **Erros de configuração:** os provedores de BaaS oferecem bastante flexibilidade de configuração, mas, inadvertidamente, isso pode ocasionar erros de configuração que comprometem a segurança dos dados. Por exemplo, controles de acesso extremamente permissivos e erros de configuração de armazenamento podem contribuir para a exposição dos dados.

Mitigations and Best Practices

- **Automação:** trate as configurações de BaaS como código de software. Use ferramentas de infraestrutura como código (IaC) para definir e gerenciar as configurações. Assim, você pode fazer o controle de versões, testar e automatizar as alterações, reduzindo o risco de erro humano. Antes de implantar recursos usando IaC, use a ferramenta de verificação para identificar erros de configuração e informações confidenciais.
- **Diretrizes de configuração:** estabeleça e mantenha diretrizes de configuração de segurança para sua plataforma BaaS. Essas diretrizes devem definir configurações padrão seguras, controles de acesso, requisitos de criptografia e outros parâmetros de segurança.
- **Análise de segurança:** examine regularmente as configurações de BaaS para identificar e tratar os erros de configuração imediatamente. As ferramentas de verificação de configuração automatizadas podem facilitar muito o processo de análise. Essas ferramentas podem verificar as configurações de BaaS em busca de erros de configuração comuns, vulnerabilidades e descumprimento das práticas recomendadas de segurança.

Agentes de ameaça usam serviços na nuvem sem servidor para propagar malware

A arquitetura sem servidor atrai desenvolvedores e empresas por ser flexível, econômica e fácil de usar. Esses mesmos atributos fazem com que os serviços de computação sem servidor oferecidos por todos os provedores de nuvem atraiam também os agentes de ameaça e sejam usados para propagar e interagir com seu malware, hospedar e direcionar usuários a páginas de phishing, e para executar malware e scripts maliciosos feitos especialmente sob medida para serem executados em um ambiente sem servidor. A comunidade de pesquisa de segurança descobriu uma grande variedade uso indevido de infraestrutura legítima sem servidor por agentes mal-intencionados. Esse tipo de uso afeta todos os provedores de serviços de nuvem, incluindo Google Cloud, AWS, Azure, CloudFlare e outros.

A missão do Grupo de Análise de Ameaças do Google (TAG) é rastrear, monitorar e combater ameaças graves contra o Google e nossos usuários. Em 2023, o TAG detectou pessoas com motivação financeira que estavam usando indevidamente o Cloud Run e o Cloud Functions, os produtos de computação sem servidor do Google Cloud, para propagar malware e hospedar páginas de phishing.

Em resposta, as equipes do Google trabalharam em conjunto para interromper essas ações ao procurar instâncias maliciosas, atualizar a detecção no Safe Browsing e adicionar melhorias na segurança de produtos para impedir ameaças futuras. Conforme descrito no estudo de caso abaixo, nossa intervenção reduziu em 99% uma campanha de malware em relação a seus níveis de pico.

O Google Cloud Run e o Cloud Functions são serviços oferecidos pelo Google para criar e implantar serviços web. Alguns agentes de ameaça tiram proveito da flexibilidade e facilidade de implantação da plataforma, cujo objetivo é proporcionar uma experiência favorável para os usuários. Os painéis administrativos da plataforma fornecem informações detalhadas sobre solicitações e métricas de desempenho. É uma interface familiar para as pessoas que propagam malware por ser semelhante aos sistemas de distribuição de tráfego (TDS) que eles normalmente usam para determinar as métricas de sucesso das campanhas.

Estudos de caso

As equipes de segurança do Google buscam ativamente e interrompem ameaças que tentam usar o Google Cloud de maneira clandestina para propagar malware. Esses estudos de caso do ano passado mostram a abordagem proativa do Google Cloud para detectar e combater o uso indevido de nossos produtos de computação sem servidor e destacam nossos esforços contínuos para implementar medidas que mantenham os usuários seguros e garantam a segurança e confiança em nossas plataformas.

Em ambos os casos, agentes de ameaça com motivações financeiras usaram URLs de contêineres e domínios legítimos do Google Cloud, como cloudfunctions.net, para distribuir malware de roubo de informações e hospedar páginas de phishing de credenciais.

Propagação do infostealer Astaroth no Cloud Run e no Cloud Functions

Ao longo dos anos, os disseminadores do infostealer Astaroth usaram indevidamente uma grande variedade de provedores de serviços de nuvem e serviços online legítimos para distribuir malware para os usuários. Esses agentes de ameaça utilizaram inúmeras plataformas de nuvem, incluindo Google Cloud, Amazon AWS, Microsoft Azure e outras.

O uso indevido de recursos de computação sem servidor começou em 2019, quando pesquisadores da área de segurança observaram que eles estavam usando o Cloudflare Workers para criar URLs randomizadas para impedir a análise automatizada e propagar cargas maliciosas. Com base na América Latina, os disseminadores do infostealer Astaroth têm como principal alvo os usuários do Brasil e são conhecidos pela capacidade de atualizar com rapidez o malware e as técnicas de disseminação para evitar a detecção.

Em meados de 2023, o TAG e o Safe Browsing detectaram o uso indevido do Google Cloud por agentes que monitoramos, como o PINEAPPLE, que usaram o Cloud Run e o Cloud Functions para propagar o infostealer Astaroth. O PINEAPPLE usou instâncias comprometidas do Google Cloud e projetos do Google Cloud que eles criaram para gerar URLs de contêineres em domínios sem servidor legítimos do Google Cloud, como cloudfunctions.net e run.app. As URLs hospedavam páginas de destino que redirecionavam os usuários para uma infraestrutura maliciosa que implantava o Astaroth. Ao clicar nas URLs do Cloud Run e do Cloud Function, os usuários eram redirecionados a um bucket de armazenamento do Google Cloud que hospedava um arquivo ZIP contendo um arquivo Microsoft Installer (MSI) malicioso.

O PINEAPPLE mudou suas técnicas para convencer os gateways de que seus e-mails eram autênticos, usando, por exemplo, serviços de encaminhamento de e-mail, que não deixam mensagens com registros de falha do SPF, ou colocando dados inesperados no campo Return-Path do SMTP para exceder o tempo limite de solicitação DNS e causar uma falha na verificação de autenticação de e-mail do SPF.

Quando detectamos o uso indevido do Cloud Run e Cloud Functions pelo PINEAPPLE, as equipes do Google trabalharam juntas para buscar e interromper a atividade relacionada. Nós atualizamos as assinaturas de detecção e medidas de mitigação implementadas, que reduziram significativamente o volume das campanhas do Astaroth em 99% comparado ao auge da campanha.

Quando nossas equipes descobriam novas tentativas de uso indevido, o Safe Browsing e o TAG atualizaram as assinaturas e criaram uma detecção personalizada para identificar e bloquear as campanhas. Nós também incluímos URLs maliciosas na lista de bloqueio do Safe Browsing. O Google desativou os sites maliciosos do Cloud Run e suspendeu o projeto do Google Cloud associado. Nós também implementamos melhorias de segurança nos produtos para dificultar bastante o uso das nossas plataformas por esses agentes de ameaça.

O PINEAPPLE reage rapidamente e adapta de forma iterativa suas táticas, técnicas e procedimentos (TTPs) em resposta a novas detecções. Depois que o Google interrompeu as campanhas de uso indevido de grande escala, eles continuaram tentando usar indevidamente o Cloud Run de forma intermitente e em menor volume.

Em uma campanha recente bloqueada pelo Gmail, e-mails de spam do PINEAPPLE usaram o Ministério da Fazenda brasileiro como disfarce e direcionaram os destinatários a uma página falsa de engenharia social que simula o Portal da Nota Fiscal Eletrônica do governo brasileiro. O site instruía os visitantes a clicar em um botão para visualizar uma nota fiscal gerada pelo sistema.

Ao clicar no botão, os usuários eram direcionados a uma carga LNK hospedada em um endereço IP controlado pelos invasores. Em um provável esforço para evitar a detecção, os invasores incorporaram diversos serviços legítimos na campanha. Os links no site de engenharia social usaram o protocolo ms-search:// para direcionar os usuários para o endereço de IP dos invasores e os agentes de ameaça hospedaram o site no Google Cloud Run. O Google desativou o site malicioso no Cloud Run e suspendeu o projeto associado do Google Cloud.

Em março de 2024, as campanhas do PINEAPPLE tiveram seus mecanismos de distribuição atualizados temporariamente para usar instâncias do Google Compute Engine (GCE) com IPs públicos estáticos. Assim como nas atividades anteriores, as campanhas

Página de engenharia social imitando o sistema de emissão de notas fiscais eletrônicas do governo brasileiro

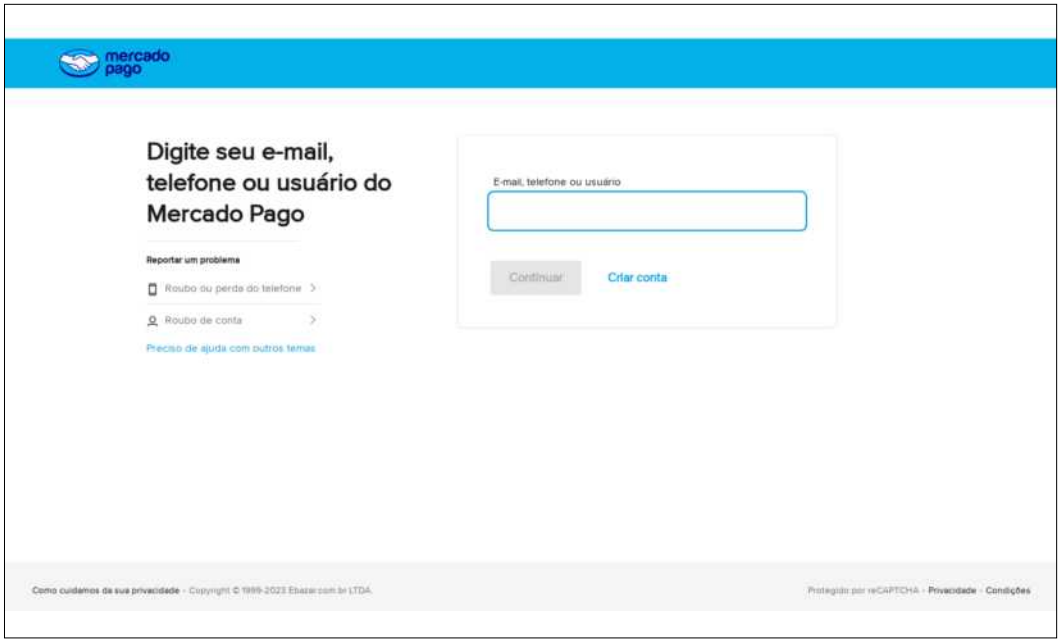
propagaram links maliciosos por e-mail. Os links do GCE funcionaram como um arquivo compactado não criptografado contendo um arquivo ZIP ou LNK. O PINEAPPLE mudou o tipo de arquivo usado, incluindo aqueles que não tinha usado antes, como .xz e.bz2. Em alguns casos, o arquivo compactado continha arquivos HTM, HTML ou MSI em vez de LNK.

Dias antes da tentativa de usar indevidamente o GCE em suas campanhas, o PINEAPPLE também testou outras plataformas de nuvem. No final de março de 2024, notamos que eles incorporaram o Azure Cloud Services e o Tencent Cloud em suas campanhas.

Pouco tempo depois, nas campanhas de maio e junho de 2024, o grupo continuou enviando spams se passando por agências federais brasileiras. Os e-mails maliciosos continham links para páginas de destino em servidores virtuais dedicados criados usando o serviço de nome de host de IP reverso da GoDaddy. Nós continuamos monitorando suas campanhas e atualizamos regularmente as proteções do Google para garantir a segurança dos usuários.

Projetos de phishing sem servidor

O FLUXROOT, outro agente localizado na América Latina e com motivação financeira, usou os contêineres do Google Cloud e testou as taxas de detecção de URLs do Google Cloud no VirusTotal. O FLUXROOT é conhecido pelo público por ter propagado o malware bancário Grandoreiro. Em 2023, o TAG identificou diversos projetos sem servidor do Google Cloud que estavam sendo usados para coletar credenciais para uma das maiores plataformas de pagamento online da América Latina. Ao descobrir os sites do FLUXROOT, o TAG e o Safe Browsing atualizaram as assinaturas de detecção e incluíram os sites na lista de bloqueio do Safe Browsing.



Página de coleta de credenciais hospedada em um projeto sem servidor do Google Cloud

A Central de confiança e segurança do Google Cloud suspendeu os projetos associados do Google Cloud e atualizou nossas detecções contra usos indevidos similares. Mais recentemente, o FLUXROOT continuou propagando o Grandoreiro, usando serviços de nuvem, como Azure e Dropbox, para disseminar o malware.

Impacto

Esses estudos de caso apontam para uma preocupação crescente: o uso indevido da computação sem servidor para fins maliciosos. Os agentes de ameaça se aproveitam da flexibilidade e fácil implantação das plataformas sem servidor para propagar malware e hospedar páginas de phishing. Os agentes de ameaça que usam indevidamente os serviços de nuvem mudam suas táticas em resposta às medidas de detecção e mitigação dos defensores. O grupo PINEAPPLE, por exemplo, melhorou várias vezes suas táticas, técnicas e procedimentos e experimentou diferentes serviços de nuvem na tentativa de evitar a detecção e continuar propagando o Astaroth.

Mitigações

As equipes de segurança do Google monitoram continuamente as ameaças aos nossos usuários e as tentativas de uso indevido dos nossos produtos. O Safe Browsing e o TAG atualizam regularmente as assinaturas de detecção e incluem URLs e domínios maliciosos na lista de bloqueio do Safe Browsing. A Central de confiança e segurança do Google Cloud monitora constantemente o uso indevido de serviços do Google Cloud e suspende projetos do Google Cloud operados por invasores, e a equipe de Engenharia de segurança de produtos do Google Cloud identifica falhas de segurança e mitigações que ajudam a melhorar a segurança dos produtos, o que dificulta cada vez mais o uso indevido de nossos produtos pelos agentes de ameaça.

Também recomendamos as seguintes abordagens para os clientes do Google Cloud, para ajudar a impedir a presença de malware na computação sem servidor:

- Para identidades e permissões, gerencie de perto as contas com muitos privilégios e acesso de administrador, e aplique o princípio do privilégio mínimo para garantir que cada usuário tenha o mínimo de permissões necessário.
- Incorpore o monitoramento e controles para detectar malware, software indesejado e outras ameaças baseadas em host usando o Applied Threat Intelligence no Google Security Operations e a Inteligência contra ameaças do Google. Os defensores da nuvem que atuam no setor público e privado também colaboram com o Serviço de análise de malware da Agência de segurança de infraestrutura e segurança cibernética do Departamento de Segurança Interna dos EUA.
- Use os alertas do Workspace sobre vazamento de senhas para monitorar as credenciais comprometidas, que são frequentemente roubadas pelo malware infostealer. Implemente um manual para redefinir as credenciais dos usuários e verificar os hosts afetados em busca de malware. O Monitoramento de ameaças digitais da Mandiant oferece proteção adicional avançada para monitorar mercados clandestinos, sites de compartilhamento de texto, blogs, fóruns e repositórios de malware e detectar vazamentos de credenciais e dados desconhecidos.
- Se você usar o Google Cloud Run, para os serviços de back-end, os tipos de mitigação de risco de cargas de trabalho conteinerizadas incluem incorporar o Container Threat Detection do Security Command Center do Google e não fazer download de contêineres que não forem confiáveis.
- Ajuste a configurações de rede do Cloud Functions e as configurações de rede do Cloud Run para permitir o controle da entrada e saída de dados da rede de e para funções individuais.

Contributors

Cris Brafman Kittner

Charles DeBeck

Kristen Dennesen

Dmitrij Lenz

Crystal Lister

Daniel Medina

Ashik Saji

Will Silverstone

Nader Zaveri

Google Cloud