Kaspersky
Hybrid Cloud
Security

A segurança de instâncias da nuvem pública é responsabilidade sua. Então, lide com ela.

2019

kaspersky

Saiba mais em kaspersky.com/hybrid

A segurança de instâncias da nuvem pública é responsabilidade sua. Então, lide com ela.

Introdução

O uso das nuvens públicas está crescendo porque elas oferecem muitos benefícios, como escalabilidade imediata, automação, facilidade de configuração e flexibilidade. Todos os envolvidos no gerenciamento de implementações de nuvens públicas, tanto de equipes de segurança de informações quanto pessoas de fora da área (como de DevOps ou WebDev), precisam garantir que a segurança dos ativos corporativos seja vista como um pilar do planejamento.

Este whitepaper foi criado para proporcionar aos especialistas em segurança da informação as informações e evidências necessárias para garantir que a segurança de cargas de trabalho na nuvem, ou seja, a segurança de cargas de trabalho na nuvem do sistema operacional que a carga de trabalho executa, seja tratada como um fator essencial em cenários de implementação em nuvem. Afinal de contas, se ocorrer uma violação de segurança na nuvem, o problema será seu. Independentemente de quem seja responsável tecnicamente, você terá de lidar com as consequências.

Nosso objetivo é neutralizar a visão equivocada de que coisas como a exploração de vulnerabilidades de software (quebra de login, execução remota de código, etc.), o "repo poisoning" de atualizações,
a exploração de conexões de rede (por exemplo, sequestro de DNS) e o comprometimento de informações de contas só acontecem em ambientes físicos ou virtualizados, e não em nuvens públicas. Ou que, nos ambientes de nuvens públicas, os danos que um incidente de segurança causa a seus dados ou sua organização de alguma forma deixam de ser um problema seu.

Além disso, o documento destaca alguns riscos específicos para empresas que as nuvens públicas apresentam, como o roubo de recursos na nuvem. Devido à escalabilidade imediata na nuvem, cibercriminosos que assumem seu controle da nuvem são capazes de executar e utilizar um volume praticamente infinito de capacidade de computação em seu nome e às suas custas. De uma maneira ou de outra, a proteção total de sua infraestrutura de nuvem pública tende ser um investimento sensato.

Vulnerabilidades em nuvens públicas

Além dos problemas de segurança em nuvens públicas mais temidos (e com razão), o comprometimento e a desconfiguração de contas, existem vetores de ameaças que visam instâncias, utilizando vulnerabilidades em serviços expostos à Internet, como RDP e SSH.

O RDP fica ativo por padrão em instâncias da Amazon, e a autenticação de dois fatores não tem suporte estrutural. O RDP tornou-se alvo de diferentes tipos de ataque. Alguns ataques usam apenas os logins mais populares com a descoberta de senhas por força bruta, enquanto outros violam os logins usando as senhas mais comuns. Alguns atacantes executam um número restrito e aleatório de tentativas de login, com um tempo limite entre as séries de tentativas para evitar a detecção automatizada. Um outro método de ataque é tentar descobrir por força bruta a senha do serviço de login SSM-User, muitas vezes pré-instalado em instâncias do AWS.

Tentativas de violação por força bruta semelhantes visam serviços SSH continuamente e, embora o SSH ofereça mais proteção que o RDP (por exemplo, autenticação de dois fatores), um serviço configurado sem atenção pode dar conceder imediato a um agente persistente mal-intencionado. Em conjunto, os ataques de força bruta via SSH e RDP representaram 12% de todos os ataques aos 'honeypots' da IoT da Kaspersky durante o primeiro semestre de 2019.[1]

As nuvens públicas podem e expõem você a vulnerabilidades. Veja alguns exemplos de como uma vulnerabilidade em software de terceiros proporciona a um invasor a oportunidade de executar um código na própria instância.

Em 3 de junho de 2019, foi descoberta uma vulnerabilidade no Exim, um servidor de e-mail conhecido que frequentemente é implementado em nuvens públicas. Essa vulnerabilidade permitia a execução remota de código. Se o servidor foi executado abaixo da raiz, como acontece com mais frequência, o código maligno introduzido no servidor seria então executado com privilégios raiz. Em julho de 2019, foi identificada uma outra vulnerabilidade do Exim que também permitia a execução de código remoto como raiz[2].

Outro exemplo é a invasão do site oficial do Linux Mint em 2016. Nesse caso, os pacotes de distribuição foram alterados para incluir um backdoor IRC com funcionalidade de DDOS. O cavalo de Troia também podia ser usado para colocar cargas maliciosas nas máquinas infectadas.

Houveram casos de módulos node.js maliciosos, contêineres infectados no Docker Hub[3] e muitos outros. Os cibercriminosos são muito criativos para descobrir pontos de entrada nas infraestruturas, especialmente quando há muitas infraestruturas muito semelhantes e com problemas parecidos, e todas convenientemente consideradas extremamente seguras estruturalmente, portanto sem exigir qualquer proteção adicional.

Mais da metade de todas as cargas de trabalho nas nuvens públicas são executadas no Linux, e existe um mito lastimável de que os atacantes não conseguem invadi-las.

Porém, certamente existem vulnerabilidades, módulos comprometidos e scripts maliciosos em ambientes Linux. Veja as estatísticas de ameaças para Linux do nosso laboratório de antimalware:

Ameaça	**%** de usuários afetados
Exploits	**41%**
Backdoors	**24%**
Cavalos de Troia	**14%**
Outras	**21%**

1 https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

2 https://www.bleepingcomputer.com/news/security/critical-exim-tls-flaw-lets-attackers-remotely-execute-commands-as-root/

3 https://www.helpnetsecurity.com/2019/04/29/docker-hub-breach/

Violações de segurança e ataques em nuvens públicas

O que um agente malicioso pode fazer depois de entrar em sua infraestrutura na nuvem? Além de obter acesso aos seus recursos corporativos, como dados de clientes, eles podem basicamente tirar proveito dos mesmos benefícios que a nuvem pública oferece a você: escalabilidade, automação e facilidade de configuração imediatas. Tudo às suas custas.

Caso 0 – Temos um problema

Mesmo que um cibercriminoso não faça nada depois de acessar um de seus sistemas, você ainda terá um problema: você sofreu uma violação. Em muitas jurisdições no mundo inteiro, se um sistema que trabalha com dados sigilosos, protegidos ou confidenciais for acessado, a lei exige que você notifique as autoridades sobre a violação, além de resolver todos os danos causados.

Muitas vezes, os custos indiretos da correção de uma violação de dados podem ser maiores que os custos diretos, e seus efeitos geralmente duram muito mais. E, se o computador comprometido for usado como um trampolim, ou seja, uma base para a movimentação lateral, vigilância, localização e extração de informações de contas com privilégios ou a reunião e extração de dados, consequências para você poderão ser desesperadoras.

Caso 1 – Ataque baseado em serviços SSH/RDP

Pense nisto:
O pagamento pela mineração secreta consiste basicamente em transferir dinheiro para a conta de um cibercriminoso. Não financie as atividades comerciais deles às custas das suas.

Se os invasores tiveram acesso via SSH a um dispositivo infectado, eles terão um alcance muito maior para converter a infecção em dinheiro. Na enorme maioria dos casos que envolvem sessões interceptadas investigados pela Kaspersky, encontramos envios de spam, tentativas de usar nossa honeytrap como servidor proxy e (finalmente e igualmente importante) mineração de criptomoeda[4]. De fato, no primeiro semestre de 2019, nós registramos mais de 50.000 tentativas de inscrito ambientes Windows Server com mineradores.

E como é possível evitar esses ataques?

Solução

A segurança para nuvens públicas eficiente deve ser capaz de tratar de casos como esse em várias frentes:

- O controle de aplicativos em modo de negação padrão recusaria automaticamente qualquer permissão para a implementação ou ativação do software do atacante
- A proteção em tempo de execução evitaria que softwares de sequestro de recursos fossem executados
- A proteção contra comportamento identificaria software de mineração, geração de spam e outros com intenções maliciosas com base em seu comportamento

Caso 2 – Perda de uma grande soma de dinheiro em muito pouco tempo

Com a escalabilidade imediata e a automação, os cibercriminosos que não se preocupam em ficar fora do radar podem acabar com o seu orçamento. A hora de uma instância do AWS custa algo entre 5 centavos e 5 dólares, o que pode chegar a US$ 125 por dia por instância. Não há um limite para o número de instância que o atacante pode executar em seu nome. Ele pode usar modelos de formação de nuvem para automatizar a geração de nova computação na nuvem a fim de realizar uma tarefa, como mineração de criptomoeda ou um ataque DDOS. O atacante precisa apenas criar novas instâncias um pouco mais rapidamente do que você é capaz de desativá-las. Não é impossível perder US$ 14 mil em um dia [5] ou até US$ 50 ou 60 mil [6]. Ou você pode aparentemente encontrar-se executando ou tornando-se vítima de um ataque DDOS [7]...

Solução

Uma solução de segurança eficaz poderia ajudar em várias frentes:

- Visibilidade – um mecanismo de alertas e sistemas de relatórios apropriados destacariam imediatamente qualquer acúmulo de instâncias para o administrador
- Controle de acesso à Internet – seria possível implementar uma política para evitar novas instâncias e a comunicação com servidores de C&C, além de evitar ataques de rede de saída

Caso 3 – Ataques à cadeia de fornecimento

Os ambientes construídos com muitas fontes oferecem muitas opções possíveis para atacar a cadeia de fornecimento de software, incluindo o envenenamento de repositórios Linux. Por exemplo, a empresa ucraniana MeDoc sofreu um ataque em seus mecanismos de atualização[8]. As atualizações comprometidas foram usadas para lançar um ataque baseado no ExPetr, o wiper de ransomware que visa plataformas Windows, que afetou muitas organizações, como a gigantesca farmacêutica Merck, a empresa de carga Maersk e infraestruturas críticas da Ucrânia.

4 https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

5 https://dev.to/juanmanuelramallo/i-was-billed-for-14k-usd-on-amazon-web-services-17fn

6 https://www.quora.com/My-AWS-account-was-hacked-and-I-have-a-50-000-bill-how-can-I-reduce-the-amount-I-need-to-pay

7 https://www.reddit.com/r/aws/comments/3qt4e0/so_i_was_ddosed_by_35924_amazon_aws_ip_addresses

8 https://securelist.com/schroedingers-petya/78870/

https://securelist.com/in-expetrpetyas-shadow-fakecry-ransomware-wave-hits-ukraine/78973/

https://www.npr.org/sections/thetwo-way/2017/06/27/534560169/large-cyberattack-hits-ukraine-snarling-electric-grids-and-airports

Solução

Mesmo que o malware venha como parte de uma atualização do sistema protegido, ele deve ser tratado exatamente como qualquer outro executável ou script: - deve ser analisado antes da execução e monitorado enquanto é executado. O controle de aplicativos no modo de negação padrão pode acrescentar mais uma camada de segurança.

Caso 4 – Do DevOps ao DevOps seguro

Malware e vulnerabilidades inseridos em imagens de contêineres podem resultar em vazamentos de IP corporativo ou na sabotagem de linhas de produção.O ataque à MeDoc mencionado é um exemplo. Em outro ataque, acredita-se que os hackers comprometeram o ambiente do build do CCleaner a fim de inserir malware [9] nos pacotes de distribuição oficiais do produto de segurança.

Solução

As equipes de DevOps que estão migrando o desenvolvimento para a nuvem e empregando ambientes e ferramentas dinâmicos, como contêineres, precisam reconhecer o risco envolvido e gerenciá-lo protegendo o ambiente de desenvolvimento baseado em nuvem.

Nossa própria solução de segurança específica para a nuvem, o Kaspersky Hybrid Cloud Security, oferece proteção em tempo de execução para hosts do Docker, garantindo práticas seguras de desenvolvimento. Também há APIs e outras ferramentas disponíveis para a automação do desenvolvimento e sua integração ao pipeline CI/CD.

Por que isso é um problema para você?

No primeiro semestre de 2019, nós impedimos mais de 250.000 ataques às plataformas Windows Server de nossos usuários. Isso sem considerar os AdWare e RiskWare.

Qualquer provedor de nuvem pública dirá a você que a proteção das instâncias da nuvem pública é responsabilidade sua[10,11]. Isso é fato.

Também é pouco provável que seu provedor de nuvem pública se responsabilize pelas consequências de qualquer violação de segurança em termos de custos ou danos a sua marca ou sua imagem pública.

E, além disso, não há limite para o volume de computação que um atacante pode obter em seu nome sem o seu conhecimento. Mais uma vez, você seria responsável pelos custos.

Você realmente precisa de um antivírus em uma nuvem pública?

O AWS acha que sim. Esta é a recomendação deles:

"Crie uma configuração de linha de base do servidor que incorpore patches de segurança atualizados e pacotes de proteção baseados em host, incluindo antivírus, antimalware, detecção/prevenção de invasões e monitoramento da integridade de arquivos."

"Cada instância do EC2 deve cumprir os padrões de segurança da organização. Não instale funções e recursos do Windows que não sejam necessários e instale software de proteção contra código malicioso (antivírus, antimalware, atenuação de exploits), monitore a integridade do host e execute a detecção de invasões. Configure o software de segurança para monitorar e manter as configurações de segurança do sistema operacional, proteger a integridade de arquivos críticos do sistema operacional e alertar sobre desvios em relação à linha de base da segurança." [12]

Nós também acreditamos que seja possível reduzir e gerenciar o risco de modo muito mais eficaz se você pode proteger os sistemas operacionais em suas instâncias e máquinas virtuais.

É óbvio que a proteção antivírus e antimalware básica não é suficiente. As práticas recomendadas do setor determinam que cada sistema operacional em uma infraestrutura precisa de proteção abrangente em várias camadas, e os provedores de nuvem pública fazem recomendações semelhantes.

Este é o ponto em que uma solução de segurança como o Kaspersky Hybrid Cloud Security entra em ação. Nossa solução protege diferentes tipos de cargas de trabalho executadas em diversas plataformas usando várias camadas de tecnologias de segurança, que incluem fortalecimento do sistema, prevenção de exploits, monitoramento de integridade de arquivos, bloqueador de ataques de rede, antimalware estático e comportamental e outras.

É essencial garantir a aplicação ininterrupta de níveis apropriados de segurança ao seu ambiente de nuvem pública para evitar ataques que poderiam se mostrar extremamente custosos e prejudiciais. É importante que a segurança seja reconhecida como um elemento básico de sua estratégia de nuvem contínua. Afinal de contas, em última instância, o problema é seu!

9 https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/

10 https://aws.amazon.com/compliance/shared-responsibility-model/

11 https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure

12 https://aws.amazon.com/answers/security/aws-securing-windows-instances/

www.kaspersky.com

Kaspersky Hybrid Cloud Security for AWS: kaspersky.com/aws
Kaspersky Hybrid Cloud Security for Azure: kaspersky.com/azure
Kaspersky Hybrid Cloud Security: kaspersky.com/hybrid

#hybrid
#aws_instance_security
#azure_vm_security