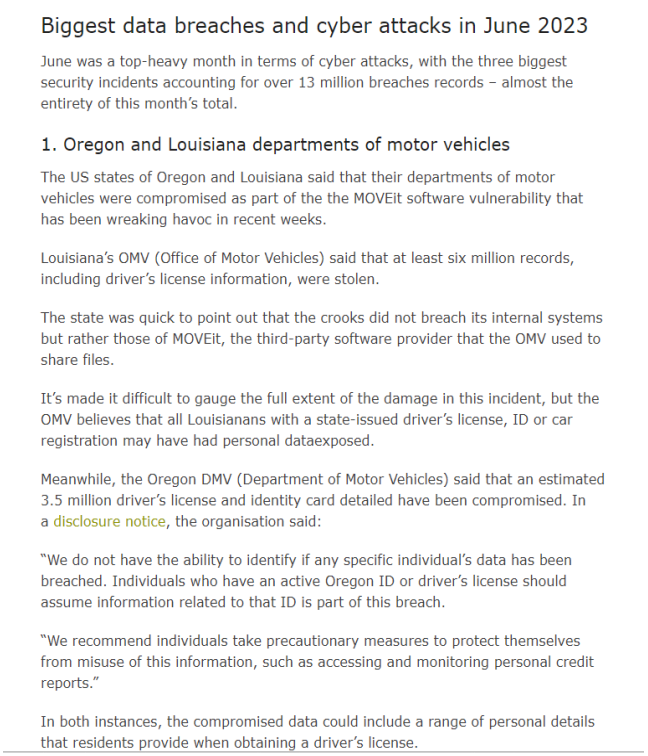
Proposta para Administração de Redes

Sumário

Apresentação..... 3
Quem somos.....5
Esta proposta contempla:..... 5
Valores.....6

Apresentação

Atualmente o mundo corporativo precisa estar conectado 100% do seu tempo. Ter conectividade tornou-se tão vital quanto a própria manutenção do negócio. Seja comunicação com os clientes, com os parceiros e até com o governo, toda empresa deve possuir conexões que suportem este trânsito de informações. Porém, com o advento das tecnologias, estar conectado não é o suficiente, surgiram termos que passaram a fazer parte da estratégia corporativa: LGPD, SGSI, PCI, HIPAA e uma grande variedade. Todos esses termos tratam da segurança e compliance das redes com os serviços ofertados. Essa preocupação se deu em função do crescente número de ataques às redes corporativas por agentes maliciosos. E são diversas as portas de entradas: E-mail, whatsapp, vulnerabilidades em dispositivos de redes e servidores. Ter um ambiente saudável e seguro atualmente, é crítico para qualquer tipo de negócio. Abaixo, algumas notícias sobre o tema segurança:



Biggest data breaches and cyber attacks in June 2023

June was a top-heavy month in terms of cyber attacks, with the three biggest security incidents accounting for over 13 million breaches records – almost the entirety of this month's total.

1. Oregon and Louisiana departments of motor vehicles

The US states of Oregon and Louisiana said that their departments of motor vehicles were compromised as part of the the MOVEit software vulnerability that has been wreaking havoc in recent weeks.

Louisiana's OMV (Office of Motor Vehicles) said that at least six million records, including driver's license information, were stolen.

The state was quick to point out that the crooks did not breach its internal systems but rather those of MOVEit, the third-party software provider that the OMV used to share files.

It's made it difficult to gauge the full extent of the damage in this incident, but the OMV believes that all Louisianans with a state-issued driver's license, ID or car registration may have had personal dataexposed.

Meanwhile, the Oregon DMV (Department of Motor Vehicles) said that an estimated 3.5 million driver's license and identity card detailed have been compromised. In a disclosure notice, the organisation said:

"We do not have the ability to identify if any specific individual's data has been breached. Individuals who have an active Oregon ID or driver's license should assume information related to that ID is part of this breach.

"We recommend individuals take precautionary measures to protect themselves from misuse of this information, such as accessing and monitoring personal credit reports."

In both instances, the compromised data could include a range of personal details that residents provide when obtaining a driver's license.

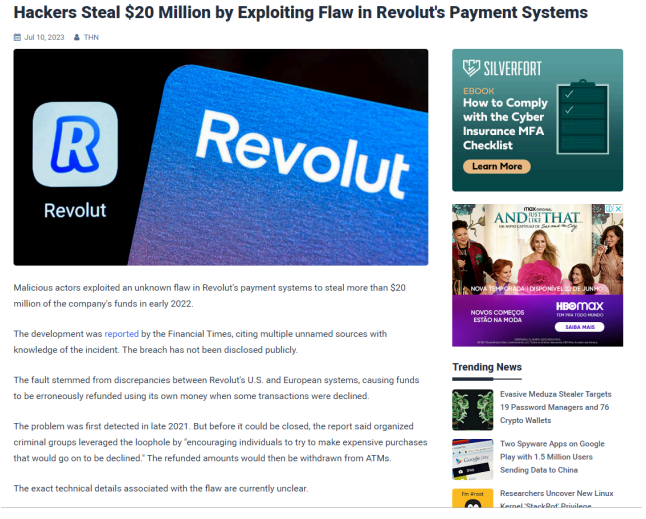
Ubiratan Cascales ▽ • 2º
Physicist | Cyber Threat Intelligence | OSINT
4 d • Editado •
+ Seguir

O porto de Nagoya, o maior e mais movimentado do Japão, ontem foi alvo de um ataque #ransomware que está afetando sua operação.

A autoridade portuária está trabalhando para restaurar os sistemas e planeja retomar as operações às 08h30 de amanhã.

Até então, todas as operações de carga e descarga de contêineres nos terminais com reboques foram canceladas, causando enormes prejuízos financeiros ao porto e graves interrupções na circulação de mercadorias.

Japan's largest port stops operations after ransomware attack
bleepingcomputer.com • 2 min de leitura



Hackers Steal $20 Million by Exploiting Flaw in Revolut's Payment Systems

Jul 10, 2023 THN

Malicious actors exploited an unknown flaw in Revolut's payment systems to steal more than $20 million of the company's funds in early 2022.

The development was reported by the Financial Times, citing multiple unnamed sources with knowledge of the incident. The breach has not been disclosed publicly.

The fault stemmed from discrepancies between Revolut's U.S. and European systems, causing funds to be erroneously refunded using its own money when some transactions were declined.

The problem was first detected in late 2021. But before it could be closed, the report said organized criminal groups leveraged the loophole by "encouraging individuals to try to make expensive purchases that would go on to be declined." The refunded amounts would then be withdrawn from ATMs.

The exact technical details associated with the flaw are currently unclear.

SILVERFORT
EBOOK
How to Comply with the Cyber Insurance MFA Checklist
Learn More

Trending News

Evasive Meduza Stealer Targets 19 Password Managers and 76 Crypto Wallets

Two Spyware Apps on Google Play with 1.5 Million Users Sending Data to China

Researchers Uncover New Linux

A ISH Tecnologia, empresa nacional de cibersegurança, divulgou um relatório dos ransomwares e vulnerabilidades que mais tiveram sucesso ao atacar empresas no primeiro semestre de 2023. Ao todo, foram detectadas seis vulnerabilidades consideradas de pontuação crítica pelos especialistas, e cerca de 1.480 invasões de ransomware bem-sucedidas em domínios institucionais, sequestrando dados bancários, criptografando informações confidenciais entre outros diversos dados.

"Mesmo com algumas vulnerabilidades e ransomwares tendo sido descobertos em janeiro, fevereiro e março, eles não foram completamente erradicados. Na verdade, seus números apenas crescem, isso porque seus criadores lançam constantes atualizações que vão apenas tornando-os atacantes mais sólidos, com um leque de maneiras de invasão e uma gama de contra-ataque contra serviços de segurança cibernética", disse Caique Barqueta, especialista em Inteligência de Ameaças da ISH Tecnologia.

Confira abaixo as vulnerabilidades e ransomwares que foram ficando cada vez mais potentes no primeiro semestre de 2023:

Vulnerabilidades

EoP (Outlook): é uma exploração de toque zero, o que significa que a falha de segurança requer baixa complexidade para abuso e não requer interação do usuário. O invasor envia uma mensagem para a vítima estendida com um caminho para um Server Message Block controlado pelo invasor remoto. Hospedado no servidor, a vulnerabilidade é explorada pelo invasor tendo a vítima visto a mensagem ou não.

PaperCut NG/MF: essa vulnerabilidade permite que os atacantes remotos ignorem a autenticação nas instalações afetadas do PaperCut. O problema resulta de controle de acesso impróprio. Um invasor pode aproveitar essa vulnerabilidade para ignorar a autenticação e executar um código arbitrário no sistema alvo, ou seja, resultando na infecção dos domínios e podendo haver instalações de diversos códigos que mudem completamente sua configuração.

Apesar de bastante conhecidos no mundo de cibersegurança, o LockBit3 e o BlackCat são constantemente atualizados e tem seus dados e configurações utilizados como modelo na comunidade de invasores

MOVEit: o MOVEit Transfer, aplicativo de transferência de dados e configurações confidenciais de informações empresariais, possui uma vulnerabilidade de injeção de SQL em seu aplicativo web. Dependendo do mecanismo utilizado para o acesso do app, um invasor pode inferir informações sobre a estrutura e o conteúdo do banco de dados e executar instruções para compartilhar, alterar ou até mesmo excluir elementos presentes na conta do MOVEit.

Ransomware

Das invasões de sucesso, dois ransomwares se destacaram: o LockBit3 e o Blackcat (AlphV) foram os dois tipos de cryptolockers que tiveram mais sucesso em invasões institucionais durante o ano.

Malware

Malvertising Used as Entry Vector for BlackCat, Actors Also Leverage SpyBoy Terminator

We found that malicious actors used malvertising to distribute malware via cloned webpages of legitimate organizations. The distribution involved a webpage of the well-known application WinSCP, an open-source Windows application for file transfer. We were able to identify that this activity led to a BlackCat (aka ALPHV) infection, and actors also used SpyBoy, a terminator that tampers with protection provided by agents.

By: Lucas Silva, RonJay Caragay, Arianne Dela Cruz, Gabriel Cardoso
June 30, 2023
Read time: 7 min (1889 words)

Authors

Lucas Silva
Incident Response Analyst

RonJay Caragay
Threats Analyst

Arianne Dela Cruz
Threats Analyst

Gabriel Cardoso

Recently, the Trend Micro incident response team engaged with a targeted organization after having identified highly suspicious activities through the Targeted Attack Detection (TAD) service. In the investigation, malicious actors used malvertising to distribute a piece of malware via cloned webpages of legitimate organizations. In this case, the distribution involved a webpage of the well-known application WinSCP, an open-source Windows application for file transfer.

Advertising platforms like Google Ads enable businesses to display advertisements to target audiences to boost traffic and increase sales. Malware distributors abuse the same functionality in a technique known as malvertising, where chosen keywords are hijacked to display malicious ads that lure unsuspecting search engine users into downloading certain types of malware.

Related Articles

Abusing Web Services Using Automated CAPTCHA-Breaking Services and Residential Proxies

Cerber Version 6 Shows How Far the Ransomware Has Come

Cryptocurrency-Mining Malware: 2018's New Menace?

See all articles ›

Quem somos

Profissionais com mais de 20 anos de experiência em TI com especializações em redes de computadores e segurança cibernética. Atuações em redes de computadores de grandes provedores de internet no Brasil, administração da rede de uma empresa multinacional, atuação como especialista em segurança da informação. Conhecimentos em diversas ferramentas de referência no mercado: Fortigate, Palo Alto, Soho, Dell, Imperva, Guadicore, SonicWall, Cisco

Esta proposta contempla:

Etapa 01:

- Levantamento dos ativos de rede (1 dia)
    - Switches
        - Marca/Modelo
        - Mac Address
        - Portas de uplink
        - Andar/Sala
    - Access Point
        - Nome da Rede
        - Nome do Equipamento na Rede
        - MacAddress
    - Mikrotiks
        - Marca/Modelo
        - Portas de Uplink
        - Vlans

Etapa 02: (2 dias)

- Reset dos equipamentos (controlador, switches, AP´s)
- Reconfiguração do Controlador
- Reconfiguração dos Switches
- Reconfiguração dos AP´s
- Configuração de redundância de links (ITS,OI)
- Sugestões de melhorias do ambiente

Etapa 03:

- Elaboração e entrega da Documentação

Valores

Financeiro:

	Mensal
Execução dos serviços propostos neste orçamento	R$ 5.000,00