RELATÓRIO DE INVESTIGAÇÃO DE AMEAÇAS PARA DISPOSITIVOS MÓVEIS DA CHECK POINT

ATAQUES CIBERNÉTICOS EM DISPOSITIVOS MÓVEIS AFETAM TODOS OS NEGÓCIOS

CHECK POINT
RESEARCH

INTRODUÇÃO

Ao mesmo tempo em que as empresas em todo o mundo adotam cada vez mais programas de mobilidade para aumentar a produtividade e a lucratividade, os ataques cibernéticos continuam a crescer em sofisticação e frequência. Entretanto, hoje cerca de dois terços dos profissionais de segurança duvidam de que suas organizações possam impedir uma violação dos dispositivos dos funcionários, enquanto que 94% esperam que a frequência dos ataques cibernéticos aos dispositivos móveis aumente.1

Este relatório, preparado pela equipe de investigação sobre ameaças para dispositivos móveis da Check Point, é o primeiro a estudar o impacto de ataques móveis em ambientes corporativos, avaliando a telemetria real de ameaças dos dispositivos corporativos e de uso pessoal. Os resultados são nítidos: a mobilidade corporativa está sob ataque constante, afetando todas as regiões e setores industriais, nas duas principais plataformas móveis, Android e iOS. As ameaças aos usuários móveis são inumeráveis e poderosas e, além disso, capazes de comprometer qualquer dispositivo ao acessar dados confidenciais a qualquer momento.

Este relatório revela as principais tendências em malware móvel e outros vetores de ataque, onde eles operam e que segmentos de mercado são os alvos mais frequentes.

OS PRINCIPAIS RESULTADOS DESTA INVESTIGAÇÃO SÃO:

TODA EMPRESA ESTÁ SOB ALGUMA FORMA DE ATAQUE MÓVEL

OS SEGMENTOS MAIS EFETADOS SÃO OS SERVIÇOS FINANCEIROS E PÚBLICOS

A MAIOR PARTE DOS ATAQUES MÓVEIS OCORRE NAS EMPRESAS NAS AMÉRICAS

1 "A Ameaça Crescente de Violações de Segurança de Dispositivos Móveis", Investigação Dimensional, Abril de 2017. https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf

METODOLOGIA

Os dados deste relatório de investigação foram coletados a partir de implantações do Check Point SandBlast Mobile em 850 organizações que garantiram um mínimo de 500 dispositivos de 1º de julho de 2016 a 1º de julho de 2017. Todos os dados foram normalizados para propósitos desta análise.

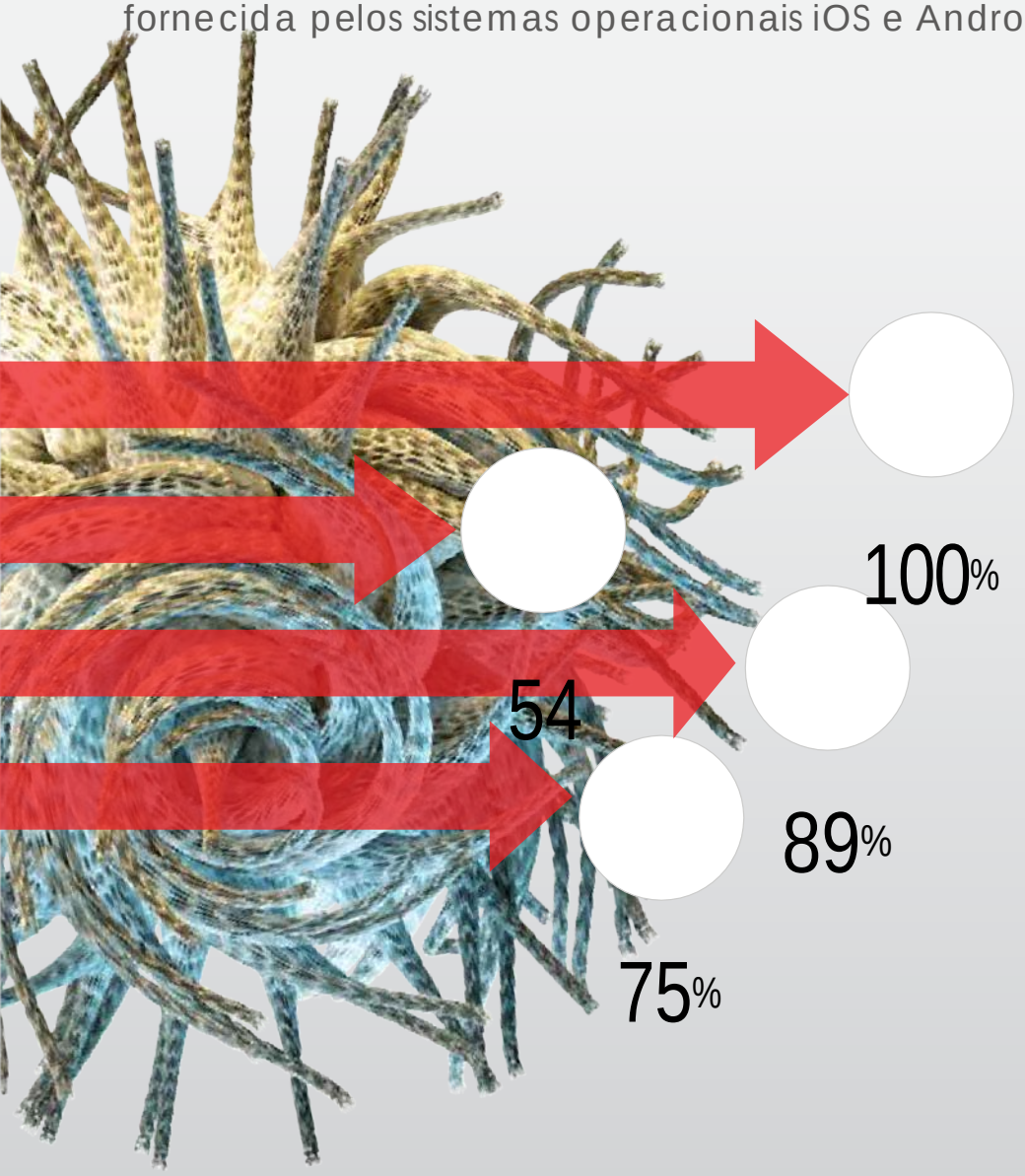
Os resultados deste estudo estão agrupados regionalmente para incluir EMEA (Europa, Oriente Médio e África), APAC (Ásia e Pacífico) e as Américas. Os setores verticais estão agrupados em sete categorias: Serviços Financeiros (bancos, seguradoras e corretoras), Órgãos Públicos, Tecnologia, Manufatura, Telcos, que se referem a operadoras móveis, e Outros, que inclui uma série de segmentos verticais que não são bem representadas na base de clientes do SandBlast Mobile.

TODA EMPRESA JÁ SOFREU UM ATAQUE MÓVEL. ELAS APENAS NÃO SABEM DISSO.

Cada organização em nossa amostra sofreu pelo menos um ataque de malware móvel ao longo do ano passado. Em outras palavras, o número médio de ataques de malware móvel por organização foi de 54.

As organizações sofrem diferentes tipos de ataques móveis além do malware. 89% tiveram pelo menos um ataque man-in-the-middle em uma rede Wi-Fi.

Embora as soluções EMM (gerenciamento de mobilidade empresarial) estivessem efetivas, 75% das organizações em nossa amostra tinham pelo menos um dispositivo iOS desbloqueado ou dispositivo Android roteado conectado em suas redes corporativas. O número médio de dispositivos roteados ou desbloqueados em nossa amostra foi de 35 por empresa. Estes resultados são preocupantes porque o processo de roteamento ou desbloqueio de um dispositivo elimina toda a segurança integrada fornecida pelos sistemas operacionais iOS e Android.



TODA EMPRESA ESTÁ SOB ATAQUE

100% DE TODOS OS NEGÓCIOS SOFRERAM UM ATAQUE DE MALWARE

54 É O NÚMERO MÉDIO DE ATAQUES DE MALWARE MÓVEL POR NEGÓCIO

89% SOFRERAM UM ATAQUE MAN-IN-THE-MIDDLE EM UMA REDE WI-FI

75% NA MÉDIA DE 35 DISPOSITIVOS ROTEADOS OU DESBLOQUEADOS NA REDE

UMA VISÃO SETOR POR SETOR DA AMOSTRA DE PESQUISA

As empresas de tecnologia representam a maior porcentagem (32%) dos dispositivos protegidos em nossa amostra, seguidos pelos serviços financeiros (21%), tais como bancos, corretoras e seguradoras (Gráfico 1). Os fabricantes formam 15% de nossa amostra, com as empresas de telecomunicações (12%), varejistas (7%) e agências públicas (5%) completando a análise.

AMOSTRA DE ESTUDO POR SETOR

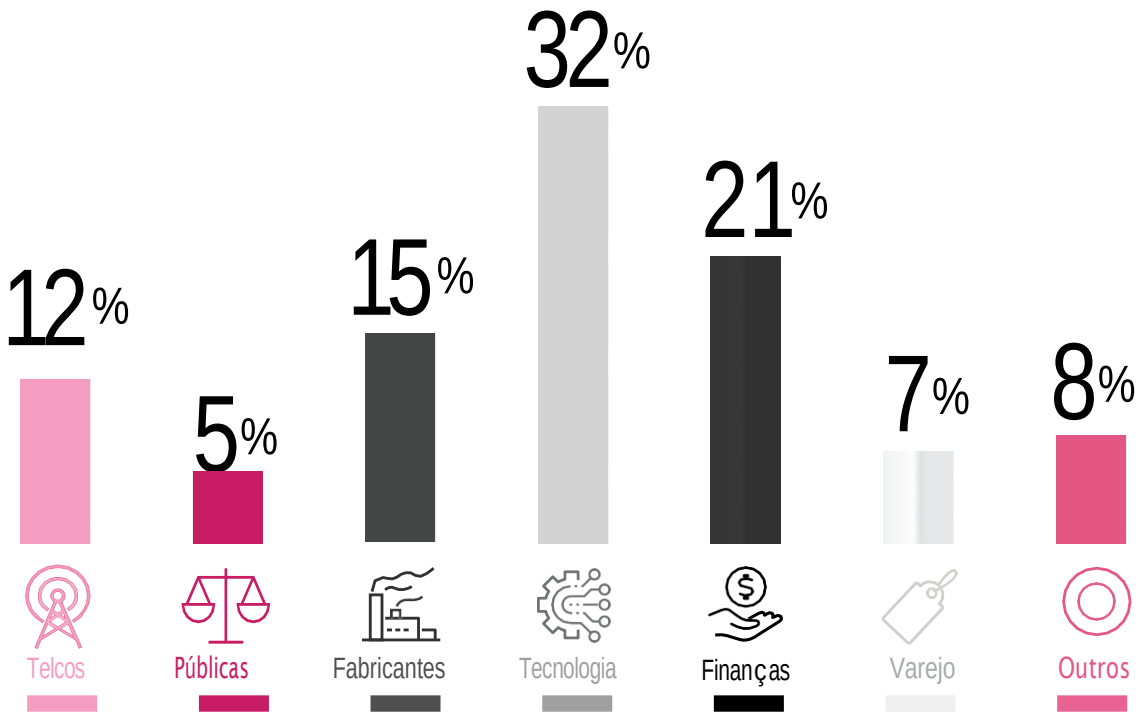


Gráfico 1

O MALWARE MÓVEL ATINGE PRINCIPALMENTE OS SERVIÇOS PÚBLICOS E OS SERVIÇOS FINANCEIROS

Através do Gráfico 2 pode ser visto facilmente que os serviços financeiros (29%) e os serviços públicos (26%) sofreram a maior parte dos ataques de malware móveis, muito além de sua representação proporcional na amostra analisada. Ambos os setores oferecem dados valiosos para os invasores, como um grande repositório de informações financeiras e pessoais. As empresas de tecnologia também foram fortemente impactadas por malware.

ATAQUES DE MALWARE POR SETOR

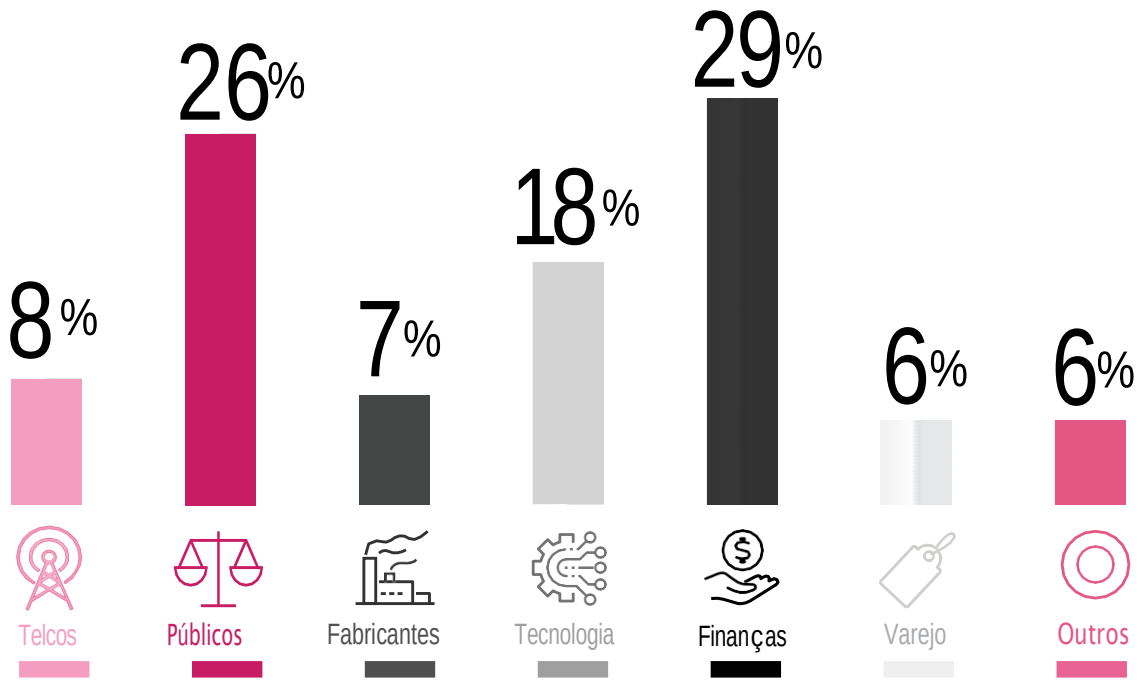


Gráfico 2

OS ATAQUES DE MALWARE VISAM DISPOSITIVOS iOS EM SERVIÇOS FINANCEIROS

O Gráfico 3 mostra a porcentagem de ataques de malware de iOS em diferentes setores. Os serviços financeiros foram o líder máximo, respondendo por 40% de todos os ataques. Os dispositivos de órgãos públicos (20%) também foram fortemente visados, seguidos pelas empresas de tecnologia (9%) e pelos fabricantes (9%). Embora muitas organizações de serviços financeiros exijam que os funcionários usem dispositivos iOS para melhorar a segurança, esses dados revelam que os iPhones e iPads não estão imunes a ataques de malwares.

MALWARE iOS POR SETOR

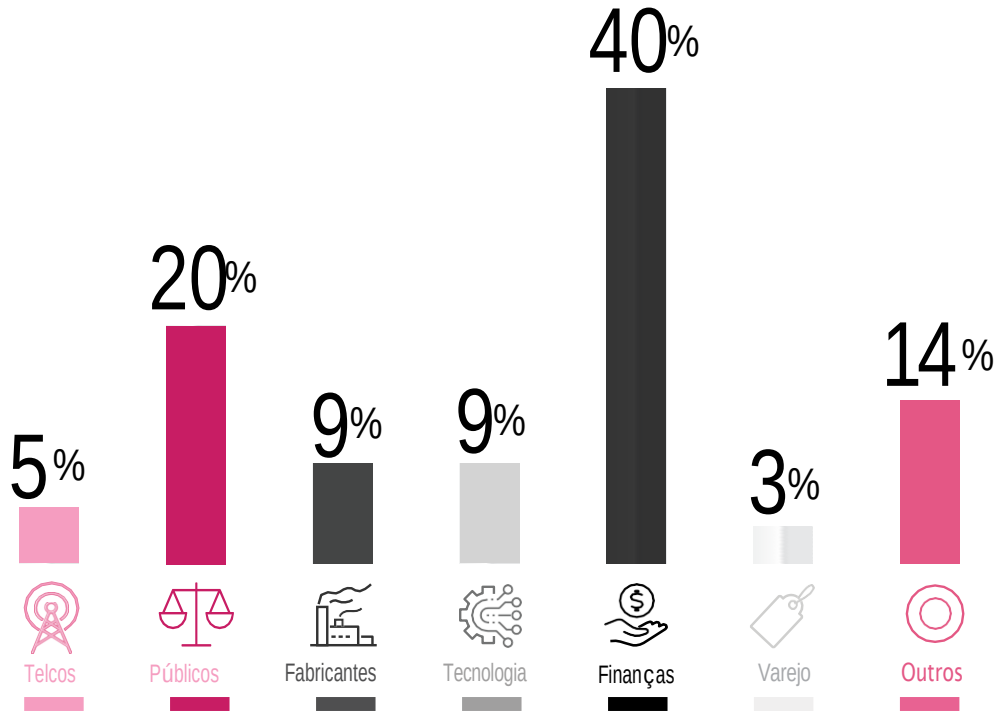


Gráfico 3

OS NEGÓCIOS DOS PRINCIPAIS SEGMENTOS ENFRENTAM UMA GRANDE VARIEDADE DE ATAQUES

O setor de serviços financeiros tem a discutível distinção de sofrer os tipos mais perigosos de malware, como visto no Gráfico 4. Por exemplo, 44% de todos os trojans de acesso remoto móvel (mRATs) foram detectados em dispositivos usados em serviços financeiros.

TIPOS DE MALWARE POR SETOR (%)

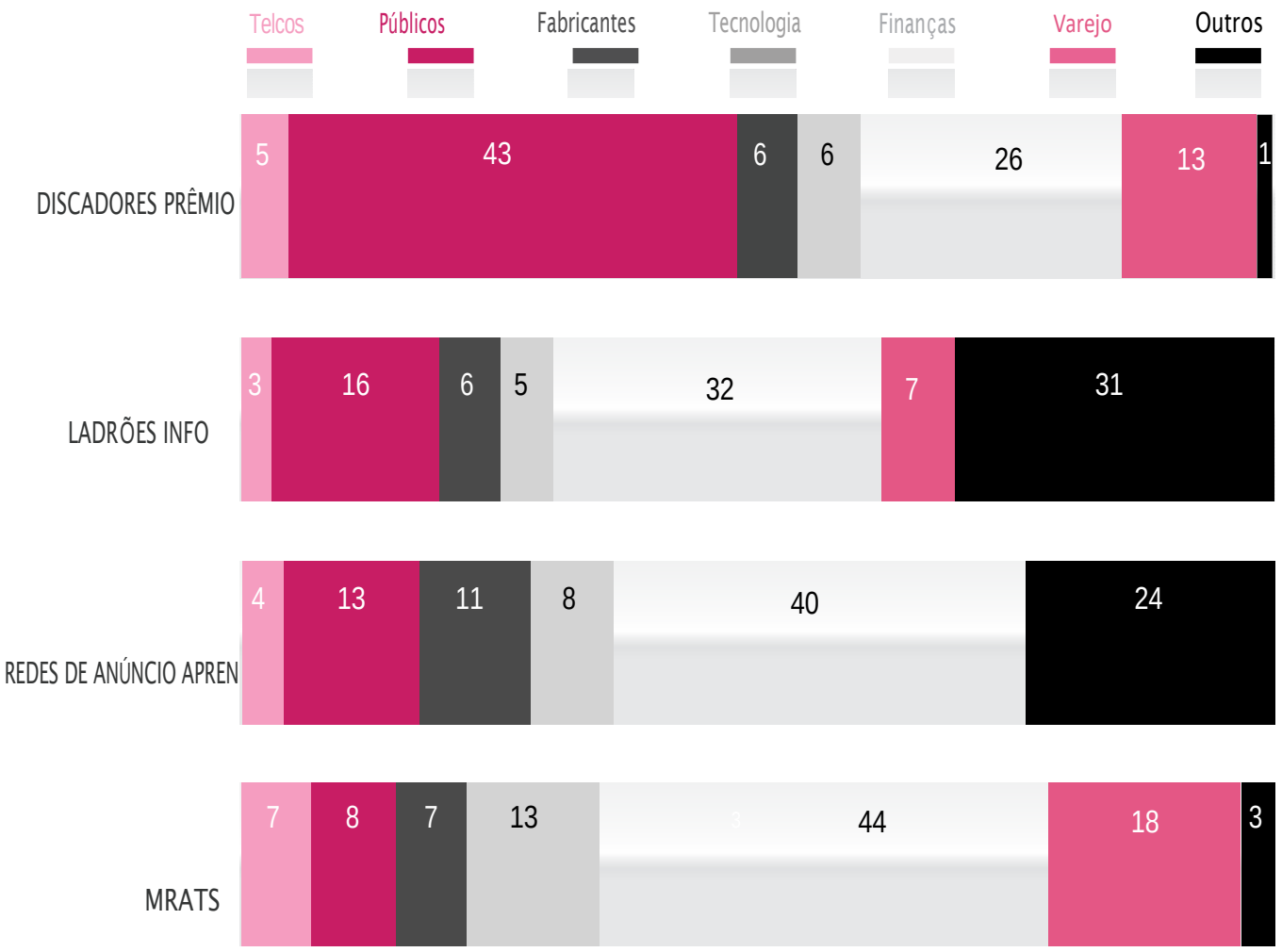


Gráfico 4

empresas. Estas ferramentas permitem que um invasor acesse o dispositivo infectado remotamente e colete informações de todos os sensores disponíveis no dispositivo, tais como sua câmera, microfone, mensagem e diretórios de chamadas, e muito mais. Em um exemplo recente, um mRAT foi localizado no dispositivo móvel do oficial de segurança de um grande banco europeu. Esse malware em particular era uma versão do Ispyoo, baseado em uma estrutura existente que era vendida comercialmente como "proteção parental" sob diferentes nomes, como Copy9, OmegaSpy e muitos mais.

Os funcionários de governo são visados por discadores premium, que abusam das permissões de SMS e chamadas para cobrar do proprietário do dispositivo por chamadas fraudulentas e mensagens de texto para serviços premium. Estes malwares mal-intencionados, tais como o ExpensiveWall, operam silenciosamente e às vezes podem ser encontrados em lojas de aplicativos oficiais.

Claramente, as atividades da maioria das indústrias podem sofrer uma ampla variedade de ataques. Enquanto alguns malwares representam ataques direcionados que são voltados para uma organização específica, outros tentam infectar o maior número possível de dispositivos, comprometendo a segurança de redes inteiras ao longo do caminho.

O SETOR DE SERVIÇOS FINANCEIROS TEM A DISCUTÍVEL DISTINÇÃO DE SOFRER OS TIPOS MAIS PERIGOSOS DE MALWARE

ONDE O MALWARE MÓVEL AFETA A MAIORIA DOS NEGÓCIOS

A amostra do estudo foi formada por empresas do mundo inteiro (Gráfico 5). Quando agrupados por região, 51% das empresas estavam localizadas na EMEA (Europa, Oriente Médio e África), 31% nas Américas e os 18% restantes na região APAC (Ásia e Pacífico).

DIVISÃO REGIONAL DA AMOSTRA

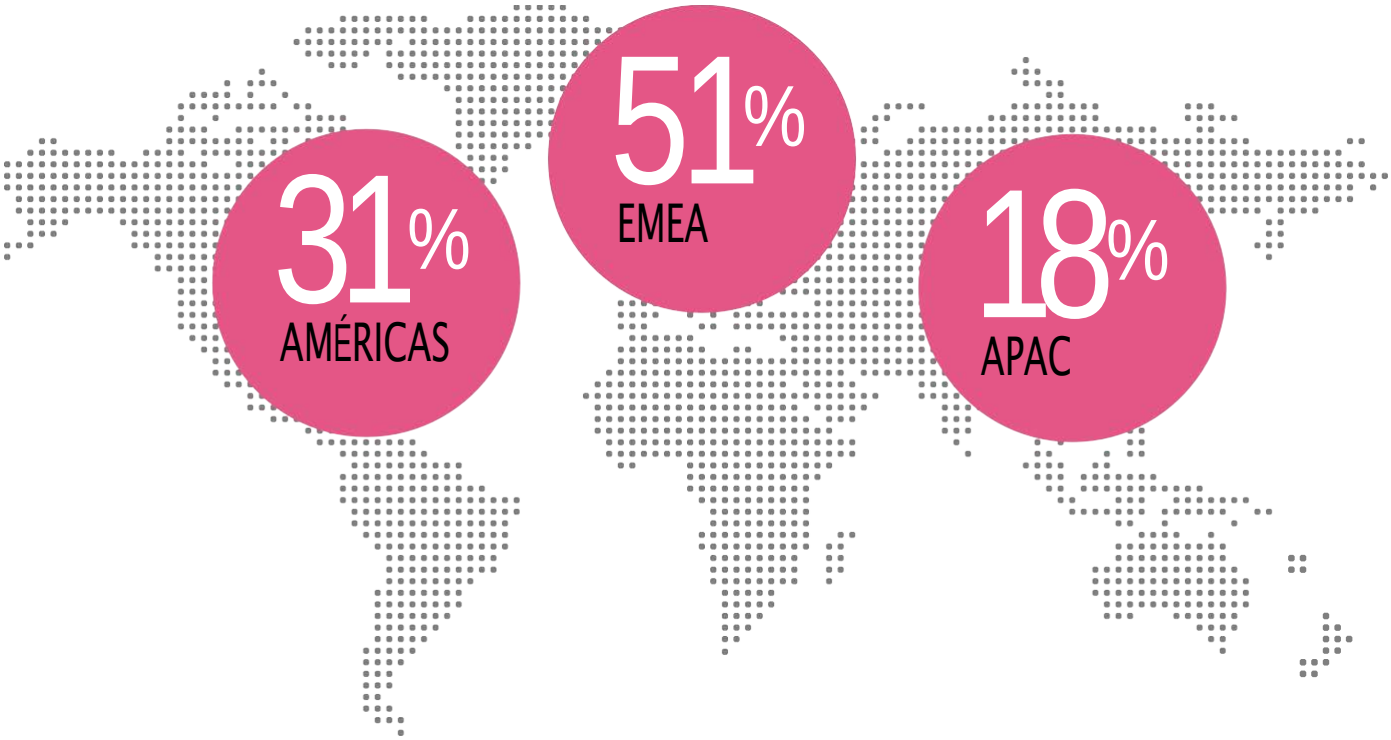


Gráfico 5

Como mostrado no Gráfico 6, as Américas foram a região mais impactada na amostra do estudo, sendo formadas principalmente por empresas nos Estados Unidos. A APAC foi responsável por um terço de todos os ataques móveis, apesar de uma representação menor na amostra. Isso pode ser explicado por várias campanhas de malware de massa que atingiram o sudeste da Ásia durante o ano passado, incluindo o HummingBad e o CopyCat. No entanto, a conclusão é que os negócios em todas as regiões são fortemente afetadas pelo malware móvel, dificultando ignorar essa tendência preocupante.

DISTRIBUIÇÃO DE MALWARE PORREGIÃO

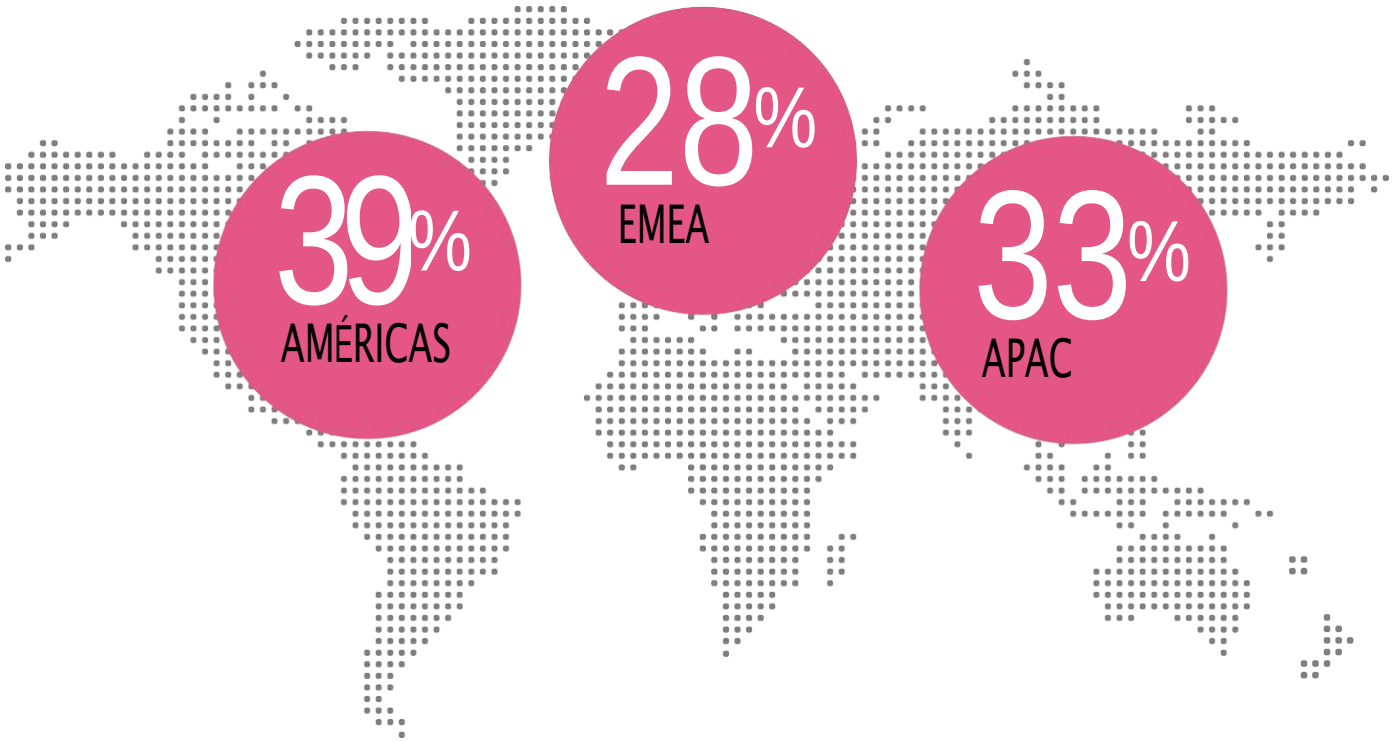


Gráfico 6

PARA ONDE O MALWARE MÓVEL ESTÁ INDO? NÃO ESTÁ NADA BONITO ...

Para os próximos anos podemos apenas esperar que os ataques móveis aumentem em proporção e sofisticação. Para os criminosos, o mundo dos dispositivos móveis possui um grande potencial: eles são mais fáceis de hackear e possuem informações ainda mais confidenciais do que os PCs.

Está previsto que o setor de serviços financeiros continue sendo o principal alvo dos cibercriminosos, seguido por agências governamentais, uma vez que estes dois setores protegem os ativos mais valiosos. As tendências de malware indicam que a distribuição geográfica dos ataques móveis se normalizará e cada região terá um aumento na quantidade de malware. Enquanto o mercado de dispositivos móveis for constituído por dois players dominantes, o iOS e o Android, o malware continuará visando a ambos e tentará penetrar suas defesas.

A segurança móvel abrangente deve ser composta por um sistema de componentes que trabalhem juntos de forma coesa a fim de identificar uma ampla variedade de ameaças e proteger os dados e, ao mesmo tempo, atendendo as preocupações de privacidade dos funcionários. Somente soluções que possam analisar o comportamento em todos os vetores relativos aos indicadores de ataque podem proteger os dispositivos móveis de forma eficaz para mantê-los seguros.

O Check Point SandBlast Mobile é uma infraestrutura de segurança multicamadas que fornece proteção completa. Ele identifica ameaças usando algoritmos no dispositivo, baseados em rede e em nuvem, e dispara respostas automáticas de defesa. Seu mecanismo de risco baseado na nuvem identifica padrões e comportamentos suspeitos ao longo do tempo,

usando aplicativos sandbox em um emulador e detectando ameaças nos níveis de dispositivo, aplicativo e rede. A infraestrutura integra-se aos investimentos de segurança existentes para suportar a resposta a incidentes e fornecer proteção contínua. Como resultado, as organizações sempre terão uma imagem precisa dos tipos de ameaças que os dispositivos em suas redes enfrentam, além de informações detalhadas sobre o que está sendo colocado em prática para mitigar estes riscos.

Em seguida, leia Um Guia da CISO para Defesas Contra Ameaças a Dispositivos Móveis.

Para mais informações: www.checkpoint.com\mobilesecurity

Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT
INFINITY