
eset
53CUR1TY
R3P0RT
AMÉRICA LATINA 2021

ÍNDICE

INTRODUÇÃO

Como todo ano, o Laboratório de Pesquisa da ESET América Latina publica o **ESET Security Report (ESR)**, um relatório que se baseia em pesquisas realizadas com profissionais de tecnologia, para conhecer o panorama da segurança corporativa na região.

A edição 2021 deste documento é o resultado de questionários aplicados a cerca de 1000 executivos e representantes de empresas em 17 países da América Latina durante os eventos digitais do ano passado, mas, além disso, inclui informações obtidas dos dados telemétricos da ESET, dos relatórios trimestrais de ameaças e de outras análises realizadas pela ESET durante a pandemia em nível global e regional.

No cerne da pandemia de Covid-19 e do enorme impacto social que teve, o desafio para a realização deste relatório foi maior, não apenas porque diminuiu a quantidade de eventos nos quais costumamos coletar as respostas dos executivos, mas também por tratar de compreender as preocupações e incidentes dentro de um novo ambiente laboral para as empresas e seus funcionários. Além disso, as empresas e organizações brasileiras também se viram impactadas pela Lei Geral de Proteção de Dados (LGPD), que desde o ano passado, tem deixado em evidência a necessidade de adequar e implementar processos que possam garantir a segurança dos dados de clientes e usuários.

Neste contexto, o relatório está enfocado em conhecer as principais preocupações dos encarregados de tomada de decisões e oferecer proteção aos ativos mais importantes nas empresas, além dos incidentes de segurança mais frequentes nas organizações durante o último ano. Essas informações foram complementadas e sustentadas com dados coletados pela telemetria da ESET.
O conjunto de informações coletadas e o cruzamento de dados obtidos de diferentes fontes oferece um panorama amplo do estado da segurança nas empresas da América Latina, além das práticas de cibersegurança adotadas e adaptadas durante a pandemia.

O documento também apresenta um estudo sobre as principais medidas de segurança que se aplicam para preservar a confidencialidade, integridade e disponibilidade das informações; desde controles tecnológicos e práticas de gestão, até iniciativas de educação e conscientização sobre temas de segurança.

DESCOBERTAS

- Os códigos maliciosos são a principal preocupação (**64%**) e a primeira causa de incidentes de segurança (**34%**) nas empresas da América Latina.

- De acordo com a telemetria da ESET, as empresas no Brasil (**19%**) foram as mais afetadas por malware segundo o total das detecções na América Latina durante 2020, seguidas pelas do México (**17,5%**) e da Argentina (**13,3%**).

- As campanhas massivas de ransomware foram reduzidas em **35%** em 2020, enquanto os ataques direcionados com este malware se tornaram mais agressivos e lucrativos, agregando características como *doxing, print bombing, cold call* e ataques de DDoS.

- O número de ataques de força bruta aos serviços de acesso remoto como RDP cresceu **704%**, enquanto os registros para usuários únicos aumentaram **196%** durante 2020 na América Latina.

- Brasil, México, Chile e Argentina são os países mais afetados por mais de uma dezena de famílias de malwares bancários que iniciaram suas operações na América Latina e estenderam sua propagação aos Estados Unidos e Europa.

- Malwares focados em mineração de criptomoedas aumentaram sua atividade no final de 2020 em concordância com o aumento no valor das criptomoedas. A Tailândia (**17,9%**) foi o país com maior porcentagem de detecções, seguido do Peru (**10,1%**) e Equador (**5,1%**).

- Com base na telemetria da ESET, as empresas no Brasil (**26,4%**) foram as mais afetadas pelos casos de phishing durante 2020, seguidas das empresas no Peru (**22,8%**) e México (**12%**).

- As soluções antimalware são os controles de segurança técnicos mais utilizados, com **86%** das respostas obtidas. A prática de gestão da segurança mais aplicada são as atualizações do software com **71%** de respostas afirmativas.

- Os dispositivos móveis são cada vez mais utilizados para atividades corporativas como videoconferências, acesso a e-mail ou informação, ainda que uma porcentagem muito baixa (**15%**) utilize uma solução antimalware em tais dispositivos.

- Para **76%** dos executivos e responsáveis pela tomada de decisões, o orçamento para a área de segurança se manteve ou foi reduzido com relação aos anos anteriores, e **81%** afirmou que os recursos com os quais contam para segurança são insuficientes.

- Em relação à conscientização e educação em cibersegurança, **78%** dos pesquisados realiza atividades com este fim entre os colaboradores de maneira ocasional ou periódica.

AS EMPRESAS NO BRASIL FORAM AS MAIS AFETADAS POR MALWARE SEGUNDO O TOTAL DAS DETECÇÕES NA AMÉRICA LATINA DURANTE 2020.

CIBERSEGURANÇA EM TEMPOS DE PANDEMIA

O mundo enfrentou grandes desafios frente à pandemia. A crise provocada pelo coronavírus colocou grandes dificuldades e desafios para os governos, para as pessoas e empresas em todos os setores, o que representou novos paradigmas na forma de interagir. O trabalho remoto nas organizações foi apenas uma amostra das mudanças radicais que aconteceram no mundo inteiro.

O novo normal imposto pela Covid-19 também modificou consideravelmente o trabalho dos responsáveis das áreas de segurança, nas quais foi necessário mudar prioridades, identificar necessidades e estabelecer condições. Foram acentuadas tendências observadas antes da pandemia e, por isso, foi necessário considerar, ampliar ou acelerar a transformação digital dos negócios.

O NOVO NORMAL IMPOSTO PELA COVID-19 TAMBÉM MODIFICOU CONSIDERAVELMENTE O TRABALHO DOS RESPONSÁVEIS DAS ÁREAS DE SEGURANÇA, NAS QUAIS FOI NECESSÁRIO MUDAR PRIORIDADES, IDENTIFICAR NECESSIDADES E ESTABELECER CONDIÇÕES.

Em muitos casos, as condições desfavoráveis para adotar o trabalho remoto e plataformas na nuvem atuaram contrariamente aos objetivos, ao que se somaram os orçamentos ajustados devido à baixa na admissão e ao aparecimento de novas leis e regulamentos, como as legislações relacionadas ao trabalho remoto. A pandemia representou novos desafios, oportunidades e, ao mesmo tempo, novos riscos.

Se muito antes da pandemia os ciberataques apresentavam uma tendência a aumentar, isso se manteve com os confinamentos, em particular as campanhas de phishing e malware. A diferença atual reside no fato de que os ambientes são cada vez mais hostis, se considerado que, antes do confinamento, escritório e casa estavam completamente separados, salvo em casos eventuais de trabalho a partir de casa.

Agora a rede da empresa também inclui as redes domésticas, nas quais provavelmente se aplicam práticas deficientes e se utilizam ferramentas de segurança precárias, diferente dos controles de segurança implementados nas redes e sistemas corporativos. As empresas se viram na necessidade de implementar esquemas de trabalho remoto de forma rápida e improvisada, fazendo com que, de um dia para o outro, os dispositivos pessoais dos colaboradores informalmente fizessem parte da rede corporativa, com a disparidade de condições de segurança que isso implica.

Um estudo realizado pela ESET descobriu que **80%** dos representantes das empresas relataram estar mais preocupados com os riscos de segurança relacionados a fatores humanos. Neste mesmo estudo, se destaca também a percepção atual que se tem sobre a cibersegurança, já que **42%** dos entrevistados considerou que o nível de risco do trabalho remoto durante o isolamento social se equipara ao do cibercrime ou dos ciberataques, já que se encontram aparelhados, algo que foi demonstrado durante 2020.

Em um contexto de novas modalidades, no qual a pandemia ainda não terminou e continua gerando mudanças radicais e aceleradas, algumas práticas chegaram para ficar. Por exemplo, **50%** dos entrevistados considera manter no futuro as mudanças implementadas durante a pandemia, como o home office permanente ou as plataformas na nuvem implementadas durante o isolamento social.

A tendência Bring Your Own Device (BYOD), que nunca terminou de ser completamente adotada nas empresas, foi substituída por algo que podemos entender como Bring Home To Work: levar a casa ao trabalho; estas condições mostram a importância da transformação digital e da cibersegurança em qualquer lugar e a qualquer momento.

Além disso, não podemos esquecer que, assim como no ano passado, a Lei Geral de Proteção de Dados (LGPD) ganhou espaço no cenário de segurança no Brasil. Desta vez, em um panorama no qual as empresas tentam se adequar à nova legislação, realizando a revisão de processos e a implementação de novas medidas para garantir o cumprimento da LGPD, principalmente considerando que a partir de agosto de 2021 as multas e sanções previstas pela nova lei passam a ser aplicadas com multas que podem chegar a **R$ 50 milhões**. É importante destacar que os impactos da nova lei podem ir muito mais além do que o pagamento de multas por penalidades, já que o comprometimento de informações pessoais de clientes e usuários pode gerar graves consequências em termos de reputação para os negócios ou instituições.

PREOCUPAÇÕES

As preocupações daqueles responsáveis por tomadas de decisões em matéria de Segurança da Informação estão determinadas por diferentes fatores somados ao ambiente, como a proliferação de ameaças digitais, incidentes de segurança mais frequentes, tendências ou prognósticos relacionados com as tecnologias, ou ainda, condições adversas de situações que também resultam pouco frequentes, como as observadas durante a pandemia.

AS PRINCIPAIS PREOCUPAÇÕES EM MATÉRIA DE SEGURANÇA NAS EMPRESAS LATINO-AMERICANAS SÃO OS CÓDIGOS MALICIOSOS (64%), SEGUIDO PELO ROUBO DE INFORMAÇÕES (60%) E ACESSOS INDEVIDOS AOS SISTEMAS (56%).

A análise de tais preocupações é uma atividade relevante no processo de garantia dos ativos da informação, já que o trabalho de identificação de cenários de risco costuma ser utilizado para definir ou considerar medidas de segurança e proteção para a informação e outros ativos, o que implica no desenvolvimento de iniciativas para resolver problemas atuais ou se antecipar a necessidades futuras.

Como resultado das pesquisas realizadas para o ESR 2021, as principais preocupações em matéria de segurança nas empresas latino-americanas são os códigos maliciosos (**64%**), seguido pelo roubo de informações (**60%**) e acessos indevidos aos sistemas (**56%**).

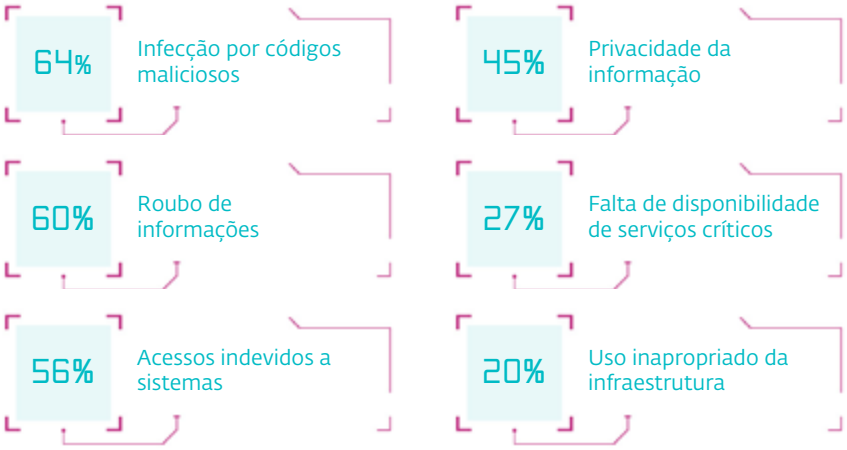

Gráfico 1. *Preocupações em matéria de Segurança da Informação nas empresas da América Latina. Fonte: pesquisa realizada pela ESET com empresas durante 2020.*

O malware se posiciona como a principal causa de preocupação nesta edição do ESR, diferentemente de relatórios passados, em particular no ano anterior, no qual a lista foi encabeçada pelo acesso indevido a informações e sistemas.

Essas mudanças podem se dar em grande parte pela proliferação dos códigos maliciosos que são mais rentáveis para os atacantes e as novas condições de trabalho, que em conjunto definem o ambiente de ameaças digitais dos últimos meses.

> Sequestro de informações: a contínua reinvenção do ransomware

O ransomware merece uma menção especial quando se fala de malware. Este tipo de código malicioso manteve sua atividade e efetividade durante 2020, entre outros motivos, devido às novas condições de trabalho nas organizações e a sua contínua reinvenção. O uso de famílias de ransomware em ataques direcionados foi consolidado durante o ano passado.

Junto à criptografia dos arquivos nos dispositivos comprometidos para exigir um pagamento como resgate pelas informações, somou-se a prática conhecida como *doxing*, isto é, o roubo de informações e posterior extorsão sob ameaça de trazer a público os dados sensíveis extraídos. Em conjunto, ambas ações aumentam a possibilidade de monetizar os ciberataques.

Além disso, agregaram-se novas táticas ao *modus operandi* do ransomware, como o que se denominou *print bombing*, que utiliza as impressoras disponíveis na rede das vítimas para imprimir a exigência do resgate. Outro meio de pressão exercido pelos grupos de cibercriminosos são as "chamadas a frio" ou *cold calls*, para a equipe das organizações afetadas que buscam evitar o pagamento do resgate respaldando sua informação, para intimá-los a pagar através de ameaças e mecanismos de extorsão.

O DOXING FOI CONSOLIDADO EM 2020, COM VÁRIOS GRUPOS DE RANSOMWARE ADOTANDO ESSA ESTRATÉGIA QUE CONSISTE EM ROUBAR INFORMAÇÕES E AMEAÇAR PUBLICÁ-LAS SE O RESGATE NÃO FOR PAGO.

Não bastasse isso, além das medidas utilizadas para exercer pressão sobre as vítimas de ransomware, adicionaram-se ataques DDoS sobre os websites das organizações afetadas, com o propósito de obrigá-las a retomar as negociações.

A operação dos grupos de ransomware pode ser entendida como ameaças persistentes já que, na maioria dos casos, a execução do código malicioso costuma ser uma das últimas etapas dos ataques nas quais as informações e a infraestrutura tecnológica foram previamente comprometidas.

Os grupos de cibercriminosos por trás dos ataques direcionados se tornam mais agressivos, atacando todo tipo de organizações que vão desde hospitais, universidades, órgãos governamentais, bancos até pequenas, médias ou grandes empresas. Ainda que alguns grupos de ransomware tenham prometido não atacar as instituições de saúde durante a pandemia, outros continuam atacando este setor crítico durante a contingência sanitária global.

Nos últimos meses de 2020 e primeiros meses de 2021, foram observados provavelmente os montantes mais elevados vistos até o momento, em relação aos resgates solicitados pelos atacantes, tornando o ransomware um negócio cibercriminoso bastante lucrativo, como é o caso do modelo *Ransomware-as-a-Service* (RaaS), no qual os desenvolvedores do malware obtêm comissões dos grupos que usam suas ferramentas maliciosas.

A tendência à baixa identificada nos ataques de ransomware de difusão massiva pode ser atribuída aos lucros superiores obtidos através dos ataques direcionados, combinados com as táticas já mencionadas. Outra condição pode estar relacionada com o RaaS e o fato de que diversas famílias de ransomware são distribuídas por outros códigos maliciosos em instâncias posteriores.

O anterior também pode ser a razão pela qual apesar das famílias de ransomware como o Maze, Revil/Sodinokibi, DopplePaymer, NetWalker ou Egregor ocuparem destaque nos meios de comunicação na região e em nível global no último ano, não aparecem como as famílias mais detectadas.

De fato, durante 2020, o WannaCry ou WannaCryptor (**56,4%**) com suas características de worm, foi a família com maior porcentagem de detecção na América Latina, seguida do STOP (**12,2%**), Crysis (**7,4%**), Phobos (**4,7%**) e Philadelphia (**1,9%**). Estas detecções estão vinculadas a hashes conhecidos que continuam se propagando em redes com sistemas desatualizados.

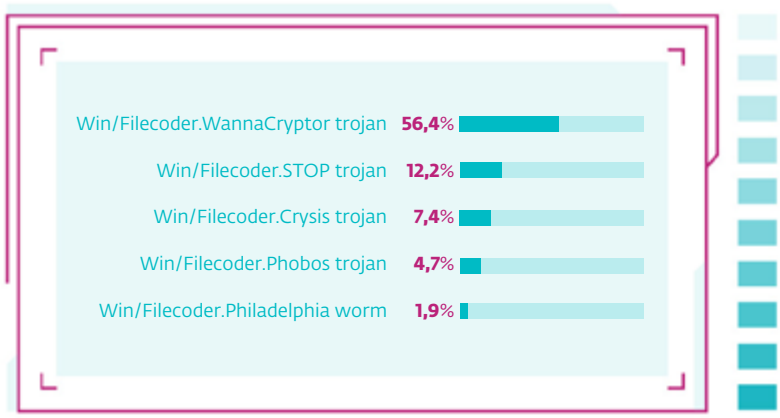

Gráfico 2. *Ransomware mais detectado na América Latina durante 2020. | Fonte: Telemetria da ESET.*

Isso também explica por que se identificam mais famílias de ransomware, enquanto as detecções diminuem. No ano passado foram registradas 1498 famílias e variantes de ransomware, **5,5%** a mais em relação a 2019, enquanto as campanhas de propagação massiva apresentaram uma redução de **35%** nas detecções no quarto trimestre em relação ao primeiro de 2020. As tendências vistas desde 2017 foram acentuadas no último ano.

EM 2020, 1498 FAMÍLIAS E VARIANTES DE RANSOMWARE FORAM REGISTRADAS, O QUE REPRESENTA UM AUMENTO DE 5,5% EM RELAÇÃO A 2019.

Os países com maior quantidade de detecções de ransomware em nível empresas na América Latina durante 2020 foram Peru (**30%**), seguido por México (**14,9%**), Venezuela (**13,2%**), Brasil (**11,3%**) e Colômbia (**7,9%**).

> Aumento na quantidade de ataques a acessos remotos

A pandemia mudou radicalmente a natureza do trabalho diário, obrigando um maior número de sistemas a se conectar à Internet e a aumentar as conexões remotas, às vezes com configurações inseguras, como a exposição pública na Internet. Sem deixar que isso passasse despercebido, os ciberdelinquentes tentaram aproveitar essas condições, que durante 2020 encontraram um alvo importante nos serviços remotos como o Protocolo de Área de Trabalho Remota (RDP).

Além das condições, há diversas motivações que os atacantes encontram para comprometer serviços como o RDP. Por exemplo, os acessos roubados costumam ser comercializados na dark web, para monetizar os ciberataques. Além disso, os sistemas comprometidos são utilizados para executar mais atividades maliciosas como instalar ferramentas adicionais em servidores, baixar e executar programas maliciosos (principalmente ransomware ou mineradores de criptomoedas), ou ain-

da, para extrair informações. Como resultado, os ataques aos serviços de acesso remoto tiveram um aumento importante no ano passado.

DURANTE 2020 FORAM REGISTRADOS 29 BILHÕES DE DETECÇÕES DE ATAQUES A RDP E AO REDOR DE 770 MIL USUÁRIOS ÚNICOS AFETADOS; OS REGISTROS REPRESENTAM UM AUMENTO DE 768% ENTRE O PRIMEIRO E O QUARTO TRIMESTRE DE 2020.

Os dados trazidos pela telemetria da ESET confirmam um aumento importante no número de ataques de força bruta a RDP bloqueados. Em nível global, durante 2020 foram registrados 29 bilhões de detecções de ataques a RDP e ao redor de 770 mil usuários únicos afetados; os registros representam um aumento de **768%** entre o primeiro e o quarto trimestre de 2020 e um aumento de **225%** para os usuários únicos.

No caso da América Latina, se comparado o primeiro trimestre de 2020 com o quarto trimestre desse mesmo ano, esses registros representam um aumento de **704%** no número de detecções dos ataques de força bruta e um aumento de **196%** no mesmo período para o número de usuários únicos afetados por essas tentativas de comprometer os acessos remotos.

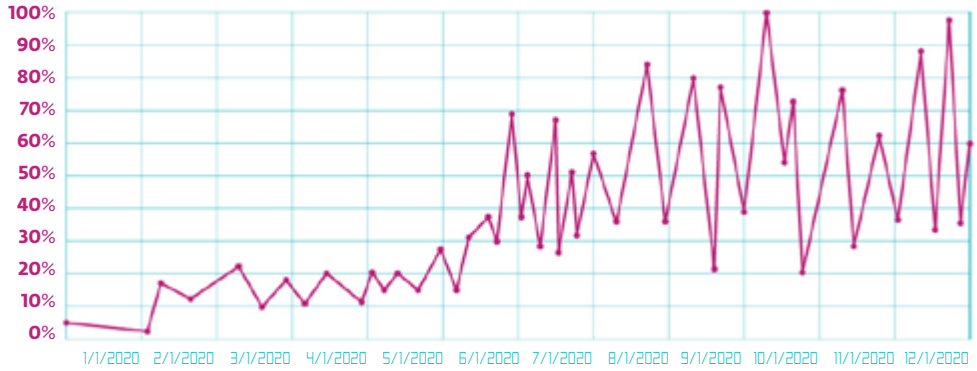

Gráfico 3. *Detecções de ataques de força bruta a RDP na América Latina (2020). | Fonte: Telemetria da ESET.*

De acordo com uma pesquisa realizada pela ESET nos primeiros meses da pandemia, apenas **24%** dos usuários manifestou que a organização para a qual trabalha trouxe as ferramentas de segurança necessárias para trabalhar remotamente e **42%** dos participantes assegurou que seu empregador não estava preparado em relação ao equipamento e conhecimentos de segurança para fazer frente ao trabalho remoto.

Em outra pesquisa realizada pela ESET no final de 2020, **87,6%** dos participantes opinou que os cibercriminosos tinham visto uma oportunidade no aumento do trabalho remoto para lançar ataques direcionados às empresas, especialmente de ransomware, após comprometer os acessos remotos.

> Spyware e backdoors:
ameaças à confidencialidade das informações

Uma preocupação recorrente para os executivos e profissionais responsáveis pela tomada de decisões em matéria de cibersegurança são as ameaças que atentam contra a confidencialidade das informações, que podem desencadear incidentes relacionados com acesso indevido, roubo de informações, impactos na privacidade dos dados, e até uso indevido de infraestruturas tecnológicas.

Neste sentido, as ameaças geralmente utilizadas com esses propósitos estão associadas ao *spyware* (software espião) e *backdoors* (portas traseiras), que, ainda que tenham apresentado tendências a diminuir durante 2020 em nível global, segundo os dados de nossa telemetria na América Latina, vários países apresentam altos níveis de detecção para esses tipos de ameaças.

Durante 2020, os países com a maior quantidade de detecções de *spyware* foram Peru, Israel e Rússia; no caso de *backdoors*, a lista foi encabeçada pela Tailândia, Indonésia e Peru. Ressalta-se que esses códigos maliciosos, junto aos criptomineradores, têm uma importante atividade no território peruano.

DURANTE 2020, OS PAÍSES COM A MAIOR QUANTIDADE DE DETECÇÕES DE SPYWARE FORAM PERU, ISRAEL E RÚSSIA

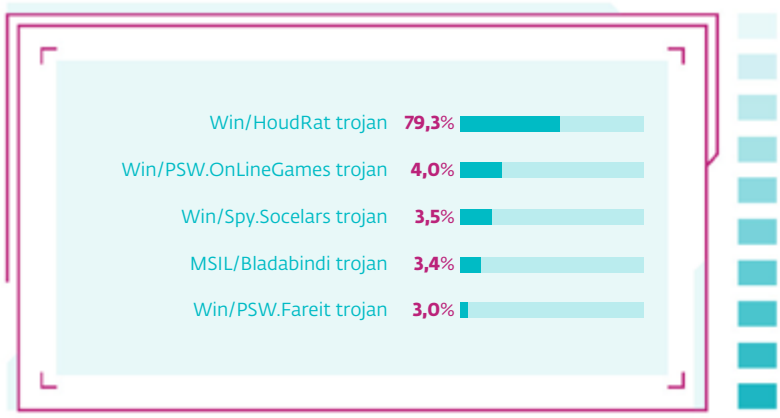

Gráfico 4. *Spyware mais detectado na América Latina (2020). | Fonte: Telemetria da ESET..*

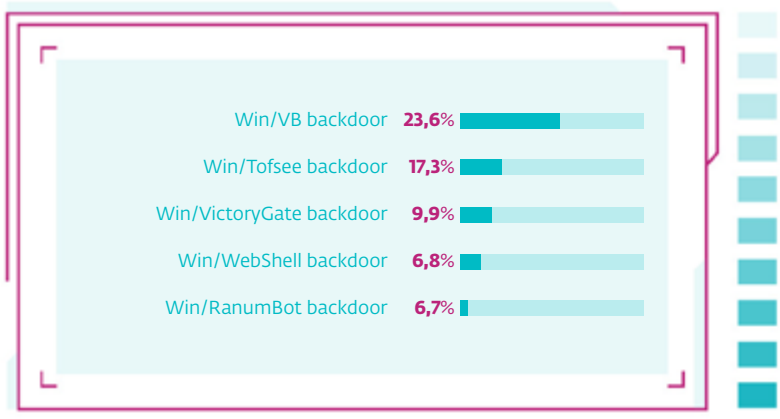

Gráfico 5. *Backdoors mais detectados na América Latina (2020). | Fonte: Telemetria da ESET.*

Vale a pena mencionar que estas categorias de malware são desenvolvidas e identificadas como parte de campanhas de espionagem sofisticadas, além de parte de ataques à cadeia de suprimentos, identificadas pela ESET ao redor do mundo.

> Exploração de vulnerabilidades,
outra via de acessos não autorizados

Além dos ataques de força bruta, a exploração de vulnerabilidades é outra das ameaças relacionadas com as conexões remotas e, em particular, com o protocolo de área de trabalho remoto. Desde o seu surgimento em maio de 2019, o BlueKeep manteve uma atividade importante, que se manteve durante 2020 com uma ligeira queda no último trimestre.

O exploit relacionado com a vulnerabilidade CVE-2019-0708 identificada no Remote Desktop Services, permite a execução remota de código e por isso busca ser aproveitada por atacantes de maneira constante como uma maneira de comprometer os sistemas conectados à internet. Em 2020, o BlueKeep teve uma redução de **8%** na quantidade de detecções para usuários únicos e uma diminuição de **13%** no total de tentativas de exploração.

Do mesmo modo, outro exploit utilizado de forma constante é o EternalBlue (geralmente associado a campanhas maliciosas como a do WannaCryptor), que também apresentou uma queda no número de detecções a usuários finais de **8%**, enquanto as detecções totais se mantiveram praticamente sem mudanças durante 2020.

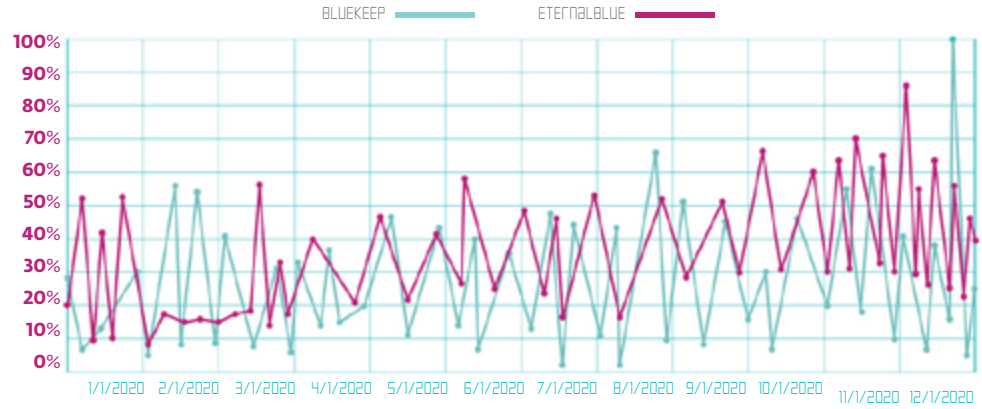

Gráfico 6. *Detecções BlueKeep e EternalBlue na América Latina (2020). | Fonte: Telemetria da ESET.*

Essas tendências à queda tanto do BlueKeep como do EternalBlue poderiam acontecer, entre outros motivos, com dispositivos sem atualização que estão sendo substituídos por hardware e software mais recente. Também pode estar associada às práticas de segurança, já que como detalhado na terceira seção deste relatório, a prática de gestão da segurança mais usada pelas empresas é a atualização de aplicativos.

Provavelmente, as tendências expostas nesta seção do **ESET Security Report 2021** condicionam as preocupações dos tomadores de decisões relacionadas à cibersegurança nas empresas latino-americanas.

> Vazamentos de dados:
desde multas a crises de reputação

Além das preocupações apontadas por nossa pesquisa para o ESR, o vazamento de dados é um tipo de incidente que tem gerado uma enorme preocupação por parte das empresas e instituições, principalmente se tivermos em conta a LGPD. Desde o ano passado, vimos como diversos casos de vazamentos de dados ganharam destaque na imprensa especializada. Além do incidente em si, a repercussão dos casos também se deve ao fato da LGPD ter entrado em vigor em setembro de 2020, o que fez com que a segurança de dados pessoais passasse a ser pauta entre os meios de comunicação, empresas, instituições e usuários em todo o país.

Entre os diversos casos, para citar alguns, podemos destacar o vazamento de informações do Ministério da Saúde com dados de 16 milhões de pacientes com Covid-19; o caso do vazamento de dados da empresa Serasa Experian que supostamente expôs informações de mais de 223 milhões de brasileiros vivos e falecidos. O incidente foi caracterizado como o maior vazamento de dados que já ocorreu no país e os dados expostos estavam sendo vendidos em fóruns na dark web. Além disso, recentemente o Departamento de Proteção e Defesa do Consumidor, do Ministério da Justiça e Segurança Pública, deu 15 dias para que as operadoras de telefonia Claro, Oi, Tim e Vivo dessem explicações sobre o vazamento de dados de mais de 100 milhões de celulares.

Esse tipo de incidente pode afetar as empresas através de sanções e multas aplicadas pela LGPD devido ao não cumprimento de princípios como transparência e segurança que estão envolvidos na gestão de dados exigida pela nova legislação, já que a lei garante a proteção de dados pessoais de clientes por parte de empresas e instituições. O vazamento de dados pode acabar atingindo a reputação de uma companhia e, mais ainda, a confiança que os clientes têm quanto a segurança de seus dados pessoais e privacidade, causando danos irreversíveis para a marca. A gestão e proteção de dados deve ser prioridade para as empresas que estão dispostas a cumprir com a lei, evitando prejuízos irreversíveis para o negócio ou instituição.

INCIDENTES

Os eventos indesejados e inesperados têm una possibilidade significativa de comprometer as operações das organizações e atentar contra a confidencialidade, integridade ou disponibilidade das informações.

Não é de se estranhar que a principal preocupação dos tomadores de decisões esteja relacionada com os códigos maliciosos, quando o malware se posiciona como a primeira causa de incidentes nas empresas latino-americanas.

Os códigos maliciosos (**34%**) ocupam a primeira posição de incidentes de segurança nas empresas da região, seguido de ataques de Engenharia Social (**20%**) e acessos não autorizados (**16%**). Por outro lado, **39%** dos participantes afirma não ter sofrido nenhum tipo de incidente de segurança em suas organizações.

OS CÓDIGOS MALICIOSOS (34%) OCUPAM A PRIMEIRA POSIÇÃO DE INCIDENTES DE SEGURANÇA NAS EMPRESAS DA REGIÃO, SEGUIDO DE ATAQUES DE ENGENHARIA SOCIAL (20%) E ACESSOS NÃO AUTORIZADOS (16%).

Gráfico 7. *Incidentes de Segurança da Informação nas empresas da América Latina.*
Fonte: pesquisas realizada pela ESET com empresas durante 2020.

De acordo com a telemetria da ESET, as empresas no Brasil foram as mais afetadas por malware com **19%** de todas as detecções na América Latina durante 2020, seguidas pelas do México (**17,5%**), Argentina (**13,3%**), Colômbia (**10,6%**) e Peru (**8,9%**).

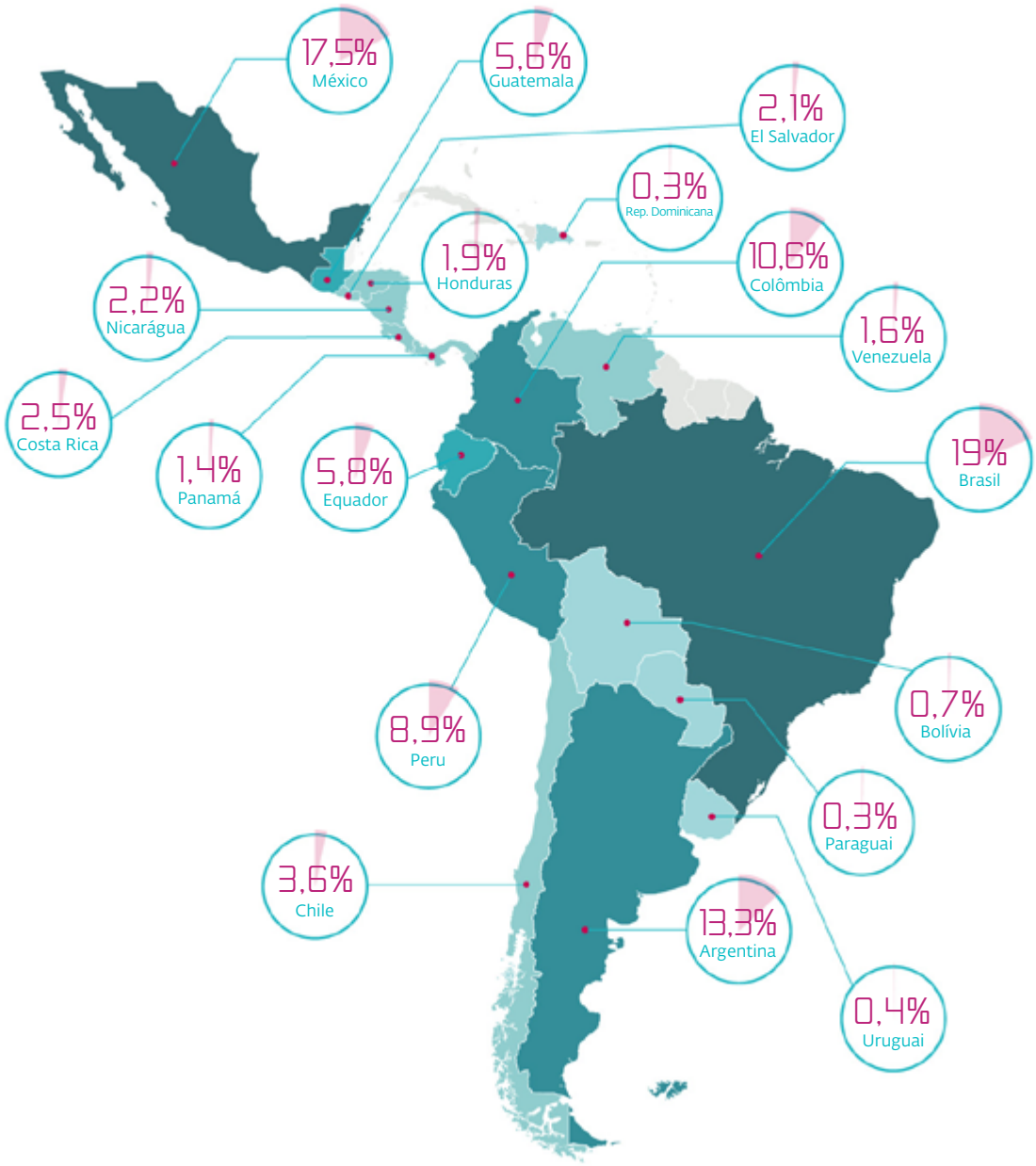

Gráfico 8. *Porcentagem de detecção de malware em empresas da América Latina em 2020. | Fonte: Telemetria da ESET.*

Os códigos maliciosos mantêm a primeira posição como a causa de incidentes nas empresas da América Latina há alguns anos neste relatório. Isso pode explicar por que se trata da principal preocupação e também se pode entender pelas diversas campanhas maliciosas que se identificam continuamente na região.

> Os códigos maliciosos mais detectados na América Latina

As ameaças digitais crescem em quantidade, complexidade e diversidade, condições que com a pandemia aumentaram o risco de sofrer um incidente de segurança devido ao aumento da superfície de ataque, uma maior dependência dos recursos de internet e a transformação digital. Consequentemente, também aumentaram as preocupações.

Em relação à quantidade, os laboratórios da ESET em nível mundial recebem ao redor de 300 mil novas variantes de malware por dia, o que nos traz uma magnitude do problema e do dinamismo dos ciberatacantes. No caso de dispositivos móveis, são identificados em média 300 novas amostras de malware para Android a cada mês.

Do mesmo modo, cada vez se desenvolve malware de maior complexidade com mecanismos que dificultam sua detecção e erradicação, que empregam avançadas técnicas de Engenharia Social e exploração de vulnerabilidades. A sofisticação considera ameaças modulares, capazes de modificar seu comportamento de acordo com as características do sistema alvo, com mecanismos de proteção antianálise para dificultar seu estudo e uma grande diversidade na sua morfologia.

Os grupos de cibercriminosos utilizam técnicas inovadoras na execução e propagação do malware para conseguir ataques cada vez mais certeiros, como o caso do denominado malware *fileless*, que tem a capacidade de executar um código malicioso inteiramente a partir da memória do dispositivo, utilizar ferramentas e processos próprios do sistema operacional para executar a atividade maliciosa, sem criar executáveis adicionais no sistema.

No que se refere à diversidade, as diferentes famílias de códigos maliciosos e suas variantes evoluíram para afetar um conjunto amplo de dispositivos inteligentes e sistemas operacionais.

No contexto da principal preocupação dos encarregados da segurança nas empresas latino-americanas, é conveniente conhecer quais são as principais detecções maliciosas na região. A seguir, foram incluídas as cinco ameaças com maior percentual de detecção na América Latina durante 2020 e uma breve descrição de cada uma delas.

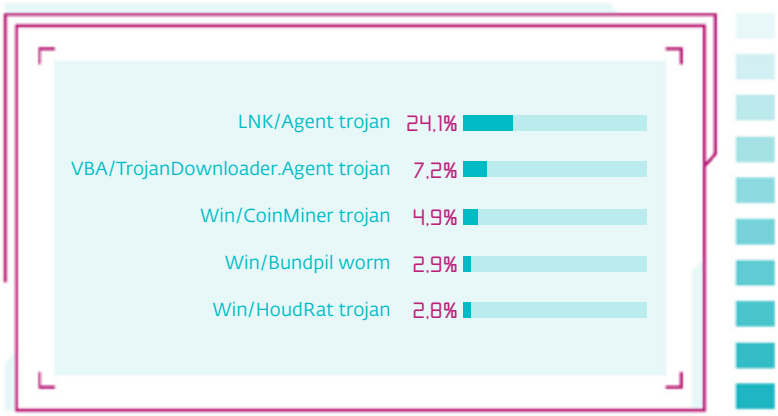

Gráfico 9. *Ameaças mais detectadas na América Latina durante 2020. | Fonte: Telemetria da ESET.*

LNK/Agent trojan

O LNK/Agent é a detecção de um trojan que utiliza arquivos de acesso direto LNK do Windows para executar outros arquivos no sistema; ganharam popularidade já que geralmente são considerados inofensivos. Os arquivos LNK/Agent não contém nenhuma carga útil e geralmente são parte de outro malware mais complexo. Frequentemente são utilizados para conseguir a persistência ou como parte do vetor de comprometimento inicial.

VBA/TrojanDownloader.Agent trojan

O VBA/TrojanDownloader.Agent é um trojan relacionado com arquivos do Microsoft Office que incluem macros maliciosas. Após a execução, a macro baixa e executa malware adicional. Os documentos maliciosos regularmente são enviados como arquivos anexos de e-mail, disfarçados como informações importantes para o destinatário, através do uso de técnicas de Engenharia Social.

Win/CoinMiner trojan

O Win/CoinMiner é um trojan que utiliza os recursos de hardware dos sistemas infectados para a mineração de criptomoedas. Parte de sua atividade maliciosa consiste em manter a persistência, por isso cria uma cópia de si mesmo no dispositivo infectado e cria chaves de registro para se executar em cada início do sistema. Após sua instalação, o trojan elimina rastros e coleta informações do sistema para enviá-las a um dispositivo remoto.

Win/Bundpil worm

O Win32/Bundpil é um worm capaz de se propagar através de meios removíveis. É parte da botnet Wauchos, também conhecida como Gamarue ou Andrómeda. O Bundpil foi projetado para melhorar a persistência da botnet e tornar mais difícil realizar uma eliminação global de sua rede. Devido a isso, utiliza Algoritmos de Geração de Domínios (DGA) para criar nomes de domínio quase de forma aleatória.

Win/HoudRat trojan

O Win/HoudRat é um trojan escrito na linguagem de scripting AutoIt. Funciona como um RAT (Remote Access Trojan) utilizado principalmente para o controle de dispositivos digitais, através da criação de uma porta traseira que permite o acesso remoto aos atacantes. O HoudRat é utilizado para o roubo de informações, em especial dados financeiros dos usuários e se propaga principalmente através de meios removíveis.

> Malware bancário na América Latina e outras regiões

Durante 2020, os malwares bancários afetaram bastante a região latino-americana, principalmente o Brasil, México, Chile e Argentina. A pesquisa realizada pelo Laboratório da ESET permitiu identificar mais de uma dezena de famílias de trojans bancários, entre os quais se encontram Amavaldo, Casbaneiro, Grandoreiro, Guildma, Krachulka, Lokorrito, Numando, Mekotio, Mispadu, Vadokrist e Zumanek.

As campanhas dos bankers são completamente focalizadas, através da suplantação de reconhecidas empresas que operam nos países em questão. Por exemplo, mais de **75%** das detecções de Mekotio foram registradas no Chile e Argentina, enquanto que mais de **85%** dos registros de Amavaldo, Casbaneiro e Mispadu ocorreram no Brasil e México.

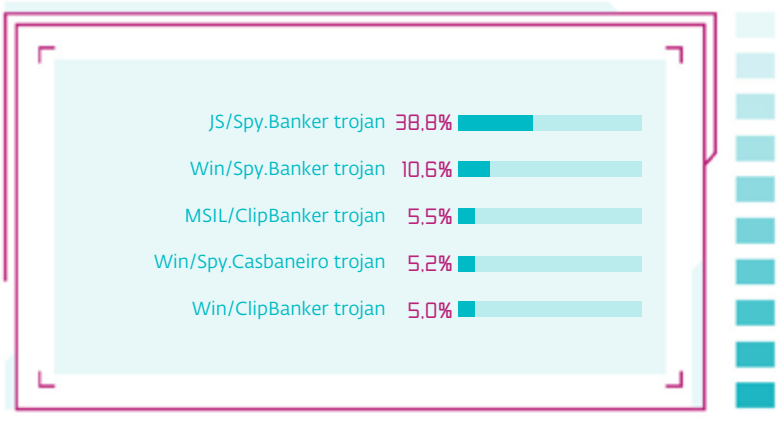

Gráfico 10. *Malware bancário mais detectado na América Latina (2020). | Fonte: Telemetria da ESET.*

Em 2020, os trojans bancários identificados inicialmente na América Latina começaram a ser distribuídos na Europa, afetando principalmente a Espanha, ainda que também foram detectadas campanhas na França, Bélgica, Itália e outros países europeus. Do mesmo modo, os Estados Unidos também se converteram em um alvo para as famílias de malware bancário.

Nos últimos meses foi identificado um decréscimo gradual nas detecções de malware bancário, provavelmente derivado de outro tipo de atividade maliciosa como o ransomware que fornece um maior retorno de investimento a seus desenvolvedores.

Outro motivo nesta tendência para a diminuição, pode se dar pelos trabalhos na interrupção da atividade maliciosa, como é o caso do TrickBot, utilizado por seus operadores principalmente como um trojan bancário para o roubo de credenciais de contas bancárias e recentemente utilizado para realizar ataques mais prejudiciais, como distribuir ransomware.

A ESET proporcionou análise técnica, informação estatística, nomes de domínio e endereços IP de servidores de comando e controle, para interromper a atividade maliciosa do Trickbot. Apenas em 2020, a ESET analisou mais de **125.000** amostras maliciosas e descriptografou mais de **40.000** arquivos de configuração utilizados pelo Trickbot.

NOS ÚLTIMOS MESES FOI IDENTIFICADO UM DECRÉSCIMO GRADUAL NAS DETECÇÕES DE MALWARE BANCÁRIO, PROVAVELMENTE DERIVADO DE OUTRO TIPO DE ATIVIDADE MALICIOSA COMO O RANSOMWARE QUE FORNECE UM MAIOR RETORNO DE INVESTIMENTO A SEUS DESENVOLVEDORES.

> Criptomineradores e a febre pelas criptomoedas

A febre pelas criptomoedas reaparece após uma tendência de baixa no número de detecções de *cryptominers* ou malware criado para a mineração de criptomoedas, que registrava uma queda constante desde 2018, um racha que foi rompido no último trimestre de 2020.

Essa mudança provavelmente aconteceu devido ao aumento no valor do Bitcoin (que passou de **60.000** dólares) e de outras moedas digitais como o Ethereum ou o Monero. Além disso, a taxa de ataques do ransomware direcionado que exige pagamentos em criptomoedas aumentou durante 2020; as vítimas foram obrigadas a adquirir as criptomoedas.

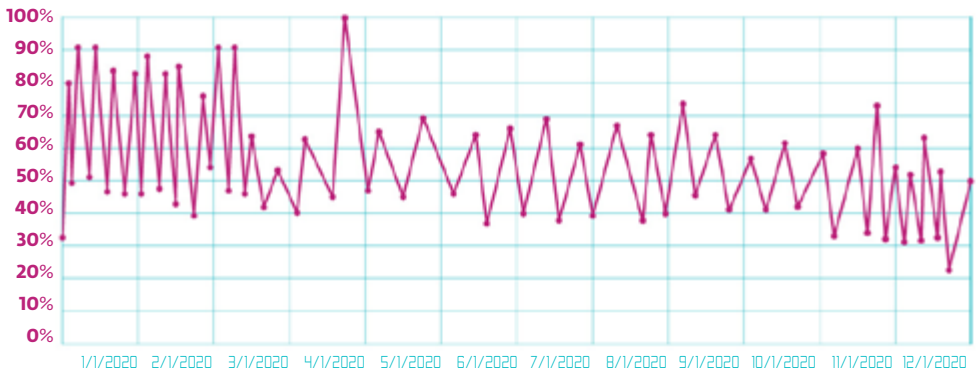

Gráfico 11. *Tendências de detecções de criptomineradores na América Latina (2020). | Fonte: Telemetria da ESET.*

Por estes motivos, não é de estranhar a proliferação das ameaças digitais em torno da mineração de criptomoedas. Em 2020, o país que encabeçou a atividade maliciosa relacionada à criptomineração foi a Tailândia com **17,9%** de todas as detecções, seguido dos países latino-americanos, Peru (**10,1%**) e Equador (**5,1%**).

No ano passado, a ESET interrompeu a atividade da botnet VictoryGate, utilizada para minerar criptomoedas, que afetou principalmente o Peru. A botnet estava formada por cerca de **35.000** dispositivos localizados na América Latina, onde mais de **90%** dos dispositivos comprometidos se localizavam em território peruano.

> Engenharia Social em torno das vacinas e Covid-19

As campanhas de Engenharia Social durante 2020 utilizaram com frequência a pandemia como isca. Diversas campanhas de phishing apareceram para se passar por reconhecidas empresas, nas quais se ofereciam supostos presentes como máscaras ou artigos esportivos, e até instituições governamentais de diversos países foram afetadas pelo uso do seu nome para enganar com aparentes programas de ajuda social, mencionando alguns exemplos.

Nos últimos meses do ano passado e primeiros meses de 2021, as campanhas falsas continuaram fazendo alusão ao coronavírus, mas agora focadas principalmente em golpes relacionados com as vacinas contra a Covid-19, com importante atividade no mundo e em países latino-americanos.

Devido ao trabalho remoto e ao uso de dispositivos, um incidente de segurança que antes teria apenas repercussões pessoais para os colaboradores agora pode implicar em um impacto negativo para as organizações e vice-versa, como resultado da maneira na qual se empregam os computadores, tanto pessoais como corporativos.

Por exemplo, no México apareceram publicações através de redes sociais e falsos websites que tentavam enganar os usuários com a venda de vacinas da Pfizer, Moderna ou AstraZeneca, e também golpes relacionados à venda de tanques de oxigênio nos momentos mais críticos da pandemia.

Na Colômbia, circularam golpes através de mensagens SMS oferecendo turnos prioritários para a aplicação das vacinas em troca de dinheiro; em Honduras circularam mensagens através do WhatsApp nas quais se anunciava a venda da vacina Sputnik V; enquanto na Argentina foram relatados casos de golpes telefônicos direcionados a adultos para ter acesso à vacina. No Brasil, circulou uma campanha de phishing que se fazia passar pelo Ministério da Saúde e prometia realizar o agendamento para o recebimento da vacina contra a Covid-19, mas o real intuito da mensagem era propagar o trojan bancário Mekotio.

O impacto deste tipo de engano é cada vez maior, já que representam um dano patrimonial por não haver garantia de obter a vacina após realizado o pagamento; no remoto caso de que se obtenha o produto, isso implicará em um risco à saúde devido à procedência duvidosa das supostas vacinas.

O caso mais representativo de Engenharia Social é o phishing, uma ameaça geralmente utilizada para o roubo de informações sensíveis. De acordo com os dados da telemetria da ESET, as empresas no Brasil foram as mais afetadas pelos casos de phishing com **26,4%** de todas as detecções na América Latina durante 2020, seguidas pelas do Peru (**22,8%**), México (**12%**), Colômbia (**9,1%**) e Argentina (**7,1%**).

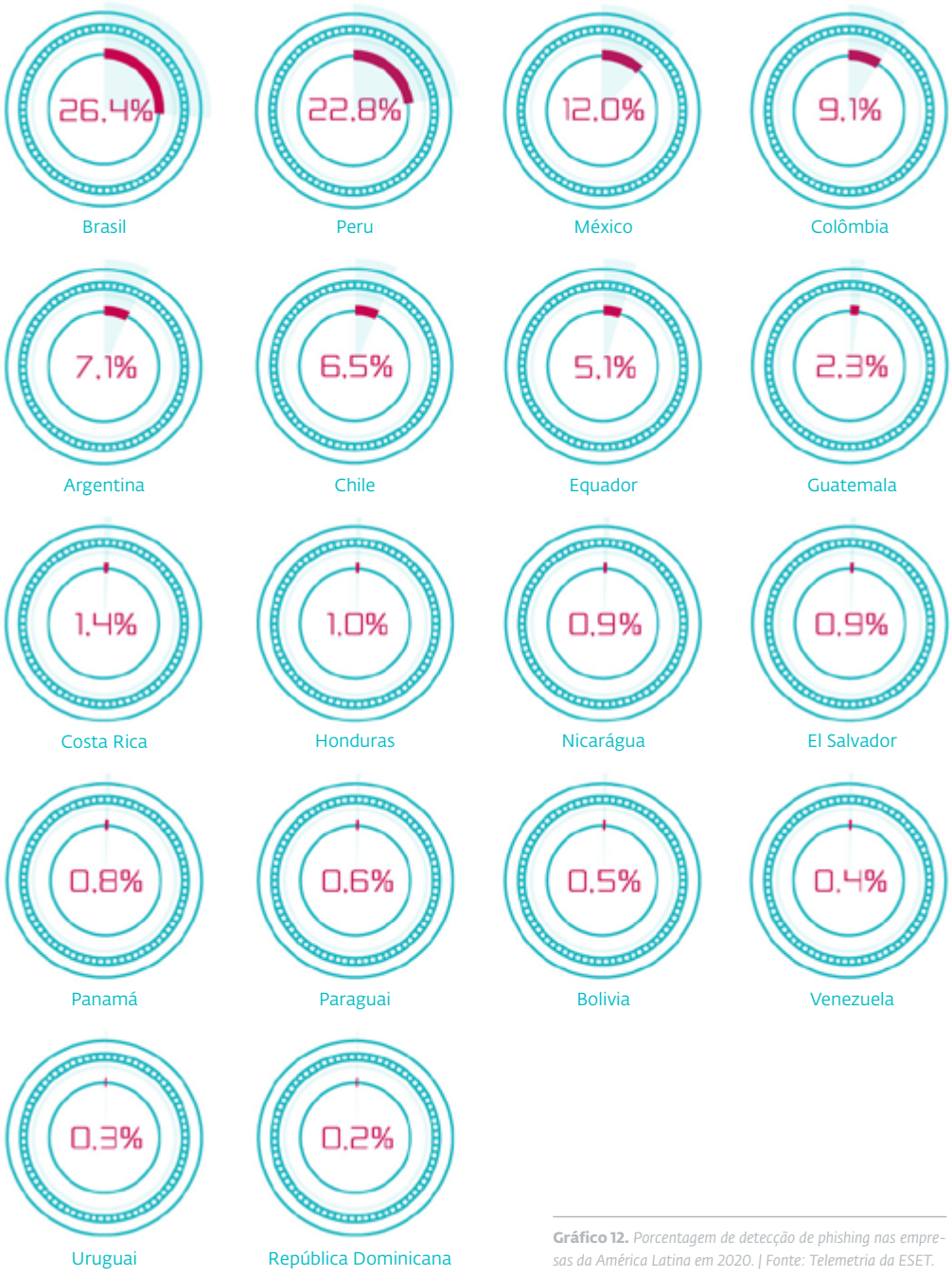

Gráfico 12. *Porcentagem de detecção de phishing nas empresas da América Latina em 2020. | Fonte: Telemetria da ESET.*

Na pesquisa realizada em junho de 2020 sobre cibersegurança em tempos de pandemia com usuários da ESET, **44,2%** afirmou ter recebido e-mails de phishing que utilizavam a Covid-19 como isca para levar o golpe adiante, o que sustenta a quantidade de campanhas de phishing que circulam em volta da pandemia.

NA PESQUISA REALIZADA EM JUNHO DE 2020 SOBRE CIBERSEGURANÇA EM TEMPOS DE PANDEMIA COM USUÁRIOS DA ESET, 44,2% AFIRMOU TER RECEBIDO E-MAILS DE PHISHING QUE UTILIZAVAM A COVID-19 COMO ISCA PARA LEVAR O GOLPE ADIANTE.

CONTROLES

Com frequência os recursos atribuídos para a implementação de controles de segurança e iniciativas orientadas a melhorar e aumentar as medidas de proteção são o resultado das análises relacionadas com as preocupações e incidentes de segurança, que ao mesmo tempo podem estar acompanhadas de avaliações de riscos.

O objetivo dos controles é a mitigação de riscos, seja mediante a redução da probabilidade de ocorrência de risco, ou a diminuição de seu impacto; no melhor dos casos, é possível atuar sobre ambas as variáveis.

> Soluções de segurança tecnológicas na pandemia

Diante desse cenário, tanto os controles tecnológicos, como as práticas de gestão, a educação e conscientização em temas de segurança, têm um papel determinante para alcançar as metas em matéria de Segurança da Informação.

AS SOLUÇÕES ANTIMALWARE (86%), FIREWALLS (75%) E SOLUÇÕES DE SUPORTE DA INFORMAÇÃO (68%).

Com base no resultado das pesquisas, os principais controles de segurança implementados nas empresas são as soluções antimalware (**86%**), firewalls (**75%**) e soluções de suporte da informação (**68%**).

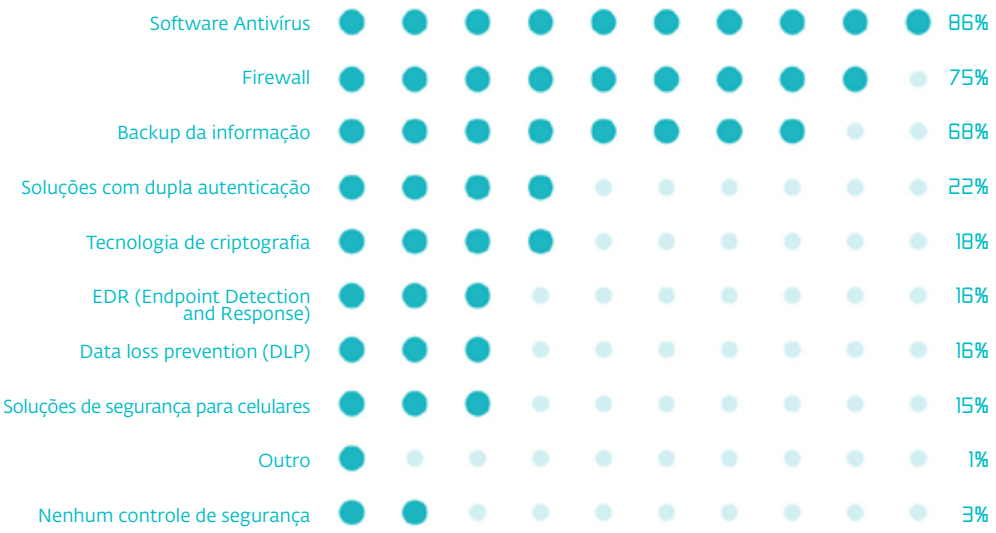

Gráfico 13. *Controles de segurança tecnológicos utilizados nas empresas da região.*
Fonte: questionários aplicados com as empresas pela ESET em 2020.

Parece lógico que o controle tecnológico mais utilizado nas empresas da região sejam as soluções antimalware (**86%**), em condições nas quais os endpoints precisam estar protegidos fora das redes corporativas e em um ambiente no qual o perímetro é praticamente inexistente na atualidade.

Do mesmo modo, parece interessante que os firewalls se mantenham como uma das ferramentas de segurança mais utilizadas na atualidade, provavelmente devido aos modelos tradicionais de segurança que foram mantidos ao longo dos anos e sua contínua evolução, ou até pela aplicação do princípio de proteção trazido por este tipo de ferramentas, que além de se implementar em nível de rede para proteger o perímetro, também são aplicados em nível de host ou Web Application Firewall (WAF).

Por outro lado, a porcentagem de empresas que utilizam uma solução e procedimentos de suporte de informações poderia se considerar relativamente baixo, sobretudo pela quantidade de incidentes de ransomware identificados nos últimos anos ou outras ameaças que atentam contra a disponibilidade ou a integridade das informações. Apesar de manter uma tendência a aumentar nas últimas edições do ESET Security Report: 2019 (**63%**), 2020 (**64%**) e 2021 (**68%**), ainda existe uma brecha importante para reduzir.

No entanto, outras soluções que poderiam contribuir para este controle da informação em um ambiente pouco controlado ou hostil, não são amplamente utilizados. É o caso das tecnologias de criptografia com apenas **18%** de aplicação entre os entrevistados, ou **16%** de soluções DLP. É destacado também a baixa porcentagem das empresas que utilizam controles de segurança nos dispositivos móveis (**15%**), dado que nos dias atuais muitos desses aparatos são utilizados para atividades laborais e se trabalha informação cada vez mais sensível a partir dos smartphones.

APENAS 15% DAS EMPRESAS IMPLEMENTAM CONTROLES DE SEGURANÇA EM DISPOSITIVOS MÓVEIS

No estudo realizado pela ESET sobre cibersegurança em tempos de Covid-19, os dados demonstram também que as soluções antimalware (**32%**) foram as ferramentas de segurança proporcionadas pelas empresas para o trabalho remoto, seguido de conexões VPN (**20%**), soluções de criptografia da informação (**13%**) e soluções de duplo fator de autenticação (**8%**),

> Práticas de gestão de segurança durante o confinamento

Segundo os dados do questionário aplicado pela ESET com empresas da região em 2020, um estudo que tem por objetivo principal a realização deste relatório, a atualização de aplicativos (**71%**) é a prática de gestão da segurança mais adotada, seguida pela implementação de políticas de segurança (**68%**), e pelas auditorias (**40%**), tanto internas como externas.

A ATUALIZAÇÃO DE APLICATIVOS (71%) É A PRÁTICA DE GESTÃO DA SEGURANÇA MAIS ADOTADA, SEGUIDA PELA IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA (68%), E PELAS AUDITORIAS (40%), TANTO INTERNAS COMO EXTERNAS.

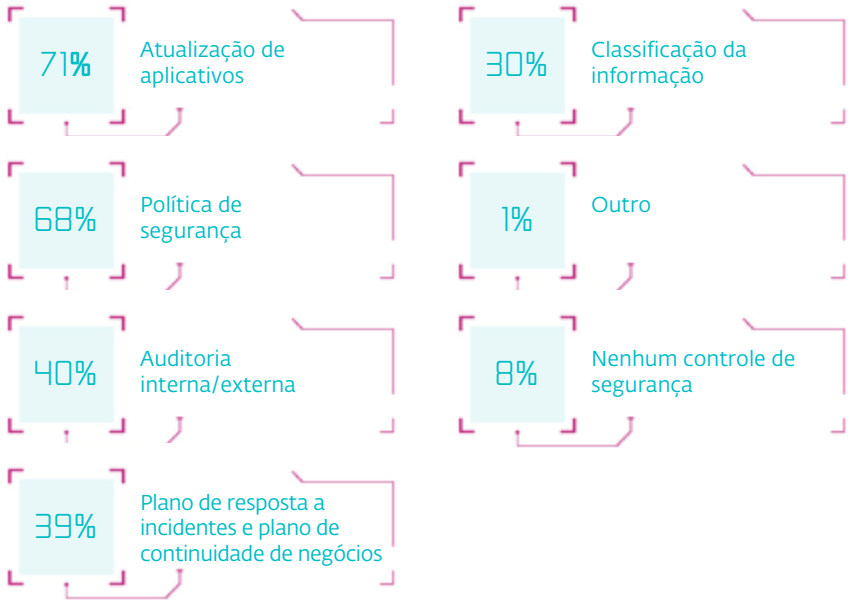

Gráfico 14. *Práticas de gestão aplicadas nas empresas da América Latina.*
Fonte: questionários aplicados pela ESET com empresas em 2020.

Vale a pena mencionar que **8%** dos entrevistados afirmaram não contar com nenhuma prática de segurança implementada. Isso pode ser contraproducente, já que a segurança não se pode limitar apenas aos controles de índole tecnológica, requer a combinação e integração de controles administrativos, físicos e técnicos.

> Investimento em cibersegurança, uma necessidade em curto prazo

De forma paralela à crise sanitária, também se sofre de uma crise econômica como resultado dos confinamentos, o que lamentavelmente aumenta as adversidades para as empresas. Em um ambiente de muitos desafios, o orçamento com o qual contam as organizações é fundamental para atingir seus objetivos, mesmo que às vezes não seja suficiente.

Dos entrevistados para o ESR 2021, **63%** disse conhecer o orçamento atribuído para a área de cibersegurança, contra **37%** que desconhece essa informação. Do grupo de entrevistados que conhecem os recursos que lhe são atribuídos, apenas **19%** considerou que era suficiente; uma baixa porcentagem se levado em consideração o ambiente adverso que as organizações enfrentam em face da pandemia.

Por outro lado, do conjunto de entrevistados que afirmou conhecer os recursos atribuídos à área de segurança, **44,4%** indicou que o orçamento se manteve, **24%** que aumentou, enquanto **22,5%** afirmou que foi reduzido.

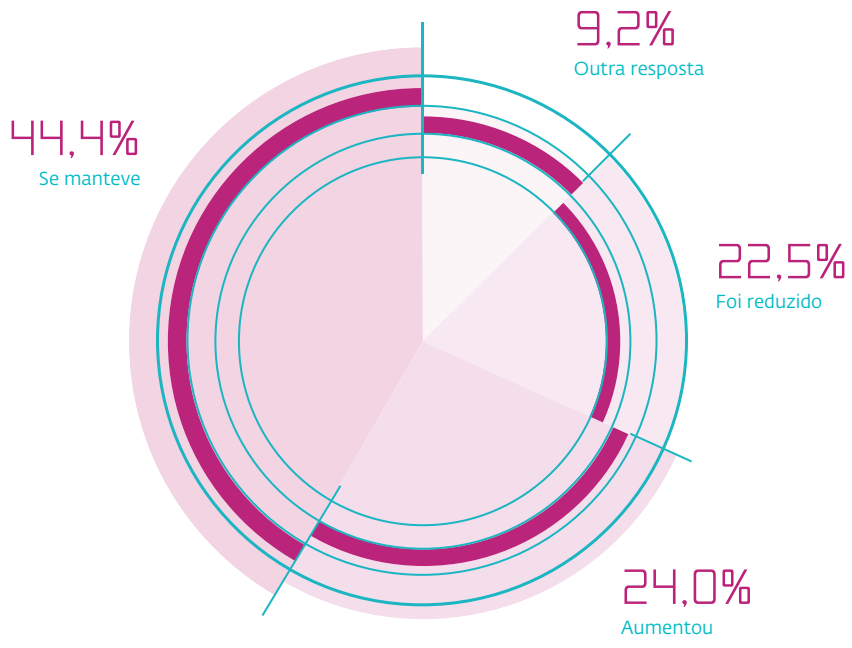

Gráfico 15. *Variação do orçamento de segurança para as empresas.*
Fonte: questionários aplicados pela ESET com empresas em 2020.

Se observarmos a partir de outra perspectiva, para **76%** dos participantes se manteve, foi reduzido ou desconhecem se houve alguma variação no orçamento atribuído para suas tarefas. Do mesmo modo, **81%** dos pesquisados considera insuficiente

os recursos destinados a segurança para cumprir com seus objetivos. Esses resultados são condizentes com outros estudos realizados pela ESET durante a pandemia e que mostra a necessidade de aumentar os orçamentos para as áreas de segurança.

81% DOS PESQUISADOS CONSIDERA INSUFICIENTE OS RECURSOS DESTINADOS A SEGURANÇA PARA CUMPRIR COM SEUS OBJETIVOS.

De acordo com o relatório global Cyberchology, *The Human Element*, um dos principais desafios relatados nas organizações durante o confinamento por Covid-19 está relacionado com o orçamento para a segurança. Na pesquisa realizada para este relatório, **46%** dos participantes manifestaram a necessidade de investimentos em segurança para curto prazo, somado às necessidades que implicam o trabalho remoto.

> Educação e conscientização: fatores-chave para a segurança

Dentre as calamidades que trouxe consigo a pandemia, é possível resgatar alguns aspectos positivos, como a educação e conscientização em matéria de segurança. As iniciativas encaminhadas para este propósito se mantêm.

37% DOS PARTICIPANTES AFIRMARAM REALIZAR ATIVIDADES DE EDUCAÇÃO OU CONSCIENTIZAÇÃO DE FORMA PERIÓDICA, ENQUANTO 41% O FAZ OCASIONALMENTE.

De acordo com as respostas para o ESR 2021, **37%** dos participantes afirmaram realizar atividades de educação ou conscientização de forma periódica, enquanto **41%** o faz ocasionalmente. **19%** não realiza este tipo de ações, o que poderia resultar contraproducente no contexto atual.

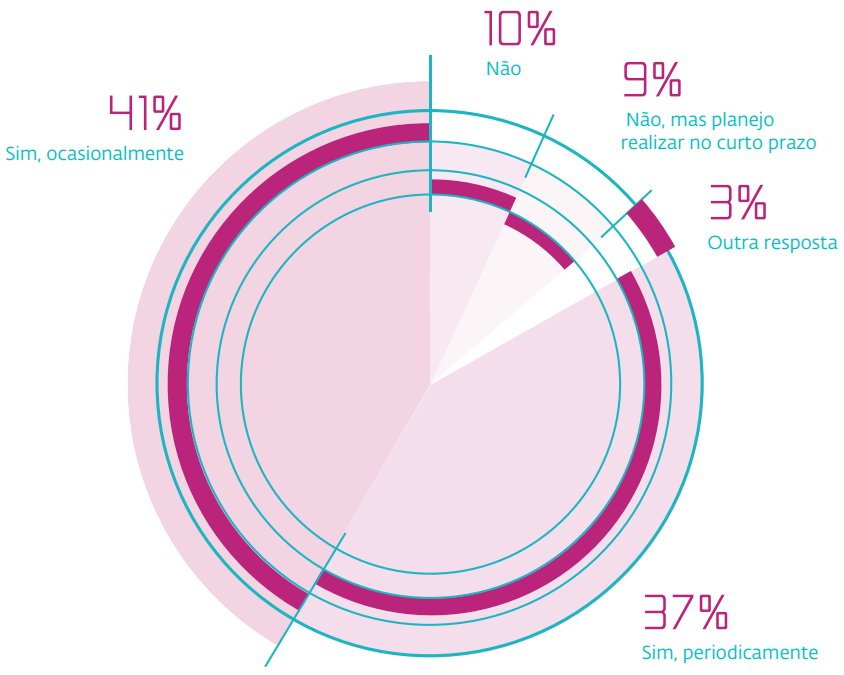

Gráfico 16. *Atividades de conscientização nas empresas latino-americanas.*
Fonte: questionários aplicados pela ESET com empresas em 2020.

A pesquisa realizada pela ESET em 2020 identificou que a grande maioria dos entrevistados (**95%**) considerou útil ou necessária a realização de capacitações de segurança digital especialmente ligadas ao trabalho remoto, o que demonstra a consciência adquirida pelos colaboradores em torno da cibersegurança durante este período.

De fato, a situação de trabalho como resultado da pandemia foi o detonador para mudar a perspectiva sobre a importância de estar capacitado em segurança digital, de acordo com **90%** dos entrevistados em outra análise realizada pela ESET em novembro de 2020 sobre as ameaças de cibersegurança no trabalho remoto. De forma contrária, apenas **20%** afirmou ter recebido capacitações no âmbito laboral sobre configurações seguras e boas práticas de trabalho remoto.

A capacitação e conscientização resultam em elementos chave para reduzir os incidentes de segurança nas organizações. Com frequência, costuma se qualificar aos usuários como "o elo mais fraco" no âmbito da cibersegurança, um adjetivo que poderia ser certeiro se considerada a quantidade de ameaças digitais orientadas a "explorar vulnerabilidades nas pessoas", principalmente mediante o uso da Engenharia Social, no qual o exemplo mais representativo é o phishing.

Usuários bem informados e capacitados, poderão tomar melhores decisões. Isso é chave nesses tempos de trabalho remoto e com a grande quantidade de campanhas maliciosas que, como vimos anteriormente, aproveitam temas relacionados à pandemia.

CONCLUSÕES

A vida mudou radicalmente de um ano para outro, em praticamente todos os aspectos. De forma repentina, as preocupações de diferentes tipos apareceram, principalmente relacionadas com a saúde, o trabalho e a economia. A estas condições, também se juntou o estresse provocado pelos ciberataques. As influências foram de todo tipo e em todos os níveis.

Entre as mudanças que se apresentaram, também se deve mencionar que a pandemia se converteu em um catalizador para executar a transformação digital em quase todas as indústrias, em grande parte com maior dependência da tecnologia para as atividades cotidianas.

Os hábitos pessoais também mudaram. Por exemplo, o uso dos dispositivos eletrônicos aumentou desde o começo do isolamento social, as compras on-line aumentaram consideravelmente e, claro, não se pode deixar de lado as atividades como o trabalho remoto, a educação a distância ou o entretenimento on-line.

Infelizmente, surgiram mais ameaças digitais e outras se consolidaram afetando tanto a usuários como empresas e até governos. Esse é o caso do malware e phishing, utilizado em torno da Covid-19; as notícias falsas que circulam pela internet e aos golpes que quase diariamente encontramos no e-mail, redes sociais ou aplicativos de mensagem.

Por isso, a cibersegurança se tornou uma das considerações mais importantes para qualquer negócio moderno, no qual a maioria das organizações permanecem on-line de algum modo e onde a tecnologia é um elemento chave para suas operações.

As considerações que eram realizadas cotidianamente são mais vigentes e necessárias do que nunca, como manter a segurança e visibilidade nos dispositivos que se encontram fora da rede corporativa, executar a atualização dos sistemas para mitigar as ameaças conhecidas e emergentes, além da conscientização e educação dos colaboradores.

As práticas de gestão da segurança das empresas pouco a pouco começaram a migrar para as atividades cotidianas em seus lares, para proteger a informação. A tênue linha que separava a segurança corporativa da doméstica, pouco a pouco foi se mesclando, deixando como manifesto que a segurança é essencial e que deve nos acompanhar em qualquer lugar e em todo momento.

É importante destacar que, diante de uma infecção, a possibilidade de recuperar a informação e a forma de fazê-lo dependerá do tipo de ameaça específica.

Em geral, nos casos do tipo lockscreen é possível recuperar o acesso ao sistema limpando a infecção ou restaurando o dispositivo. Além disso, nesses casos, se os arquivos não são criptografados, é possível recuperá-los do disco afetado. No entanto, em algumas variantes, especialmente aquelas que afetam dispositivos móveis, o bloqueio não permite a recuperação do dispositivo, por isso, a única solução terminará sendo um reset de fábrica, apagando toda a informação.

No caso dos filecoders a recuperação pode ser mais complicada. Apesar de na maioria dos casos um bom software de segurança ser capaz de remover o ransomware do dispositivo, os arquivos continuarão criptografados. Em algumas famílias de ransomware, especialmente as que utilizam a criptografia simétrica e guardam a chave dentro do código malicioso, é possível recuperar os arquivos utilizando a ferramenta específica de descriptografia. No entanto, os arquivos que foram atacados por um tipo mais sofisticado de ransomware, como o Cryptolocker, são impossíveis de descriptografar sem a chave correta.

Em qualquer caso, se ocorrer uma infecção, é recomendável limpar o dispositivo da infecção, seja utilizando uma ferramenta de segurança ou reinstalando o sistema, e, na sequência, recuperar a informação e os arquivos através de um suporte limpo.

SOBRE A ESET

+ 110 milhões de usuários em todo o mundo	**13** centros de pesquisa e desenvolvimento no mundo
+ 400 mil clientes corporativos	**200** países e territórios

Para mais informações sobre a ESET, visite: www.eset.com/br

Para estar atualizado sobre as principais notícias relacionadas com a segurança da informação, visite: www.welivesecurity.com/br