Progress. Protected.

SECURITY REPORT

< EDIÇÃO BRASIL 2022 >

ÍNDICE

INTRODUÇÃO

Devido aos recentes impactos provocados pela pandemia de Covid-19, o comportamento e a dinâmica de trabalho no mundo corporativo sofreram mudanças estruturais, que exigiram das empresas a capacidade de adaptar-se a uma nova realidade imposta em um mundo cada vez mais virtualizado e remoto.

Neste relatório, baseado em dados obtidos pela **Temetria da ESET**, apresentamos um cenário de segurança marcado pela transformação digital que chegou e trouxe diversos desafios para as empresas em todo o mundo. O conceito de segurança digital dentro das organizações ganhou novos horizontes e se tornou mais complexo do que nunca. Os ataques direcionados e cada vez mais sofisticados estão mais presentes e cabe as empresas darem a devida resposta às necessidades de segurança de seus negócios.

As superfícies de ataques nunca foram tão abrangentes como na atualidade, com usuários remotos mais susceptíveis aos riscos de segurança, com infraestruturas frágeis e que podem facilmente serem transformadas em uma espécie de porta de entrada para que cibercriminosos tenham acesso a informações valiosas de uma organização.

Em meio a tudo isso, no Brasil, nos últimos meses, presenciamos ataques à órgãos do governo, a empresas privadas e a instituições bancárias que nos fazem refletir cada vez mais sobre a necessidade do olhar das empresas para a segurança digital. Além disso, a Lei Geral de Proteção de Dados (LGPD) vem reforçar a responsabilidade das organizações nos processos de coleta e gerenciamento de dados de seus usuários.

PHISHING: UMA VELHA, MAS AINDA ATUAL, FORMA DE ATAQUE

Os phishings são a principal porta de entrada para quaisquer tipos de ambientes, e isso se deve principalmente ao fato de ser muito mais simples enganar uma pessoa dentro de um ambiente alvo, para que realize alguma ação pretendida pelos criminosos, do que burlar eventuais sistemas de defesa que uma empresa possa ter implementado.

OS ATAQUES DE PHISHING AUMENTARAM 226% EM COMPARAÇÃO COM O ÚLTIMO SEMESTRE DE 2021

De acordo com dados de Telemetria da ESET, no primeiro semestre de 2022, detectamos um aumento de 226,10% em comparação com os últimos 6 meses de 2021. Acreditamos que este aumento tão expressivo seja resultado de um conjunto de fatores, por exemplo: o impacto do trabalho híbrido aos ambientes, o uso de dispositivos não seguros fornecidos pelas empresas para que seus funcionários continuem trabalhando, ou pior, funcionários usando dispositivos pessoais para realizar atividades corporativas.

Cenários nos quais o dispositivo usado não está adequadamente protegido costumam trazer uma série de pontos negativos para um ambiente, seja ele puramente corporativo, doméstico ou misto. Os cibercriminosos costumam se adaptar muito rapidamente a essas alterações, como é o caso dos dispositivos menos seguros, e isso costuma refletir diretamente nos TTPs (Táticas, Técnicas e Procedimentos) que utilizam para entrar em um ambiente.

Observando outros dados também obtidos através da Telemetria da ESET, é possível perceber que o conteúdo utilizado em ataques de phishing mudou consideravelmente:

Conteúdos utilizados nos ataques durante o primeiro semestre de 2022:

	2021	2022
Links	79,09%	51,64%
Documentos	20,90%	48,35%

FONTE: TELEMETRIA DA ESET.

A disparidade vista em 2021, em que quase 80% dos phishings eram compostos por links maliciosos, já não existe mais. Na verdade, identificamos que os criminosos estão arquitetando cada vez mais campanhas com arquivos maliciosos diretamente anexados, muitas vezes encurtando o processo de comprometimento do alvo em algumas etapas.

O RANSOMWARE GANHA MAIS UMA VEZ A CENA

Destacando-se como a ameaça que mais trouxe retornos financeiros para os cibercriminosos, o ransomware certamente faz parte das estatísticas ao analisarmos campanhas maliciosas que rondam o Brasil.

Nossa telemetria tem mostrado uma queda significativa nas detecções de ransomware no mundo todo, desde 2016 essa tendência tem se confirmado e não tem sido diferente em 2022, porém, sempre salientamos que essa queda não necessariamente significa uma diminuição na quantidade de ameaças do tipo ransomware. A diminuição se deve principalmente ao fato de a ameaça ser barrada antes mesmo que seja possível identificar que se trata de um ransomware.

Como citamos no tópico anterior, a quantidade de phishings detectados subiu drasticamente, isso é reflexo de uma melhor qualidade de detecção, que identifica comportamentos potencialmente maliciosos antes que possam demonstrar suas características dentro de um sistema.

Mas afinal, se houve uma migração de detecções e o ransomware está sendo barrado em um estágio inicial da sua propagação, por que a ameaça ainda é uma preocupação? Para responder essa pergunta basta ver as notícias sobre ransomware que atualmente permeiam até meios de comunicação que não são focados em tecnologia. Os ataques de ransomware passaram a ser cada vez mais direcionados. E isto pode gerar uma enorme preocupação, já que as empresas não estão devidamente preparadas para enfrentar este tipo de ameaça, que cada vez mais combina engenharia social e uma profissionalização por parte das gangues de ransomware que investigam o perfil do alvo antes mesmo de executar ataques a um alvo em específico. As gangues de ransomware não apenas criptografam as informações obtidas, mas também podem realizar vazamentos de dados.

Isto é uma demonstração muito clara de que o ransomware não diminuiu em nada as suas atividades. Mas, para corroborar com o que é perceptível por todo o mundo, uma análise realizada pela empresa de segurança cibernética **Cybersecurity Ventures** demonstra que essa ameaça traz prejuízos crescentes ao longo do tempo, e que a tendência é que as empresas disponibilizem ainda mais recursos para combater a esse tipo de incidente. Segundo a análise da empresa, os gastos com a ameaça podem chegar a mais de **42 bilhões de dólares** em 2024.

Os incrementos de milhões de dólares nas cifras desprendidas com o ransomware ano após ano nos mostram, principalmente, que os ataques bem sucedidos dessa ameaça serão cada vez mais frequentes e, no caso de ambientes sem a proteção adequada, estes ataques serão ainda mais efetivos.

Agora que entendemos que devemos continuar nos preocupando com o ransomware por um bom tempo, é interessante saber quais famílias de ransomware são as mais atuantes no Brasil, para assim podermos ter uma ideia de direcionamento de esforços para a proteção contra este tipo de ameaça. Dando continuidade a análise dos dados fornecidos por nossa telemetria, é possível observar que as principais famílias atuantes no Brasil são focadas no **sistema operacional Windows**. E isto se deve principalmente ao fato deste sistema operacional ser o mais utilizado em todo o mundo, mas vale salientar que todos os sistemas operacionais possuem suas versões para essa ameaça. Confira as famílias mais detectadas pelas soluções ESET durante o primeiro semestre de 2022:

> Crysis: esta família ganhou destaque na imprensa nacional e internacional após a divulgação de chaves-mestras, ferramenta capaz de remover a criptografia dos arquivos sem o pagamento de um resgate, serem publicadas em fóruns na Internet. Esta família é muito famosa e existem diversas variantes desta ameaça sendo detectada por todo o Brasil e em outros países da América Latina.

> **STOP:** esta família pode ser distribuída de diversas formas: das mais tradicionais, como utilizando um downloader preparado por criminosos, à exploração de vulnerabilidades em serviços muito usados como o RDP (Remote Desktop Protocol), por exemplo.

> WannaCryptor: uma variante do famoso ransomware WannaCry, com características de worm que se propagou amplamente ao se aproveitar da vulnerabilidade descoberta no protocolo SMBv1 (EternalBlue) para fazer vítimas em todo o mundo em meados de 2017.

É importante salientar que as variantes de um determinado tipo de ransomware costumam se aproveitar das mesmas vulnerabilidades exploradas no ransomware original, o que indica que, mesmo usufruindo de uma falha antiga, o ransomware pode ainda estar fazendo vítimas atualmente.

TROJANS: O "PRESENTE DE GREGO" AINDA EXISTE

A mudança de comportamento observada nas empresas é reflexo de uma necessidade imposta pelo cenário que temos vivido durante a pandemia. Como muitas empresas não estavam preparadas, sem planos de continuidade de negócios devidamente elaborados e testados, foi possível perceber uma grande adopção de serviços em nuvem, sejam estes disponibilizados pela própria empresa ou contratados de forma terceirizada, visando permitir que os funcionários continuassem exercendo suas respectivas funções remotamente, assim como foi determinado pelos países durante a crise sanitária.

APESAR DOS TROJANS TEREM CAÍDO PARA A TERCEIRA POSIÇÃO EM NÚMERO DE DETECÇÕES NO BRASIL, OS ESFORÇOS PARA CONTER A AMEAÇA NÃO DEVEM SER DEIXADOS DE LADO

Os trojans se posicionaram ao longo dos anos como uma das ameaças mais direcionadas a nossa região, fazendo com que o Brasil liderasse a lista de detecções por muito tempo. Essas ameaças possuem diversas subdivisões, quase como especializações dentro de um mesmo tipo. Dentre as subdivisões mais atuantes em nosso território estão os **RATs (Remote Access Trojans)**, que foca em ser uma ameaça silenciosa com capacidades de controlar e monitorar todo o dispositivo infectado; e os **trojans bancários**, que visam atacar vítimas enquanto elas realizam transações com os bancos escolhidos como alvo pelos cibercriminosos.

Diferente de anos anteriores, nossa telemetria apontou alterações de foco por parte dos cibercriminosos, fazendo com que o Brasil não esteja mais no topo da lista de detecções. Atualmente o país com o maior número de incidentes desse tipo de ameaça é o **México**, com **10.6%** de todas as detecções do mundo, seguido pela **Turquia (8,6%)** e o **Brasil (7,5%)**. Mesmo caindo para a terceira posição em número de detecções, vale reforçar que são detecções globais e que é interessante que a terceira posição não nos impeça de direcionar esforços para conter a ameaça.

É importante frisar que, diferente de outras ameaças como o ransomware, os trojans não querem ser vistos, pois quanto maior for o tempo de permanência da ameaça dentro de um sistema, mais chances os criminosos terão de alterar características do sistema ou realizar vazamentos de dados.

O ANDROID CONTINUA NA MIRA DOS CIBERCRIMINOSOS

Interpretando as mudanças perceptíveis ao longo dos anos, mesmo antes de levarmos em conta a pandemia, é razoável inferir que dispositivos móveis são pontos de atenção quando se trata de segurança de dados. E esta atenção é igualmente importante quando pensamos em ambientes corporativos ou domésticos, visto que boa parte das empresas permite que seus funcionários usem dispositivos pessoais para realizar atividades do âmbito empresarial. Se observarmos as funções acumuladas por smartphones ao longo do tempo, é possível perceber que estes dispositivos ganham cada vez mais importância no que se refere ao acesso à informações.

O que iniciou com um simples recebimento de token de acesso via SMS, se transformou rapidamente em uma ferramenta de entrada a diversos tipos de sistemas e aplicativos internos de uma empresa; não raramente incluindo acesso a e-mails, servidores de compartilhamento de arquivos e acesso remoto aos sistemas. As facilidades trazidas por esses dispositivos deveriam gerar um olhar de segurança, o que infelizmente não observamos com tanta frequência.

COM 28,7%, O BRASIL É O PAÍS DA AMÉRICA LATINA COM MAIS DETECÇÕES DE MALWARES PARA ANDROID

Talvez a pergunta "Por que o foco dos criminosos está direcionado ao Android?" surja, e ela é muito simples de ser respondida: cibercriminosos sempre focam em mercados no quais possam fazer cada vez mais vítimas. Se observarmos os números da StatCounter referentes a utilização de sistemas operacionais para dispositivos móveis, percebemos que os **dispositivos Android detêm de forma consistente mais de 71% do mercado**. Apesar do Android estar na mira do criminosos, assim como acontece com os sistemas operacionais para computadores, os atacantes também desenvolvem malwares para outras plataformas, como o iOS, por exemplo.

Países afetados por malwares para Android

Brasil	28.7%
México	27.3%
Peru	8.9%
Argentina	7.9%
Colômbia	6.1%

FONTE: TELEMETRIA DA ESET (1º SEMESTRE DE 2022).

Tendo em vista a informação dada por nossa telemetria que mostra que o país da América Latina mais afetado por ameaças focadas no Android é o Brasil, com **28,7%** das detecções, também é interessante saber quais tipos de ameaça podem afetar os dispositivos móveis.

Normalmente, todos os tipos de ameaça passíveis de afetarem um sistema operacional Windows, por exemplo, podem afetar também um sistema operacional Android - basta que sejam realizadas as modificações necessárias para que a abordagem seja feita a um sistema operacional diferente.

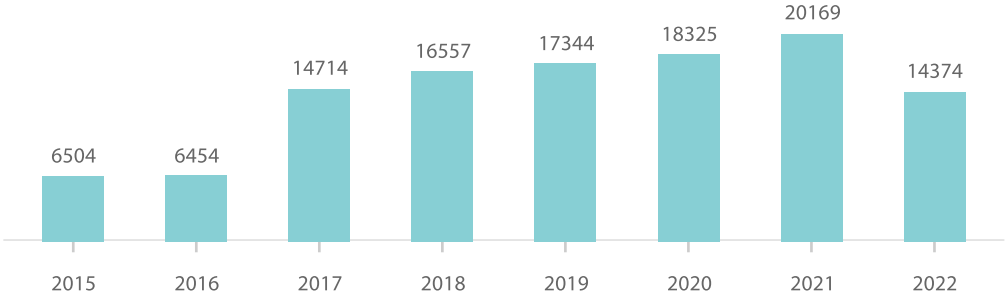
Ainda assim, algumas ameaças são mais utilizadas do que outras por trazerem mais benefícios aos criminosos, são elas: os **ransomwares**, os **trojans bancários** e os **RATs**. Elas guardam características que os criminosos consideram valiosas, já que são capazes de extrair ou comprometer determinados tipos de informações frequentemente contidas nos dispositivos móveis.

VULNERABILIDADES: A SOLUÇÃO É ATUALIZAR!

Vulnerabilidades são apresentadas normalmente quando determinado software se comporta de forma diferente do que é esperado quando recebe algum tipo de interação específica. Este comportamento anômalo costuma desencadear uma alteração interna na estrutura de um software e pode ou não permitir um comportamento malicioso baseado neste tipo de interação.

Observando gráficos, como os disponibilizados pela CVE Details, percebemos que as vulnerabilidades estão em uma tendência de alta e, ao que tudo indica, isso não mudará por um bom tempo - vulnerabilidades são associadas a novos softwares ou dispositivos e a quantidade de softwares e dispositivos ofertados para o público em geral não para de aumentar.

Vulnerabilidades ao longo do tempo



Fonte: CVE Details.

Mesmo sem levarmos em consideração as vulnerabilidades que não foram reportadas e que são vendidas em sites e fóruns na Deep/Dark Web, a quantidade de falhas existentes é de extrema significância. Por estar diretamente associada a forma como um determinado software se comporta, a correção de uma vulnerabilidade normalmente é disponibilizada pelo próprio fabricante do software afetado. Além disso, também é interessante que o fornecedor mantenha seu produto livre de falhas, e este é um dos pontos preocupantes no Brasil.

Boa parte das empresas não se preocupa com o monitoramento do ciclo de vida dos softwares e não gere adequadamente suas respectivas atualizações, fazendo com que o ambiente esteja repleto de diversos tipos de softwares que podem se tornar alvos em potencial.

Separamos as vulnerabilidades mais presentes no âmbito corporativo, de acordo com os nossos dados de detecção durante o primeiro semestre de 2022:

> **CVE-2012-0143:** a vulnerabilidade com mais detecções no Brasil está vinculada ao pacote office - Windows na versão 2003 e Mac na versão 2008. Ela permite que os criminosos possam executar comandos remotamente (RCE) e assumir o controle do dispositivo comprometido.

> **CVE-2010-2568:** afeta diversas versões do sistema operacional Windows, dentre elas, o Windows 7, o Windows Server 2003 e o Windows Server 2008. Similar a primeira colocada, também é extremamente crítica e permite a execução de comandos remotamente (RCE). Esta vulnerabilidade foi utilizada na campanha de propagação de um dos worms mais conhecidos do mundo em 2010, o Stuxnet.

> **CVE-2017-11882:** em terceiro lugar, temos outra vulnerabilidade crítica que afeta a várias versões do pacote office para Windows, incluindo o Office 2010, 2013 e 2016. Também permite a execução remota de comandos (RCE).

Como mostrado no gráfico, existem diversas outras vulnerabilidades que podem ser exploradas, muitas delas foram amplamente noticiadas em um passado recente tamanha a sua criticidade, como por exemplo o Bluekeep, focado em comprometer servidores RDP; o Log4Shell que se aproveita de uma vulnerabilidade em uma biblioteca do Java; e a vulnerabilidade Follina, que explora uma ferramenta de diagnóstico presente no pacote Office.

Existe outro ponto em comum entre as vulnerabilidades mais detectadas por nossas soluções além do fato de serem vulnerabilidades relacionadas a produtos Microsoft, todas elas são falhas descobertas há mais de cinco anos atrás. Isto indica, dentre muitas outras coisas, que é um hábito comum entre as empresas não atualizar seus softwares já há muito tempo, sendo que a vulnerabilidade mais antiga que citamos

data de 2010 e os cibercriminosos ainda hoje continuam se aproveitando dela para adentrar em ambientes.

Para fazer com que um ambiente esteja o mais seguro possível, é necessário direcionar esforços também para atualização e manutenção de softwares já existentes e, sempre que possível, mantê-los monitorados por profissionais qualificados.

MANTENDO O AMBIENTE SEGURO

Apresentamos uma série de características e ameaças diretamente vinculados ao Brasil - todas elas detendo possibilidades de atacar todo e qualquer tipo de estrutura. E por isso achamos pertinente trazermos também o que pode aumentar o nível de segurança de um ambiente para fazer frente a essas ameaças. O aumento de campanhas de phishing nos dá fortes indícios de que proteger adequadamente servidores de e-mail, sejam eles internos da estrutura da empresa ou serviços contratados, é fundamental para mitigar tentativas de acesso por este meio. Tendo em vista que este tipo de abordagem contém principalmente URLs ou arquivos maliciosos, é interessante se certificar que todo e qualquer host na rede, sendo ele uma estação de trabalho ou dispositivo móvel, tenha, minimamente, uma proteção de endpoint presente nele e, sempre que possível, adicionar camadas de proteção para que ameaças totalmente desconhecidas, com camadas de ofuscação robustas e/ou extremamente direcionadas, também possam ser impedidas.

Adequar as permissões de todos os usuários da rede para que tenham sempre o mínimo privilégio possível a fim de que consigam exercer suas funções sem problemas. Este tipo de adequação, conhecida como Least Privilege, é um dos alicerces que auxilia o ambiente a chegar em um modelo Zero Trust, que tem como prioridade validar acessos a usuários e dispositivos para que tudo aquilo que não esteja condizente com a suas métricas não consiga realizar nenhum tipo de atividade dentro do ambiente.
Para que seja possível caminhar nessa direção, também é necessário gerir adequadamente tudo o que está presente dentro do ambiente: desde a versão do software utilizado para criar arquivos compactados até o update do sistema operacional do principal servidor que o negócio possui. Todos eles precisam ser adequadamente mantidos e, sempre que não forem mais necessários, removidos de todo o ambiente. Esta medida também faz com que as empresas tenham uma visibilidade muito maior para garantir a proteção do ambiente.

E não podemos esquece de um aspecto fundamental neste processo de segurança: a educação e conscientização dos colaboradores de uma empresa. O investimento na educação dos colaboradores em segurança cibernética pode prover a autonomia

adequada para que cada indivíduo seja um agente proativo à serviço da segurança, e não o elo mais fraco da corrente.

Cuidar de todo o aspecto tecnológico é de suma importância, mas também ressaltamos que existem tipos de ataque nos quais não é possível se obter métricas, abordagens feitas diretamente aos usuários que muitas vezes nem passam por crivos de soluções de proteção tecnológicas e que ainda assim podem trazer sérios problemas de segurança para o ambiente. Para suprir esse ponto, que solução de proteção alguma consegue alcançar, é necessário conscientizar os usuários do ambiente e torná-los também uma valiosa medida de proteção contra ameaças.

CONCLUSÕES

Este novo cenário, que é resultado de uma série de adaptações e mudanças provocadas pelo mundo pós-pandêmico, também trouxe à tona outro problema: as soluções de proteção e os investimentos adotados pelas empresas permanecem gerações atrás de ataques cada vez mais sofisticados, complexos e multivetoriais.

É, sem dúvida, cada vez mais necessário que as empresas possam investir em orçamentos mais direcionados à segurança digital, na implementação de medidas que cumpram com as determinações exigidas pela LGPD na proteção de dados, na definição de medidas preventivas e na criação de mecanismos de mitigação de ataques.

A segurança digital deve ser uma estratégia de negócio. Os casos de vazamentos de dados, por exemplo, não são mais uma notícia incomum e ser vítima de um incidente pode colocar em risco todo o planejamento de uma empresa, arruinar sua reputação e causar grandes perdas econômicas.

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, acesse: www.eset.com/br

Para estar atualizado sobre as principais notícias relacionadas ao mundo da segurança digital, acesse: www.welivesecurity.com/br