BlackBerry | Cybersecurity

RESUMO EXECUTIVO

RELATÓRIO GLOBAL DE INTELIGÊNCIA DE AMEAÇAS

MARÇO DE 2024

Período do relatório: setembro a dezembro de 2023

O *Relatório Global de Inteligência de Ameaças da BlackBerry®* mais recente foi publicado e registra um período movimentado para os agentes de ameaças. Esta edição do relatório da BlackBerry abrange quatro meses, de 1º de setembro a 31 de dezembro de 2023, em vez do período habitual de três meses. No entanto, os resultados foram ajustados para comparações por dia e por minuto.

Neste período de relatório, as soluções de segurança cibernética da BlackBerry®bloquearam mais de **5,2 milhões de ataques cibernéticos** no total. Considerando os dados por minuto, os ataques aumentaram de 26 por minuto no período anterior para **31 por minuto** neste período, um **aumento de 19%** nos ataques cibernéticos por minuto em comparação com o relatório anterior.

Em termos de novas amostras de malware, uma média de cerca de **5.300 amostras *únicas* por dia** tiveram clientes da BlackBerry como alvo. Um **aumento de 27%** em relação ao período de relatório anterior.

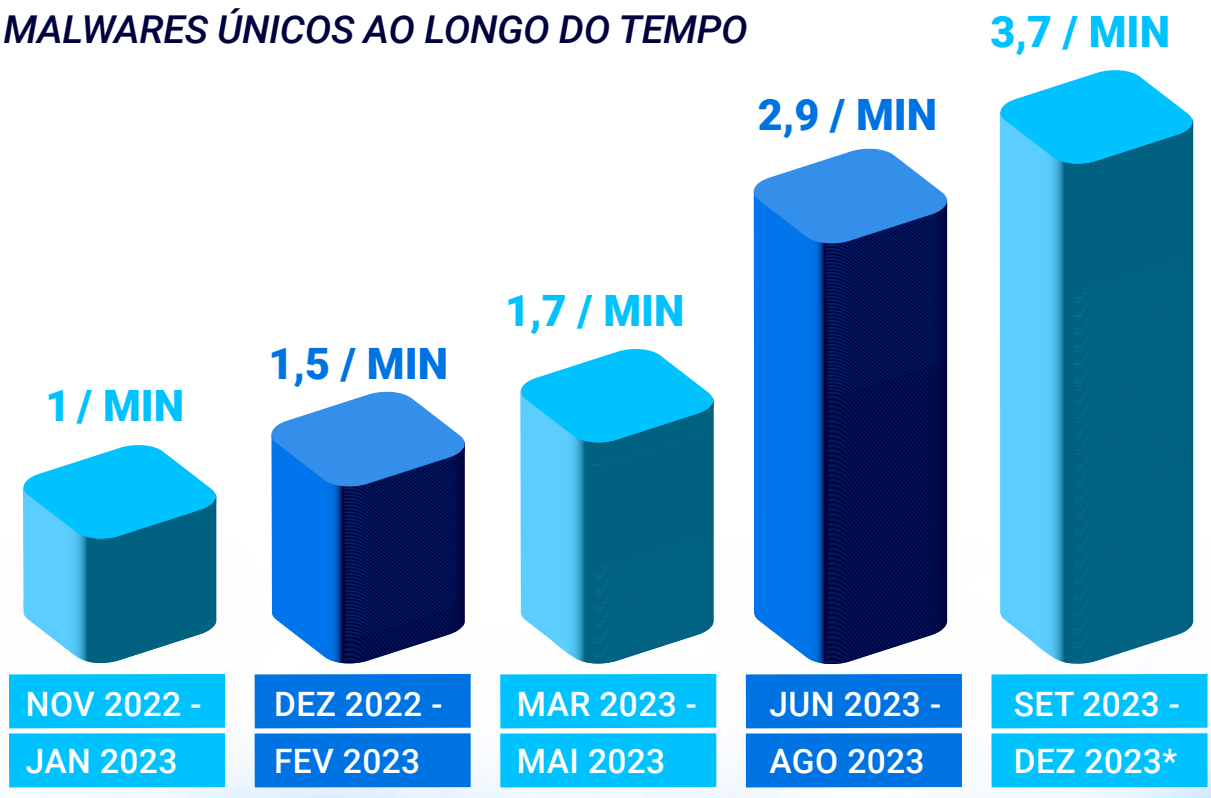

Figura 1: Amostras de malware únicas por minuto ao longo do tempo.

As **infraestruturas críticas** atraíram o maior volume de ataques cibernéticos neste período de relatório, como indica o gráfico na próxima página. Infraestrutura crítica inclui setores como comunicações, defesa, energia, finanças, governo, saúde, transportes e serviços públicos. As instalações nestes setores receberam mais de **62% de todos os ataques cibernéticos**, (mais de dois milhões de ataques no total) e as organizações financeiras receberam metade desses ataques.

As ameaças cibernéticas emergiram como uma arma nova e altamente destrutiva, capaz de perturbar ou destruir usinas de aquecimento e tratamento de água, hubs de transporte, hospitais e centros governamentais de uma região. Com a crescente digitalização da infraestrutura crítica, atualmente os agentes de ameaças podem atacar uma instalação explorando configurações incorretas de segurança e outras vulnerabilidades — tudo remotamente. O Relatório de Riscos Globais de 2024[1] do Fórum Econômico Mundial classifica a ameaça da insegurança cibernética como um dos "riscos globais mais graves previstos para os próximos dois anos".

Os incentivos financeiros também podem motivar ataques a infraestruturas. Os agentes de ameaças podem usar malwares que roubam informações (infostealers) para acessar um sistema e baixar secretamente dados como planos de defesa, contas financeiras, prontuários de saúde ou esquemas de instalações para vender a outros agentes de ameaças na dark web.

As ameaças cibernéticas contra infraestruturas críticas observadas com mais frequência incluem:

- **PrivateLoader:** Uma família de downloaders maliciosos escritos em C++ e observados continuamente desde que foram descobertos pela primeira vez em 2021. Com frequência, é usado para instalar infostealers no computador ou dispositivo da vítima.
- **RisePro:** Um infostealer comoditizado que está disponível desde 2022.
- **SmokeLoader:** Um malware de download que geralmente se espalha por meio de documentos ou links de phishing, visando organizações governamentais e de energia.
- **PikaBot:** Foi uma ameaça de destaque ao longo do ano. Este malware modular é muito semelhante ao cavalo de Tróia QakBot e tem capacidade para receber vários comandos de seu C2.
- **Inteligência Artificial (IA):** Pode ser cada vez mais usada para atingir infraestruturas críticas, especialmente processos governamentais e eleitorais, e para divulgar informações falsas. Jen Easterly, diretora da CISA, alertou,[2] "A IA generativa ampliará os riscos de segurança cibernética e tornará mais fácil, rápido e barato inundar o país com conteúdo falso".

AS INSTALAÇÕES DE INFRAESTRUTURAS CRÍTICAS FORAM ALVO DE MAIS DE 2 MILHÕES DE ATAQUES CIBERNÉTICOS.

As **empresas** também foram alvos frequentes, principalmente para obter ganhos financeiros. Esta categoria inclui varejistas, fabricantes, distribuidores atacadistas e serviços profissionais. Mais de **um milhão de ataques** tiveram como alvo o setor de empresas, o que é quase **33% de todos os ataques** bloqueados pelas soluções de segurança da BlackBerry. O ransomware foi um método de ataque comum contra empresas, assim como os infostealers. Em termos de novos malwares, **53% de todos os hashes exclusivos** deste período foram lançados contra empresas. Um malware exclusivo em geral é usado quando o atacante tem um interesse muito específico em uma determinada organização ou setor.

As principais ameaças às empresas incluíram SmokeLoader e PrivateLoader (descritos acima), bem como Formbook/XLoader, OriginLogger e Remcos. As ameaças observadas com frequência contra empresas durante o período de relatório foram:

- **Formbook:** Um infostealer antigo que foi reformulado como XLoader, captura dados de formulários e navegadores de Internet e registra as teclas digitadas.
- **Remcos:** Softwares de controle remoto e vigilância que são RATs vendidos comercialmente. Embora também sejam usados como ferramentas legítimas de vigilância, os Remcos são frequentemente usados por grupos de crimes cibernéticos.
- **OriginLogger:** É parte da família Agent Tesla, que consiste em RATs com capacidade de roubo de informações. Pode capturar dados de navegadores de Internet, registrar teclas digitadas e até capturar telas do dispositivo da vítima.

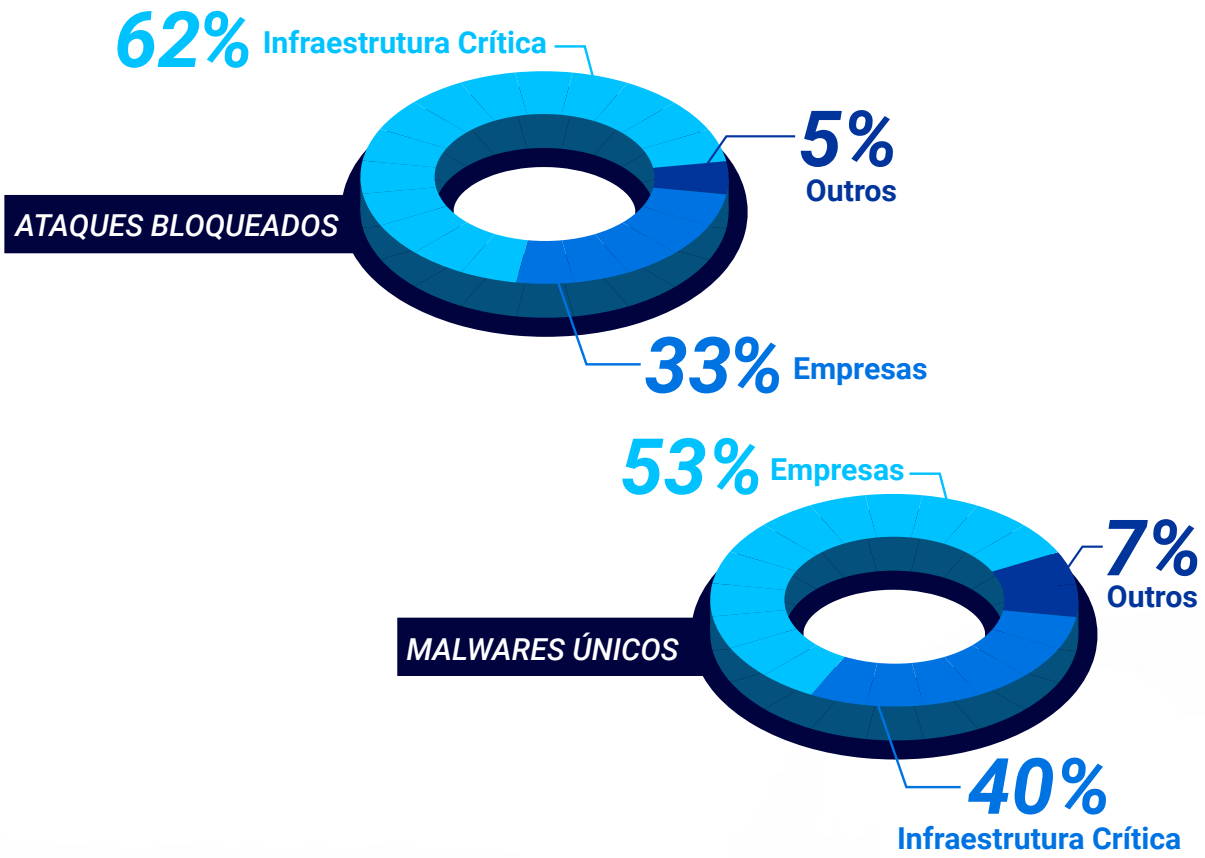

Figura 2: Ataques contra setores específicos bloqueados e hashes de malware únicos, setembro a dezembro de 2023.

CONTRA-ATAQUE

Uma notícia positiva foi o esforço multinacional de Estados Unidos, França, Alemanha, Reino Unido e outros países que derrubou com sucesso o Qakbot, um importante botnet de malware. A Operação Duck Hunt também removeu remotamente o malware Qakbot de 700 mil dispositivos infectados, incluindo 200 mil computadores[3] nos Estados Unidos. O Qakbot havia roubado mais de US$ 8,6 milhões em lucros ilícitos de criptomoedas, que foram apreendidos na Operação Duck Hunt.

Os *Relatórios Globais de Inteligência de Ameaças da BlackBerry* visam fornecer inteligência acionável e contextual sobre ameaças cibernéticas. Para ajudar os profissionais de segurança cibernética nos esforços para combater crimes cibernéticos, o relatório tem várias seções dedicadas a identificação e bloqueio das ameaças dominantes observadas neste período. Descreve as ameaças mais prevalentes por sistemas operacionais, bem como os agentes das ameaças e suas ferramentas.

Além disso, incluímos seções sobre:

- **Resposta a incidentes e análise.** A equipe de Resposta a Incidentes (RI) da BlackBerry® Cybersecurity Services fornece observações importantes sobre as ameaças às quais respondeu no período de relatório. O serviço de RI desenvolve planos de resposta rápida para ajudar a mitigar o impacto dos ataques cibernéticos e garantir que a recuperação digital adote as melhores práticas.
- **Common Vulnerabilities and Exposures (CVE).** O CVE é um programa MITRE que informa sobre vulnerabilidades e exposições publicamente conhecidas em softwares comerciais. Este período de relatório observou novas vulnerabilidades nos produtos Cisco®, Apache®, Citrix® e JetBrains®.
- **Técnicas MITRE comuns.** A BlackBerry registrou as 20 principais técnicas (das 300 da estrutura MITRE ATT&CK®) usadas para ataques cibernéticos neste período.
- **Contramedidas aplicadas.** A BlackBerry analisou as cinco principais técnicas MITRE observadas neste período e forneceu contramedidas para elas.
- **Dados e observações do CylanceGUARD.** O CylanceGUARD® é um serviço MDR por assinatura que fornece monitoramento 24 horas por dia, 7 dias por semana, 365 dias por ano e ajuda as organizações a bloquear ameaças cibernéticas sofisticadas que buscam brechas no programa de segurança do cliente. A equipe do BlackBerry MDR rastreou milhares de alertas durante o período do relatório.

Nosso objetivo é habilitar os leitores a converter nossas descobertas em recursos práticos de busca e detecção de ameaças. Para obter mais informações, leia o *Relatório Global de Inteligência de Ameaças da BlackBerry* – março de 2024.

[1] https://www.weforum.org/publications/global-risks-report-2024/
[2] https://www.foreignaffairs.com/united-states/artificial-intelligences-threat-democracy
[3] https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown

BlackBerry | Cybersecurity

Sobre a BlackBerry: A BlackBerry (NYSE: BB; TSX: BB) fornece softwares e serviços de segurança inteligentes para empresas e governos no mundo inteiro. A empresa habilita mais de 235 milhões de veículos. Com sede em Waterloo, Ontário, Canadá, a empresa alavanca IA e aprendizado de máquina para entregar soluções inovadoras nas áreas de segurança digital, proteção e privacidade de dados, e é líder em gerenciamento de segurança de endpoints, criptografia e sistemas incorporados. A visão da BlackBerry é clara — proteger um futuro conectado em que você pode confiar.

Para obter mais informações, acesse BlackBerry.com e siga @BlackBerry