**De acordo com o relatório da FortiGuard Labs**

**Destrutivo Malware Wiper aumentou mais de 50% no segundo semestre de 2022**

*A propagação em massa de malware wiper continua a mostrar a evolução destrutiva dos ciberataques. No final do ano, este malware expandiu-se para vários países, impulsionando um aumento de 53% na sua atividade.*

## Lisboa, 01 de março de 2023

**Derek Manky, Chief Security Strategist & Global VP Threat Intelligence, FortiGuard Labs**

"Para os cibercriminosos, manter o acesso e evitar a deteção não é uma conquista pequena, uma vez que as defesas cibernéticas continuam a evoluir para proteger as organizações. Para contrariar, os adversários estão a evoluir com mais técnicas de reconhecimento e a implementar alternativas de ataque mais sofisticadas para permitir as suas tentativas destrutivas com métodos de ameaça do tipo APT, tais como o malware wiper ou outros códigos avançados. Para se protegerem contra estas táticas avançadas de cibercrime, as organizações devem estar focadas em permitir uma inteligência de ameaça coordenada e acionável em tempo real, orientada por *machine learning*, através de todos os dispositivos de segurança para detetar ações suspeitas e iniciar a mitigação em toda a superfície de ataque".

A Fortinet®, líder mundial de cibersegurança que fomenta a convergência entre segurança e redes, acaba de divulgar o relatório semestral Threat Landscape da FortiGuard Labs. O cenário das ameaças e a superfície de ataque das organizações estão em constante transformação, e a capacidade dos cibercriminosos de conceber e adaptar as suas técnicas a este ambiente continua a representar um risco significativo para as empresas de todas as dimensões, independentemente da indústria ou da geografia. Para uma visão detalhada do relatório, bem como de algumas decisões importantes, consulte o [blog](https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings-2h-2022?utm_source=pr&utm_medium=pr&utm_campaign=threat-report-2h-2022).

Destaques do relatório do segundo semestre de 2022:

* A propagação em massa de malware wiper continua a mostrar a evolução destrutiva dos ciberataques.
* A nova inteligência permite aos CISOs priorizar os esforços de mitigação dos riscos e minimizar a superfície de ataque ativa com a expansão da abordagem da "Zona Vermelha".
* A ameaça de ransomware permanece em níveis elevados sem qualquer evidência de abrandamento global com novas variantes ativadas pelo Ransomware-as-a-Service (RaaS).
* O malware mais prevalecente tinha mais de um ano e tinha passado por uma grande quantidade de especiação, destacando a eficácia e economia da reutilização e reciclagem do código.
* Log4j continua a ter impacto nas organizações de todas as regiões e indústrias, principalmente em tecnologia, governo e educação.

**Malware Wiper destrutivo tipo APT aumentou em 2022**

A análise dos dados do malware wiper revela uma tendência para cibercriminosos que utilizam de forma consistente técnicas de ataque destrutivas contra os seus alvos. Também mostra que com a falta de limites na internet, podem facilmente escalar estes tipos de ataques, que foram em grande parte permitidos pelo modelo de Cybercrime-as-a-Service (CaaS).

No início de 2022, a FortiGuard Labs identificou a presença de vários novos wipers em simultâneo com a guerra entre a Rússia e a Ucrânia. No final do ano, esta forma de malware expandiu-se para vários países, impulsionando um aumento de 53% na atividade do wiper, só no Q3 para o Q4. Embora parte desta atividade tenha sido possibilitada pelo malware wiper, que pode ter sido inicialmente desenvolvido e implementado por atores do Estado-nação em torno da guerra, está a ser captado por grupos cibercriminosos e está a espalhar-se para além da Europa. Infelizmente, a trajetória deste malware destrutivo não parece estar a abrandar com base no volume de atividade visto no quarto trimestre, o que significa que qualquer organização continua a ser um potencial alvo, e não apenas organizações baseadas na Ucrânia ou países circundantes.



**Volume de Malware Wiper**

**Mapeamento de CVEs revela zona vermelha de vulnerabilidade para ajudar os CISOs a definir prioridades**

As tendências *exploit* ajudam a identificar o que os cibercriminosos estão interessados em atacar, sondar para futuros ataques e o que têm como alvo ativo. A FortiGuard Labs tem um vasto arquivo de vulnerabilidades conhecidas e, através do enriquecimento destes dados, foi capaz de identificar as que são exploradas ativamente em tempo real e mapear zonas de risco através da superfície de ataque.

No segundo semestre de 2022, menos de 1% do total das vulnerabilidades observadas numa organização de dimensão empresarial estavam em endpoints e ativamente sob ataque, dando aos CISOs uma visão clara da Zona Vermelha através da inteligência da superfície de ataque ativa de que deveriam dar prioridade aos esforços para minimizar o risco e onde concentrar os esforços para corrigir.

**Motivações financeiras mantêm a Cibercriminalidade e o Ransomware em níveis elevados**

Com as diversas intervenções realizadas pela equipa de Resposta a Incidentes (IR) da Fortiguard Labs, descobriu-se que a motivação financeira no cibercrime resultou no maior volume de incidentes (73,9%), seguido pela espionagem (13%). Ao longo de 2022, 82% dos cibercrimes motivados por dinheiro envolveram ransomware ou scripts maliciosos, mostrando que a ameaça global de ransomware permanece elevada e sem qualquer evidência de abrandamento, graças à crescente popularidade de [Ransomware-as-a-Service (RaaS)](https://www.fortinet.com/blog/industry-trends/the-war-on-cybercrime-and-ransomware-are-you-ready?utm_source=blog&utm_medium=blog&utm_campaign=RaaS) na dark web.

De facto, o volume de ransomware aumentou 16% a partir do primeiro semestre de 2022. De um total de 99 famílias de ransomware observados, as cinco principais famílias representaram cerca de 37% de toda a atividade de ransomware durante o segundo semestre de 2022. GandCrab, um malware RaaS que surgiu em 2018, está no topo da lista. Embora os criminosos por detrás do GandCrab tenham anunciado que se iriam reformar depois de terem obtido mais de 2 mil milhões de dólares em lucros, houve muitas iterações do GandCrab durante o seu tempo ativo. É possível que o longo legado deste grupo criminoso ainda esteja a perpetuar-se, ou que o código tenha sido simplesmente construído, alterado e relançado, demonstrando a importância de parcerias globais entre todos os tipos de organizações para desmantelar permanentemente as operações criminosas. A rutura efetiva das cadeias de abastecimento concorrentes requer um esforço a nível global com relações fortes, de confiança e colaboração entre os intervenientes na cibersegurança em organizações e indústrias públicas e privadas.

**Adversary Code Reuse mostra a natureza engenhosa dos adversários**

Os cibercriminosos são de uma natureza empreendedora e procuram sempre maximizar os investimentos e conhecimentos existentes para tornar os seus esforços de ataque mais eficazes e rentáveis. A reutilização de código é uma forma eficiente e lucrativa de os cibercriminosos se basearem em resultados bem-sucedidos, enquanto fazem alterações iterativas para aperfeiçoar os seus ataques e ultrapassar obstáculos defensivos.

Quando a FortiGuard Labs analisou o malware mais prevalecente no segundo semestre de 2022, a maioria dos principais pontos foram detidos por malware com mais de um ano de existência. A FortiGuard Labs analisou ainda uma coleção de diferentes variantes de Emotet para analisar a sua tendência de reutilização de código. A investigação mostrou que o Emotet passou por uma especiação significativa com variantes que resultaram em cerca de seis "espécies" diferentes de malware. Os cibercriminosos não estão apenas a automatizar ameaças, mas também a adaptar ativamente o código para o tornar ainda mais eficaz.

**A ressurreição do mais antigo botnet demonstra a resiliência das cadeias de abastecimento concorrentes**

Além da reutilização de códigos, os adversários estão também a aproveitar as infraestruturas existentes e ameaças mais antigas para maximizar as oportunidades. Ao examinar as ameaças botnet por prevalência, a FortiGuard Labs descobriu que muitas das principais redes botnets não são novas. Por exemplo, a rede botnets Morto, que foi observada pela primeira vez em 2011, surgiu no final de 2022. E outras como Mirai e Gh0st.Rat continuam a ser predominantes em todas as regiões. Surpreendentemente, das cinco principais redes botnets observadas, só a RotaJakiro é desta década.

Apesar de ser tentador desconsiderar as ameaças mais antigas, como histórias do passado, as organizações, de qualquer setor, devem continuar a manter-se vigilantes. Estas botnets "vintage" continuam a ser omnipresentes por uma razão: continuam a ser muito eficazes. Os cibercriminosos engenhosos continuarão a aproveitar a infraestrutura de botnets existente e a desenvolvê-la em versões cada vez mais persistentes com técnicas altamente especializadas, porque o ROI está lá. Especificamente, no segundo semestre de 2022, alvos significativos de Mirai incluíam managed security service providers (MSSPs), o setor das telecomunicações/transportadoras, e o setor transformador, que é conhecido pela sua tecnologia operacional (OT) abrangente. Os cibercriminosos estão a fazer um esforço concertado para visar essas indústrias com métodos comprovados.

**Log4j continua amplamente difundido e alvo dos cibercriminosos**

Mesmo com toda a publicidade que Log4j recebeu em 2021, e no primeiro semestre de 2022, um número significativo de organizações ainda não corrigiram ou aplicaram os controlos de segurança apropriados para proteger as suas organizações contra uma das vulnerabilidades mais notáveis da história.

No segundo semestre de 2022, a Log4j estava ainda fortemente ativa em todas as regiões. De facto, a FortiGuard Labs identificou que 41% das organizações detetaram atividade Log4j, mostrando quão generalizada a ameaça permanece. A atividade da IPS Log4j foi mais prevalecente nos setores da tecnologia, governo e educação, o que não deve ser surpresa, dada a popularidade do Apache Log4j como software de open-source.

**Análise de uma parte da história do Malware: transferências de entrega demonstram urgência para sensibilização do utilizador**

A análise de estratégias adversárias dá valiosos conhecimentos sobre como as técnicas e táticas de ataque estão a evoluir para melhor proteger contra futuros cenários de ataque. A FortiGuard Labs analisou a funcionalidade de malware detetado com base em dados de sandbox para rastrear as abordagens de entrega mais comuns. É importante notar que isto apenas analisa as amostras detonadas.

Ao rever as oito táticas e técnicas mais utilizadas no sandboxing, o *drive-by-compromise* foi a tática mais utilizada pelos cibercriminosos para obter acesso aos sistemas das organizações em todas as regiões do mundo. Os adversários estão principalmente a ganhar acesso aos sistemas das vítimas quando estas navegam na internet e descarregam involuntariamente um *payload* malicioso, visitando um website comprometido, abrindo um anexo de correio eletrónico malicioso ou mesmo clicando num link ou numa janela pop-up enganosa. O desafio com a tática de drive-by é que, uma vez acedida e descarregada, é, em muitos casos, demasiado tarde para o utilizador escapar, a menos que tenha uma abordagem holística da segurança.

**Mudar para conseguir enfrentar de frente as ameaças**

A Fortinet é líder em cibersegurança de classe empresarial e inovação em rede, ajudando os CISOs e as equipas de segurança a parar um ataque kill chain, a minimizar o impacto dos incidentes de cibersegurança e a preparar-se melhor para potenciais ameaças cibernéticas.

As soluções de segurança da Fortinet incluem uma variedade de ferramentas poderosas como firewalls de próxima geração (NGFW), telemetria e análise de rede, endpoint detection e response (EDR), extended detection e response (XDR), digital risk protection (DRP), security information e event management (SIEM), sandboxing em linha, *deception*, security orchestration, automation e response (SOAR), e muito mais. Estas soluções fornecem capacidades avançadas de deteção e prevenção de ameaças que podem ajudar as organizações a detetar e responder rapidamente a incidentes de segurança em toda a sua superfície de ataque.

Para complementar estas soluções e apoiar as equipas com escassez de profissionais e talento na área da cibersegurança, a Fortinet também oferece serviços de inteligência de ameaças e de resposta a ameaças com capacidade de machine learning. Estes fornecem informação atualizada sobre as últimas ciber ameaças e permitem às empresas responder rapidamente a incidentes de segurança, minimizando o impacto na organização. Os serviços Fortinet de aumento de human-based SOC e de inteligência de ameaças também ajudam as equipas de segurança a prepararem-se melhor para as ameaças cibernéticas e fornecem capacidades de monitorização de ameaças e de resposta a incidentes em tempo real.

Este conjunto abrangente de soluções e serviços de cibersegurança permite aos CISOs e às equipas de segurança concentrarem-se na viabilização dos negócios e dos projetos de maior prioridade.

**Visão Geral do Relatório**

Este último relatório global Threat Landscape representa a inteligência coletiva da [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=blog&utm_medium=blog&utm_campaign=fglabs), extraída da vasta gama de sensores da Fortinet que recolhem milhares de milhões de eventos de ameaça observados em todo o mundo durante o segundo semestre de 2022. Usando a estrutura MITRE ATT&CK, que classifica táticas, técnicas e procedimentos adversos (TTPs), o relatório Threat Landscape da FortiGuard Labs destaca a descrição de como os atores da ameaça visam as vulnerabilidades, constroem infraestruturas maliciosas e exploram os seus alvos. O relatório também cobre perspetivas globais e regionais, bem como tendências de ameaças que afetam tanto ambientes de TI como OT.

**Recursos Adicionais**

* Subscreva o [blog](https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings-2h-2022?utm_source=pr&utm_medium=pr&utm_campaign=threat-report-2h-2022) para obter informações importantes desta investigação enquanto a equipa da FortiGuard Labs examina cada um dos tópicos do [relatório](https://global.fortinet.com/lp-en-ap-2022globalthreatlandscape-H2?utm_source=website&utm_medium=pressrelease&utm_campaign=TL_Report-NAMER-US&utm_content=RR-TLandscapeReport-G&utm_term=R&lsci=7012H0000021peSQAQ&UID=ftnt-6060-42058) nas próximas semanas.
* Saiba mais sobre inteligência e investigação de ameaças da [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=blog&utm_medium=blog&utm_campaign=fglabs) e [Outbreak Alerts](https://www.fortinet.com/fortiguard/outbreak-alert?utm_source=blog&utm_medium=blog&utm_campaign=outbreak), que fornecem indicadores importantes para mitigar ataques de cibersegurança.
* Saiba mais sobre o [portfólio](https://www.fortinet.com/solutions/enterprise-midsize-business/security-as-a-service/fortiguard-subscriptions?utm_source=blog&utm_medium=blog&utm_campaign=services) de Serviços de Segurança FortiGuard da Fortinet.
* Saiba mais sobre a [formação gratuita de cibersegurança](https://www.fortinet.com/training/cybersecurity-professionals?utm_source=PR&utm_medium=PR&utm_campaign=freetraining) da Fortinet, que inclui uma ampla consciencialização cibernética e formação de produtos. Como parte da Training Advancement Agenda (TAA), da Fortinet, o Fortinet Training Institute também oferece formação e certificação através dos programas [Network Security Expert (NSE)](https://www.fortinet.com/training-certification?utm_source=PR&utm_medium=PR&utm_campaign=NSE), [Academic Partner](https://www.fortinet.com/training/academic-partner-program?utm_source=PR&utm_medium=PR&utm_campaign=academicpartner) e [Education Outreach](https://www.fortinet.com/training/education-outreach-program?utm_source=pr&utm_medium=pr&utm_campaign=outreach).
* Leia sobre como os [clientes da Fortinet](https://www.fortinet.com/customers?utm_source=pr&utm_medium=pr&utm_campaign=customers) estão a proteger as suas organizações.
* Siga a Fortinet no [Twitter](https://twitter.com/Fortinet?utm_source=PR&utm_medium=PR&utm_campaign=twitter), [LinkedIn](https://www.linkedin.com/company/6460/admin/?utm_source=PR&utm_medium=PR&utm_campaign=li), [Facebook](https://www.facebook.com/Fortinet/?utm_source=PR&utm_medium=PR&utm_campaign=fb) e [Instagram](https://www.instagram.com/behindthefirewall/?utm_source=PR&utm_medium=PR&utm_campaign=IG). Subscreva a Fortinet no [blog](https://www.fortinet.com/blog?utm_source=PR&utm_medium=PR&utm_campaign=blog) ou no [YouTube](https://www.youtube.com/channel/UCJHo4AuVomwMRzgkA5DQEOA?sub_confirmation=1).

**Sobre a FortiGuard Labs**

A FortiGuard Labs é a organização de investigação e inteligência de ameaças da Fortinet. A sua missão é fornecer aos clientes da Fortinet as melhores informações sobre ameaças da indústria, concebidas para os proteger de atividades maliciosas e de ciberataques sofisticados. É composta por alguns dos hunters de ameaças mais conhecedores da indústria, investigadores, analistas, engenheiros e cientistas de dados da indústria, trabalhando em laboratórios dedicados à investigação de ameaças em todo o mundo. A FortiGuard Labs monitoriza continuamente a superfície de ataque mundial utilizando milhões de sensores de rede e centenas de parceiros de partilha de informações. Analisa e processa esta informação utilizando IA e outra tecnologia inovadora para extrair esses dados para novas ameaças. Estes esforços resultam em informações oportunas e acionáveis sobre ameaças sob a forma de atualizações de produtos de segurança Fortinet, investigação proactiva de ameaças para ajudar os nossos clientes a compreender melhor as ameaças e os atores que enfrentam, e informações sobre ameaças para ajudar os nossos clientes a compreender melhor e defender o seu panorama de ameaças. Saiba mais em <https://www.fortinet.com>, no [Blog da Fortinet](https://www.fortinet.com/blog?utm_source=blog&utm_medium=blog&utm_campaign=blog), e [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_medium=pr&utm_campaign=fglabs).

**Sobre Fortinet**

A [Fortinet](https://www.fortinet.com/blog?utm_source=pr&utm_medium=pr&utm_campaign=boiler) (NASDAQ: FTNT) torna possível a existência de um mundo digital em que podemos sempre confiar através da sua missão de proteger pessoas, dispositivos e dados em qualquer lugar, sendo que hoje oferece cibersegurança onde for necessário, com um portfólio com mais de 50 serviços de nível empresarial. Mais de meio milhão de clientes confiam nas soluções Fortinet, que se encontram entre as mais adotadas, mais patenteadas e mais validadas na indústria. O [Fortinet Training Institute](https://www.fortinet.com/nse-training?utm_source=pr&utm_campaign=nse-training), um dos maiores e mais amplos programas de formação da indústria, dedica-se a tornar a formação em cibersegurança e novas oportunidades de carreira disponíveis a todos. A [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=fortiguardlabs), a organização de elite da Fortinet de inteligência de ameaças e investigação, desenvolve e utiliza tecnologias machine learning e de IA para fornecer aos clientes proteção e inteligência de ameaças. Saiba mais em https://www.fortinet.com, no [Blog da Fortinet](https://www.fortinet.com/blog?utm_source=blog&utm_medium=blog&utm_campaign=blog), e na [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_medium=pr&utm_campaign=fglabs).

**Para mais informação contacte:**

**Lift Consulting**

Erica Macieira | erica.macieira@lift.com.pt | 910549515

Inês Filipe | ines.filipe@lift.com.pt | 910 283 054