Leitura do relatório ENISA Threat Landscape 2025 - Against Invaders - Not

Data: 2025-10-06 07:06:28

Autor: Inteligência Against Invaders

Leitura do relatório ENISA Threat Landscape 2025

Panorama de ameaças da ENISA 2025: o aumento do ransomware, do phishing de IA e da espionagem apoiada pelo Estado marcam um cenário convergente e persistente de ciberameaças na UE.

O relatório ENISA Threat Landscape 2025 fornece uma análise abrangente do cenário de ameaças em evolução na Europa. O relatório analisa os eventos ocorridos entre julho de 2024 e junho de 2025, incluindo quase 4.900 incidentes verificados. A edição deste ano combina profundidade técnica com insights estratégicos.

O relatório enfatiza como o cenário de ameaças está amadurecendo, caracterizado pela rápida exploração de vulnerabilidades, pela profissionalização do crime cibernético e pela crescente convergência entre criminosos, alinhados ao Estado e hacktivista Operações.

“Paralelamente, ferramentas hacktivistas e ecossistemas criminosos se cruzam cada vez mais. O surgimento do FunkSec no final de 2024 trouxe o ransomware FunkLocker, misturando mensagens políticas com extorsão financeira, ressaltando a rapidez com que a marca orientada por ideologia pode se transformar em monetização.” lê o relatório. “Os hacktivistas, em busca de financiamento e visibilidade, adotaram o ransomware além do DDoS e das desfigurações. A CyberVolk, operando de acordo com os interesses russos, usou e promoveu várias cepas – AzzaSec, HexaLocker, Parano, bem como LockBit e Chaos – desde maio de 2024. Matar Seg, originalmente uma marca hacktivista pró-Rússia alinhada com o Anonymous, estreou sua plataforma em junho de 2024.”

O ransomware continua a ser uma das ameaças mais perigosas, representando a atividade mais perturbadora e economicamente prejudicial em toda a UE. A ENISA observa que os grupos de ransomware descentralizaram as operações após as principais ações de aplicação da lei, adotando táticas agressivas de dupla e tripla extorsão e explorando os temores de conformidade regulatória para pressionar as vítimas.

O crescimento de Ransomware como serviço (RaaS), vazamentos públicos de ferramentas de construção e o aumento de corretores de acesso reduziram drasticamente as barreiras à entrada, promovendo um mercado criminoso diversificado e resiliente.

Atores patrocinados e alinhados ao Estado escalaram simultaneamente as campanhas de ciberespionagem de longo prazo, particularmente telecomunicações, redes logísticas e setores de manufatura na UE. Essas operações mostram técnicas avançadas, incluindo comprometimentos da cadeia de suprimentos, malware modular e abuso de drivers assinados para manter a persistência e evitar a detecção.

Um elemento marcante do relatório é o domínio das operações hacktivistas, que respondem por quase 80% de todos os incidentes registrados. Estes são principalmente de baixo impacto Negação de serviço distribuída (DDoS) motivadas por ideologia ou geopolítica, muitas vezes aproveitando ferramentas de baixo custo e facilmente disponíveis. Embora seu impacto direto permaneça limitado, sua escala demonstra como as operações cibernéticas se tornaram instrumentos de protesto e influência digital.

Do ponto de vista setorial, a administração pública continua a ser a mais visada (38 % dos casos), seguida dos transportes, em que as infraestruturas marítimas e logísticas enfrentaram perturbações significativas devido a campanhas de ransomware e espionagem. As operações de aviação e frete também sofreram incidentes que afetaram a continuidade, enquanto a infraestrutura digital e os serviços online continuam a atrair a atenção de operadores de ransomware e agentes de espionagem.

O phishing continua sendo o principal vetor de intrusão (60%), evoluindo para modelos industrializados baseados em assinatura, como Phishing como serviço (PhaaS). Essas plataformas permitem que até mesmo adversários pouco qualificados conduzam campanhas sofisticadas, aproveitando o conteúdo gerado por IA, mídia sintética e automação. Enquanto isso, a exploração de vulnerabilidades (21,3%) continua sendo a pedra angular do acesso inicial, com os adversários muitas vezes armando as falhas recém-divulgadas em poucos dias. A ENISA enfatiza a urgência de patches oportunos e higiene cibernética robusta como principais medidas de defesa.

Uma preocupação crescente destacada no relatório é o papel da Inteligência artificial. No início de 2025, o phishing assistido por IA e a engenharia social representavam mais de 80% da atividade global observada nessa categoria. Os invasores estão explorando modelos de IA com jailbreak, conteúdo sintético de voz e vídeo e envenenamento de modelos para automatizar operações de reconhecimento, representação e influência, tornando a detecção e a atribuição cada vez mais difíceis.

“Como uma tendência previsível, os Large Language Models (LLMs) são aproveitados para criar phishing mais convincente
e-mails; com mais de 80% de todos os e-mails de phishing identificados entre setembro de 2024 e fevereiro
2025 usando IA até certo ponto. A IA é notavelmente usada em vishing e fraudes online envolvendo falsificação de identidade, com o uso de deepfakes, bem como para desenvolvimento de malware.” continua o relatório. “Observou-se que os grupos de ameaças estavam aproveitando LLMs comerciais para aumentar as operações, bem como LLMs desbloqueados ou retreinados (desviados), como WormGPT, EscapeGPT e FraudeGPT, para automatizar atividades de engenharia social e acelerar o desenvolvimento de ferramentas maliciosas”.

No geral, o ENISA Threat Landscape 2025 descreve um ambiente de ameaças convergente e persistente, onde as distinções tradicionais entre cibercrime, espionagem e hacktivismo são cada vez mais confusas. Em vez de ataques únicos de alto impacto, a Europa agora enfrenta campanhas contínuas, diversificadas e sobrepostas que coletivamente corroem a resiliência e a confiança.

A ENISA conclui instando os Estados-Membros e organizações da UE a priorizar a colaboração intersetorial, aumentar a consciência situacional e incorporar a resiliência por meio de melhor gerenciamento de vulnerabilidades, compartilhamento de inteligência de ameaças e investimento em capacitação em segurança cibernética. O relatório traça um quadro claro: o cenário europeu de ameaças já não é definido por incidentes isolados, mas por uma pressão constante e adaptativa

sobre a infraestrutura digital e a sociedade no seu conjunto.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking, ENISA Threat Landscape 2025)