Hackers estatais russos colaboram em ataques contra a Ucrânia - Against

Data: 2025-09-20 13:37:45

Autor: Inteligência Against Invaders

Dois agentes de ameaças ligados ao Estado russo, [Gamaredon](#) e [Turla](#), estão trabalhando juntos para comprometer alvos de defesa de alto valor na Ucrânia, de acordo com um novo relatório da ESET.

Essas colaborações envolvem o uso compartilhado de ferramentas em campanhas durante 2025 e refletem uma cultura estratégica mais ampla dentro da segurança interna e da defesa nacional da Rússia.

Em quatro ataques observados em fevereiro, a ESET capturou uma carga mostrando que o Turla era capaz de emitir comandos por meio de implantes Gamaredon.

A ferramenta de download PteroGraphin, considerada exclusiva do Gamaredon, foi usada para reiniciar o malware backdoor Kazuar do Turla. Portanto, é provável que o PteroGraphin tenha sido usado como método de recuperação pelo Turla, possivelmente depois que o Kazuar travou ou não foi iniciado automaticamente.

O Kazuar foi usado para baixar os dados da máquina, incluindo o nome do computador e o nome de usuário da vítima, a lista de processos em execução, a versão do sistema operacional e listas de arquivos e diretórios em vários locais.

Em abril e junho de 2025, os instaladores do Kazuar v2 foram implantados diretamente pelas ferramentas Gamaredon.

Essas descobertas levaram os pesquisadores a concluir com alta confiança que os dois grupos estão colaborando.

“Esta é a primeira vez que conseguimos vincular esses dois grupos por meio de indicadores técnicos”, observaram os pesquisadores da ESET no [relatório](#) publicado em 19 de setembro.

“A invasão em grande escala da Ucrânia em 2022 provavelmente reforçou essa convergência, com os dados da ESET mostrando claramente as atividades de Gamaredon e Turla com foco no setor de defesa ucraniano nos últimos meses”, acrescentaram.

Grupos FSB colaboradores com diferentes estratégias de segmentação

Acredita-se que Gamaredon e Turla sejam afiliados ao Serviço Federal de Segurança da Rússia (FSB).

Ambos os grupos têm sido altamente ativos desde a invasão da Ucrânia pela Rússia em 2022.

Embora o Gamaredon tenha sido observado comprometendo “centenas, senão milhares de máquinas”, o Turla só foi detectado em sete máquinas na Ucrânia nos últimos 18 meses. Isso sugere que o grupo está interessado apenas em máquinas específicas, provavelmente aquelas que contêm inteligência altamente sensível, observaram os pesquisadores.

Ambos os atores estão focados na espionagem cibernética.

Gamaredon está ativo desde pelo menos 2013, visando principalmente instituições governamentais ucranianas.

Turla está ativo desde pelo menos 2004, possivelmente desde o final dos anos 1990. Ele se concentra principalmente em alvos de alto perfil, como governos e entidades diplomáticas, na Europa, Ásia Central e Oriente Médio.

Além dos ataques detectados em fevereiro, abril e junho, os pesquisadores observaram outros casos de ferramentas Gamaredon presentes em máquinas na Ucrânia onde o Kazuar também estava presente.