ESET descobre colaboração Gamaredon-Turla em ataques cibernéticos na

Data: 2025-09-21 22:44:31

Autor: Inteligência Against Invaders

ESET descobre colaboração Gamaredon-Turla em ataques cibernéticos na Ucrânia

A ESET encontrou evidências de que os grupos ligados à Rússia Gamaredon e Turla colaboraram em ataques cibernéticos à Ucrânia entre fevereiro e abril de 2025.

A ESET relatou grupos ligados à Rússia Gamaredon e Turla colaborou em ataques cibernéticos contra entidades na Ucrânia.

O grupo APT vinculado à RússiaGamaredon(também conhecido como Shuckworm,Armagedom,Urso Primitivo,ACTÍNIO,Callisto)é conhecida por atacar organizações governamentais, policiais e de defesa na Ucrânia desde 2013.

OTurlaGrupo APT (também conhecido comoCobra,Uroburos,Insetos d'água,Urso Venenosoe CRIPTÔNIO)está ativo desdepelo menos 2004, visando organizações diplomáticas e governamentais e empresas privadas no Oriente Médio, Ásia, Europa, América do Norte e do Sul e nações do antigo bloco soviético.

Turla vem do Centro 16 do FSB, o sucessor da 16ª Diretoria da KGB focada em inteligência estrangeira, enquanto Gamaredon se conecta ao Centro 18, enraizado na 2ª Diretoria de Segurança Interna da KGB. Essas unidades muitas vezes trabalharam juntas no passado, e suas funções ainda se sobrepõem hoje, especialmente na Ucrânia. Enquanto as agências russas competem ferozmente, grupos dentro do mesmo serviço geralmente cooperam – como Turla e Gamaredon agora.

De acordo com pesquisadores da ESET, os grupos apoiados pelo Estado russo Gamaredon e Turla se uniram em ataques cibernéticos à Ucrânia entre fevereiro e abril de 2025. A Gamaredon implantou suas próprias ferramentas para reiniciar os sistemas e, em seguida, lançou Malware Turla em alvos ucranianos selecionados. Essa rara colaboração mostra como diferentes agentes de ameaças podem se coordenar para maximizar o impacto, aumentando a sofisticação e a persistência de ataques contra sistemas ucranianos críticos durante um clima geopolítico tenso.

No início de 2025, a ESET detectou quatro co-compromissos na Ucrânia, onde o grupo APT Gamaredon implantou várias ferramentas como PteroLNK e PteroGraphin, enquanto o Turla instalava Kazuar malware. Em um sistema, Turla até usou o implante de Gamadon para reiniciar o Kazuar, provando a colaboração ativa entre os dois grupos de ciberespionagem. Mais tarde, Gamaredon implantou o Kazuar v2 diretamente, confirmando a dependência de Turla em Gamaredon para acessar os principais alvos ucranianos. Os especialistas apontaram que isso marca o primeiro elo técnico entre os dois grupos.

“Em fevereiro de 2025, por meio da telemetria da ESET, detectamos quatro co-compromissos diferentes de Gamaredon-Turla na Ucrânia.” lê o relatório publicado pela ESET. “Nessas máquinas, a Gamaredon implantou uma ampla gama de ferramentas, incluindoPteroLNK, PteroStew, PteroOdd, PteroEffigy e PteroGraphin, enquanto o Turla implantou apenas o Kazuar v3.”

Nos últimos 18 meses, os pesquisadores rastrearam o Turla em sete máquinas ucranianas. Gamaredon violou quatro deles pela primeira vez em janeiro de 2025, então Turla implantou o Kazuar v3 durante o mês seguinte. O último caso Turla antes disso datava de Fevereiro de 2024. Enquanto Gamaredon inunda a Ucrânia com infecções, o segundo APT escolhe apenas os sistemas mais valiosos, provavelmente aqueles que possuem inteligência sensível, confirmando seu foco em alvos de espionagem de alto valor.

Ambos os grupos APT ligados ao FSB da Rússia parecem estar colaborando na Ucrânia. Gamaredon tem um histórico de compartilhamento de acesso com outros atores como InvisiMole, enquanto Turla frequentemente sequestra a infraestrutura de outros, como visto com Plataforma de petróleo em 2019, Andrômeda em 2023 e Amadey em 2024. Analistas acreditam que o cenário mais provável é que Gamaredon entregou à Turla acesso a máquinas selecionadas, permitindo as operações da Kazuar. Menos provável, Turla sequestrou as ferramentas de Gamaredon ou Gamaredon secretamente usou o próprio Kazuar.

Abaixo estão as três hipóteses para explicar as observações da ESET:

*“**Improvável**: Gamaredon tem acesso ao Kazuar e o implanta em máquinas muito específicas. Dada a abordagem barulhenta de Gamaredon, não achamos que seria tão cuidadoso implantar Kazuar em apenas um conjunto muito limitado de vítimas. **Muito provável**: Dado que ambos os grupos fazem parte dos Russian FSB (embora em dois centros diferentes), o Gamaredon forneceu acesso aos operadores do Turla para que eles pudessem emitir comandos em uma máquina específica para reiniciar o Kazuar e implantar o Kazuar v2 em alguns outros.” continua o relatório.*

“Improvável: Turla comprometeu a infraestrutura do Gamaredon e aproveitou esse acesso para recuperar o acesso em uma máquina na Ucrânia. Como o PteroGraphin contém um token codificado que permite modificar as páginas C&C, essa possibilidade não pode ser totalmente descartada. No entanto, isso implica que Turla foi capaz de reproduzir toda a cadeia Gamardedon.

O método de acesso inicial do Gamaredon permanece obscuro, mas os pesquisadores observam que o grupo geralmente depende de spear-phishing e arquivos LNK maliciosos em unidades removíveis, espalhados por meio de ferramentas como o PteroLNK.

ESET lançado indicadores de comprometimento (IoCs) e amostras pelos ataques que investigou.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,Gamaredon)