Talos

ANÁLISE DO ANO 2022

UCRÂNIA

BAIXE AQUI O RELATÓRIO COMPLETO EM INGLÊS

O suporte contínuo do Talos à Ucrânia tem sido um grande foco de nossos esforços operacionais este ano. Impulsionado pela nossa missão principal de proteger o povo e a infraestrutura ucraniana, o Talos lançou uma força-tarefa de mais de 40 voluntários dedicados a defender nossos clientes e parceiros. Essa equipe de especialistas monitora clientes de infraestrutura essencial para identificar ameaças, corrigir ataques e coletar informações.

PRINCIPAIS ADVERSÁRIOS E AMEAÇAS

A lista a seguir representa um instantâneo dos adversários e ameaças que o Talos observou que visaram as entidades ucranianas e seus aliados em 2022:

- Antes e depois da invasão, vimos diversos limpadores destrutivos e outros produtos de malware contra alvos ucranianos, inclusive WhisperGate, HermeticWiper, CaddyWiper, DoubleZero e CyclopsBlink.
- Os criminosos cibernéticos exploraram a situação ao anunciar ferramentas cibernéticas ofensivas que, na verdade, eram malware que visavam entidades russas e usavam iscas de e-mail com temas relacionados à crise para realizar golpes financeiros e fornecer cavalos de Troia de acesso remoto.
- O grupo Gamaredon, patrocinado pelo estado russo, distribuiu malware para roubo de informações, e um agente supostamente patrocinado pelo estado tentou realizar um ataque à cadeia de fornecimento chamado GoMet.
- O agente de ameaças com sede na China, Mustang Panda, realizou campanhas de phishing contra entidades na Europa e na Rússia usando documentos "oficiais" falsos como iscas.
- O grupo de hacktivistas alinhado à Rússia, Killnet, lançou ataques de negação de serviço contra sites nos países a favor a Ucrânia.

TENDÊNCIAS DE COMPORTAMENTO

De acordo com os dados que coletamos desde o início de 2022, vimos as seguintes tendências indicativas de comportamentos de oponentes ativos na Ucrânia:

- Utilitários comuns, como PowerShell e Windows Management Instrumentation (WMI), continuam sendo os principais alvos dos oponentes que buscam utilizar o ataque " live off the land" e evitar a detecção.

Figura 1.*Principais ataques cibernéticos contra a Ucrânia.*

UCRÂNIA

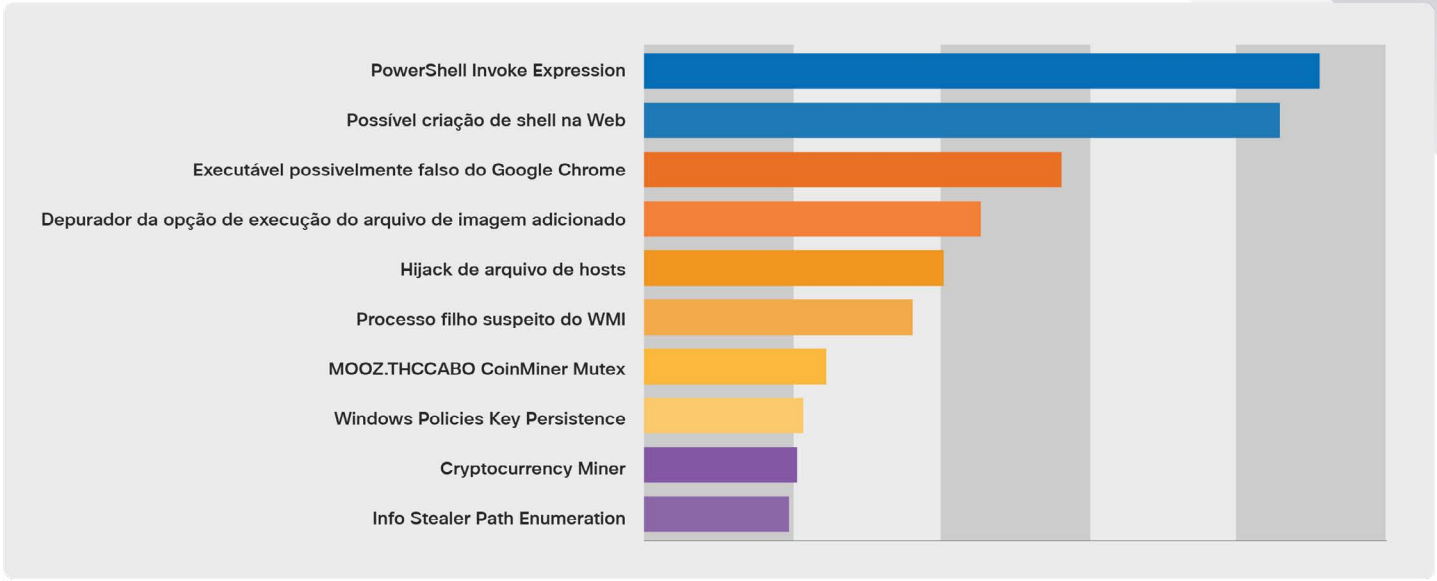

Figura 2. *A maioria das regras de proteção comportamental ativas do Cisco Secure Endpoint em clientes ucranianos em que o Cisco Secure Endpoint foi implantado.*

- Técnicas como a utilização de executáveis do Google Chrome e o uso de chaves de políticas do Windows para estabelecer a persistência foram vistas em maior número.
- Um aumento observado nas detecções de ladrões de informações e mineradores de criptomoedas. No entanto, vemos agentes em todo o espectro avançado, cujo objetivo principal é a atividade destrutiva.
- Observamos um pico nos alertas de " execução de proxy binário assinado usando rundll32" na Ucrânia, mas também em nível global. Essa técnica utiliza o acervo de links dinâmicos (DLL) para executar código mal-intencionado.

Apesar do aumento da atividade contra alvos na Ucrânia, nossa equipe de resposta a incidentes observou menos ameaças contra os clientes da Cisco em geral durante o primeiro semestre de 2022. É possível que o conflito tenha atraído agentes de ameaças que, de outra forma, estariam realizando ataques em outro lugar.

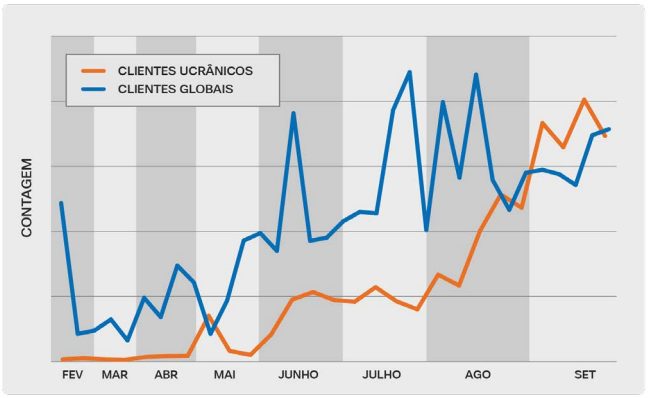

Figura 3. *Detecções de prevenção de exploração para "execução de proxy binário assinado usando rundll32" em clientes ucranianos e clientes globais, de fevereiro a setembro. 2022.*

CONCLUSÃO

Não há indicação de que a cadência de ataques cibernéticos contra a Ucrânia esteja diminuindo, nem o conflito cibernético necessariamente terminará com a interrupção das hostilidades. As tensões regionais e a diversidade dos agentes de ameaças envolvidos no conflito sugerem que os ataques contra a Ucrânia provavelmente continuarão. Além disso, avaliamos que os agentes de ameaças digitais na Rússia provavelmente realizarão ataques destrutivos, conforme necessário, para afetar o resultado da guerra.

