CERT-UA avisa que UAC-0245 tem como alvo a Ucrânia com backdoor CA

Data: 2025-10-02 18:02:27

Autor: Inteligência Against Invaders

CERT-UA avisa que UAC-0245 tem como alvo a Ucrânia com backdoor CABINETRAT

O CERT-UA avisa que o UAC-0245 tem como alvo a Ucrânia com o backdoor CABINETRAT por meio de suplementos maliciosos do Excel XLL detectados em setembro de 2025.

A Equipe de Resposta a Emergências de Computadores da Ucrânia (CERT-UA) alertou sobre ataques cibernéticos do grupo UAC-0245 usando o backdoor CABINETRAT. A campanha, vista em setembro de 2025, envolvia suplementos maliciosos do Excel XLL que se passavam por ferramentas de software (por exemplo, “UBD Request.xll”, “recept_ruslana_nekitenko.xll”).

Os arquivos são executáveis (PE, Portable excutable) que podem ser carregados pelo Excel Add-in Manager usando o procedimento (função exportada) “xlAutoOpen”.

Os indivíduos visados relataram que os invasores tentaram espalhar o arquivo malicioso “500.zip” via Signal, disfarçando-o como um documento de detenção de fronteira na Ucrânia.

“Posteriormente, foi recebida uma mensagem dos participantes da troca de informações sobre a gravação de uma tentativa de distribuir o arquivo “500.zip” usando o Signal sob o disfarce de um documento sobre a detenção de pessoas que tentavam cruzar a fronteira do estado da Ucrânia.” lê-se no relatório *publicado pelo CERT-UA.*

Quando iniciado, o XLL solta um EXE na pasta de inicialização, um XLL chamado “BasicExcelMath.xll” em %APPDATA% e um PNG chamado “Office.png”. Em seguida, ele modifica o Registro do Windows para manter a persistência, inicia o Excel no modo oculto e executa o suplemento XLL. O XLL extrai e executa o código shell CABINETRAT do arquivo PNG.

A carga útil XLL e seu código shell incluem verificações anti-análise. Eles verificam a presença de pelo menos dois núcleos de CPU e 3 GB de RAM e plataformas de virtualização (VMware, VirtualBox, Xen, QEMU, Parallels, Hyper-V), para evitar a detecção. Eles também verificam se o SID do usuário não termina com “500”; e verifique o sinalizador de depuração PEB.

“Considerando a novidade de táticas, técnicas e procedimentos, e não levando em conta os casos conhecidos de uso de arquivos XLL em ataques cibernéticos direcionados realizados pelo UAC-0002 grupo, em particular, contra instalações de infraestrutura crítica na Ucrânia, um identificador separado UAC-0245 foi criado para rastrear a atividade descrita.” continua o relatório.

CABINETRAT é uma ferramenta de código shell escrita em C que reúne dados do sistema

operacional e do programa instalado. O código malicioso executa comandos, manipula arquivos, faz capturas de tela e se conecta a um C2 sobre TCP. Ele primeiro sonda as portas 18700, 42831, 20046 e 33976 (tipo porta).

A maioria das mensagens é compactada com MSZIP e dividida se for muito grande. Principais tipos de mensagens:

- **0**: aperto de mão (“Ninja” ? servidor responde “Bonjour”)
- **1**: executar um programa e enviar resultados
- **2**: saída do comando send
- **4**: enviar um arquivo solicitado para o servidor (exfiltrar)
- **5**: receber e salvar um arquivo do servidor
- **6**: enviar GUIDs do BIOS após o handshake
- **7**: enviar informações da versão do sistema operacional (do registro do Windows)
- **8**: relatar discos conectados
- **9**: Listar programas instalados (chaves de desinstalação do registro)
- **10**: listar conteúdo do diretório (caminho + máscara de pesquisa)
- **11**: tire e envie uma captura de tela
- **12**: enviar um código de erro
- **13**: excluir um arquivo ou pasta

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,Ucrânia)