O novo carregador “CountLoader” usa PDFs para iniciar ataques de ranso

Data: 2025-09-19 07:29:33

Autor: Inteligência Against Invaders

Os pesquisadores de segurança descobriram um sofisticado novo carregador de malware chamado

“CountLoader” que aproveita os arquivos PDF armas para fornecer cargas úteis de ransomware às

vítimas em várias regiões, com foco particular em metas ucranianas.

O CountLoader representa uma escalada significativa nas técnicas de entrega de malware, operando através de três versões distintas: .NET, PowerShell e JScript implementações.

O carregador de malware foi diretamente ligado a vários grupos de ransomware proeminentes, incluindo Lockbit**Assim,** Blackbasta e Qilin, demonstrando a natureza interconectada das operações cibernéticas modernas.Paste.txt

Analistas silenciosos de ameaça que descoberto e nomeado o malware avaliar com confiança média-alta que o CountLoader serve como uma ferramenta ou funções de corretor de acesso inicial (IAB) como parte do arsenal de um afiliado de ransomware.

Esta avaliação é baseada em evidências técnicas que conectam os agentes descartados do CountLoader às amostras de malware observadas em vários incidentes de ransomware.Paste.txt

A sofisticada metodologia de segmentação do ator de ameaças tornou-se evidente por meio de uma campanha de atração baseada em PDF, projetada especificamente para se passar pela polícia ucraniana.

O PDF malicioso, distribuído em um arquivo .zip chamado “Vymoha_NA_YAVKU” (convoca a aparecer), apresenta às vítimas um documento de aparência oficial supostamente da “Polícia Nacional da Ucrânia”, solicitando sua aparição para interrogatório.

No banco de dados de malware de Urlhaus, Urlhaus[.]abuso[.]CH, nossa equipe encontrou vários domínios rotulados como “entregando o Vidar InfoStealer e Emmenhtal Malware”, de acordo com os repórteres iniciais.

Essa técnica de engenharia social explora as tensões geopolíticas atuais para aumentar a probabilidade de interação da vítima.Paste.txt

Capacidades técnicas avançadas

A versão JScript do CountLoader se destaca como a implementação mais abrangente, contendo aproximadamente 850 linhas de código com extensa funcionalidade.

No final deste processo, o CountLoader inicia seu loop principal. O loop é executado uma vez e continua a funcionar enquanto o valor “Iniciar” for definido no caminho da execução do HTA.

O malware emprega seis métodos diferentes para download de arquivos e três técnicas distintas de execução, demonstrando o profundo entendimento dos desenvolvedores dos sistemas operacionais do Windows e das técnicas de evasão defensiva.Paste.txt

A infraestrutura de comando e controle utiliza um algoritmo sofisticado de geração de domínio, tentando conexões com domínios numerados sequencialmente seguindo o padrão “MS-Team-Ping[number].com. ”

Os implementos de malware são mecanismos de tentativa persistentes, tentando até um milhão de tentativas de conexão em vários Servidores C2. Todas as comunicações empregam criptografia XOR com a codificação BASE64, usando uma chave de seis caracteres extraída do servidor Responses.Paste.txt.

Se o CountLoader receber a sequência “Sucesso” de uma C2, ela continuará sua operação principal.

Os mecanismos de persistência do carregador incluem modificações de registro e criação de tarefas programadas.

O CountLoader estabelece a persistência através da tecla Windows Run em “HKCU Software Microsoft Windows CurrentVersion Run OneDRiver” e cria tarefas programadas com nomes projetados para se representar processos de atualização do Google Chrome, como “GoogleUskSaskSystem135.0.7023.”

Conexões de ransomware

A análise da entrega da carga útil do contador revelou vários alvos de alto valor, com sistemas de domínio recebendo tratamento prioritário.

A função exclusiva é usada aqui para definir a string recebida anteriormente da fase de conexão como o cabeçalho do portador de autorização para esta solicitação.

Os ambientes corporativos receberam consistentemente tarefas adicionais de reconhecimento, incluindo comandos de enumeração do domínio do Windows e coleta de informações do sistema.

Os estágios de malware baixaram cargas úteis principalmente nas pastas “musica” dos usuários, uma escolha incomum que se alinha com táticas anteriormente observadas em campanhas.poste.txt

As cargas úteis capturadas incluem beacons de greve de cobalto, implantes de adapxc2, ferramentas de acesso remoto PureHVNC e malware de coleta de informações da LUMMA.

A análise técnica revelou específica Greve de cobalto Marcas aquáticas (1473793097 e 1357776117) que os pesquisadores de segurança já haviam vinculado as operações de Ransomware Blackbasta, Qilin e Lockbit, estabelecendo conexões claras entre o CountLoader e o Ransomware estabelecido Ecosystems.Paste.txt

A análise de infraestrutura descobriu padrões consistentes nas operações do ator de ameaças,

incluindo convenções de nomeação de subdomínio padronizadas usando prefixos “SSO” e “login” projetados para misturar tráfego malicioso com comunicações corporativas legítimas.

Essa abordagem sugere recursos automatizados de geração de infraestrutura e maturidade operacional.Paste.txt

Mitigações

As organizações devem priorizar a implementação do monitoramento abrangente para indicadores de contador do carregador, particularmente aqueles freqüentemente direcionados por grupos cibernéticos russos ou atores de ameaças persistentes avançadas.

O uso de malware de utilitários legítimos do Windows como certutil, bitsadmin e Powershell Para a entrega da carga útil, requer análise comportamental, em vez de abordagens de detecção baseadas em assinatura.

As equipes de segurança de rede devem monitorar o padrão de URI “/API/getFile?

Além disso, o monitoramento para tentativas seqüenciais de geração de domínio e atividade incomum nos diretórios de “música” dos usuários podem fornecer indicadores de aviso antecipados.Paste.txt

As configurações de segurança de email devem incluir recursos aprimorados de análise em PDF, principalmente para documentos contendo scripts incorporados ou referências externas.

A campanha de representação policial ucraniana demonstra a importância da conscientização cultural e regional na inteligência de ameaças, à medida que os invasores alavancam cada vez mais eventos geopolíticos para melhorar a eficácia da engenharia social.

A descoberta do CountLoader destaca a sofisticação em evolução dos mecanismos de entrega de malware e ressalta a importância crítica de estratégias defensivas de várias camadas no combate operações de ransomware que abrangem vários grupos de atores de ameaças e regiões geográficas.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.