# CastleBot MaaS lançou diversas cargas úteis em ataques coordenados de

Data: 2025-08-09 08:07:39

Autor: Inteligência Against Invaders

O IBM X-Force descobriu o CastleBot, uma estrutura de malware nascente que opera como uma plataforma Malware-as-a-Service (MaaS), permitindo que os cibercriminosos implantem um espectro de cargas úteis que variam de infostealers a backdoors sofisticados implicados em operações de ransomware.

Detectado pela primeira vez no início de 2025 com maior atividade desde maio, o CastleBot facilita a entrega de ameaças como Suporte de rede e WarmCookie, que têm laços históricos com ataques de ransomware.

A flexibilidade dessa estrutura permite que os operadores filtrem vítimas, gerenciem infecções e direcionem com precisão ativos de alto valor, coletando dados de enumeração de host, como nomes de usuário, nomes NetBIOS, arquitetura do sistema e IDs de vítimas exclusivos calculados por meio de um gerador congruente linear a partir de números de série de volume.

O componente principal do malware se comunica com servidores de comando e controle (C2) usando contêineres serializados criptografados pelo ChaCha por HTTP, solicitando tarefas que podem incluir várias cargas úteis em uma única campanha, complicando assim os métodos tradicionais de detecção.

## Cenário de malware como serviço

A cadeia de infecção do CastleBot começa com instaladores de software trojanizados distribuídos por meio de sites falsos reforçados por Envenenamento de SEO, em que as páginas maliciosas superam as legítimas nos resultados de pesquisa.

Também foi observado aproveitando os repositórios do GitHub que se passam por software válido e a técnica ClickFix para atrair usuários.

A arquitetura de três estágios compreende um stager de código shell leve que baixa e descriptografa cargas úteis usando chaves XOR como “GySDoSGySDoS”, seguido por um carregador que mapeia seções PE, resolve importações e manipula estruturas PEB_LDR_DATA para imitar o carregamento legítimo do módulo, evitando ferramentas de detecção e resposta de endpoint (EDR).

De acordo com o relatório, O backdoor principal, empregando hash de AP para resolução de API, descriptografa sua configuração, incluindo IDs de campanha e chaves ChaCha e se registra no C2 enviando dados criptografados do host.

As tarefas são executadas com base em métodos de inicialização, como injeção de processo por meio de gancho NtManageHotPatch para ignorar verificações Windows 11 24H2 ou persistência por meio de tarefas agendadas usando a interface COM ITaskService.

Atualizações recentes em julho de 2025 introduziram aprimoramentos como desvio WOW64 para binários de 32 bits e métodos de inicialização expandidos, incluindo execução de MSI por meio de msiexec.exe e injeção avançada usando QueueUserAPC para chamadas de API reduzidas.

As campanhas analisadas pela X-Force revelam diversas cargas úteis: uma cadeia começando com um instalador SSMS armado descriptografa o CastleBot via Dave Loader, implantando o WarmCookie de um C2 em 170.130.165.112; outro entrega Rhadamanthys, Remcos e DeerStealer em sequência.

As implantações do NetSupport exploram o ClickFix em sites falsos do DocuSign, enquanto outras envolvem SecTopRAT, HijackLoader e MonsterV2, geralmente por meio de arquivos ZIP e sideload de DLL.

A natureza orientada por afiliados desse modelo MaaS, com distribuição privada, ressalta seu potencial de escalar para ransomware, como visto nos laços com os alvos da Operação Endgame.

## Evolução contínua

À medida que o CastleBot evolui, incorporando verificações anti-VM, mensagens de erro falsas e técnicas de injeção adaptativa, os defensores devem priorizar EDR atualizado, treinamento de usuários contra downloads não verificados, autenticação multifator e bloqueio de tráfego de saída não HTTPS.

A X-Force antecipa mais refinamentos para combater as medidas de segurança, sinalizando uma mudança em direção a vetores de acesso inicial dinâmicos e envenenados por SEO no cibercrime.

## Indicador de Comprometimento (IoCs)

| Tipo de indicador | Indicador | Contexto |
|---|---|---|
| URL | http://173.44.141.89/service/ | Servidor CastleBot C2 |
| URL | http://mhousecreative.com/service/ | Servidor CastleBot C2 |
| SHA256 | 202f6b6631ade2c41e4762e5877ce0063a3beabce0c3f8564b6499a1164c1e04 | Núcleo do CastleBot |
| SHA256 | 5bca7f1942e07e8c12ecd9c802ecdb96570dfaaa1f44a6753ebb9ffda0604cb4 | Carga útil do WarmCookie |
| IPv4 | 170.130.165.112 | Servidor WarmCookie C2 |

**Ache esta notícia interessante! Siga-nos no**Google Notícias**,**LinkedIn**, &**X**para obter atualizações instantâneas!**