Whitepaper: Evasão de EDR em 2026

Discussão técnica sobre tendências de detecção e evasão em ambientes monitorados, com foco em execução em memória, telemetria de processo e operação de baixo ruído.

Autor principal	David Chang - Head of Offensive Security
Apoio técnico	Sarah Jenkins - Lead Cloud Engineer
Versão	1.3 - release externa
Publicação	Março de 2026
Status	Aprovado para divulgação

Nota: este documento descreve padrões técnicos observados em pesquisas públicas e em exercícios controlados de Red Team. O objetivo é apoiar entendimento defensivo e avaliação de riscos.

1. Mudança de foco nas detecções

Produtos de EDR continuam evoluindo a partir de três frentes principais: correlação de processo, inspeção de memória e telemetria de rede. Isso reduziu a efetividade de abordagens ruidosas baseadas em script, APIs amplamente monitoradas e padrões previsíveis de injeção remota.

Em 2026, a discussão mais relevante deixou de ser 'qual técnica bypassa o produto X' e passou a ser 'quanto ruído operacional cada cadeia de execução gera'. Em outras palavras, o sucesso de um implante está menos ligado a um truque isolado e mais à coerência entre execução, contexto e volume de telemetria produzida.

2. Pontos de atenção recorrentes

- Resolução dinâmica de APIs e redução de dependência em funções frequentemente instrumentadas.
- Uso disciplinado de memória e cuidado com sequências clássicas de alocação, escrita e execução.
- Telemetria de rede com intervalos e tamanhos próximos do comportamento esperado do ambiente.
- Evitar cadeias de execução que produzam sinais fáceis de correlacionar entre endpoint, autenticação e rede.

Trecho ilustrativo

```
// Trecho ilustrativo: execução com menor dependência de APIs de alto nível
NTSTATUS status = Custom_NtAllocateVirtualMemory( hProcess, &remoteBuffer,
0,
&payloadSize,
MEM_COMMIT | MEM_RESERVE,
PAGE_READWRITE
);

// Etapas posteriores, como escrita, alteração de proteção e início de execução, // devem
ser avaliadas em conjunto com o contexto operacional e a telemetria produzida.
```

3. Implicações defensivas

Do ponto de vista defensivo, ETW, visibilidade de memória, contexto do binário executado e eventos associados à criação de threads continuam sendo fontes valiosas quando bem correlacionadas. Controles maduros combinam esses sinais com identidade, rede e histórico de mudanças para priorizar respostas.

Para organizações que executam simulações de adversário, a principal recomendação é medir resultados por ruído operacional, tempo de detecção e qualidade de correlação, e não apenas por obtenção de acesso inicial.

4. Referências do laboratório

Parte das pesquisas internas da OceanSec Labs é consolidada em repositórios técnicos utilizados em exercícios controlados e validação de hipóteses de detecção. Versões públicas e materiais derivados passam por revisão editorial e sanitização antes da divulgação.

Contato para imprensa técnica: press@oceansec.com | Revisão editorial: Lúcia Mendes | Referência interna: OSL-RT-2026-WP-13