AV/EDR Bypass Técnicas para novos hackers

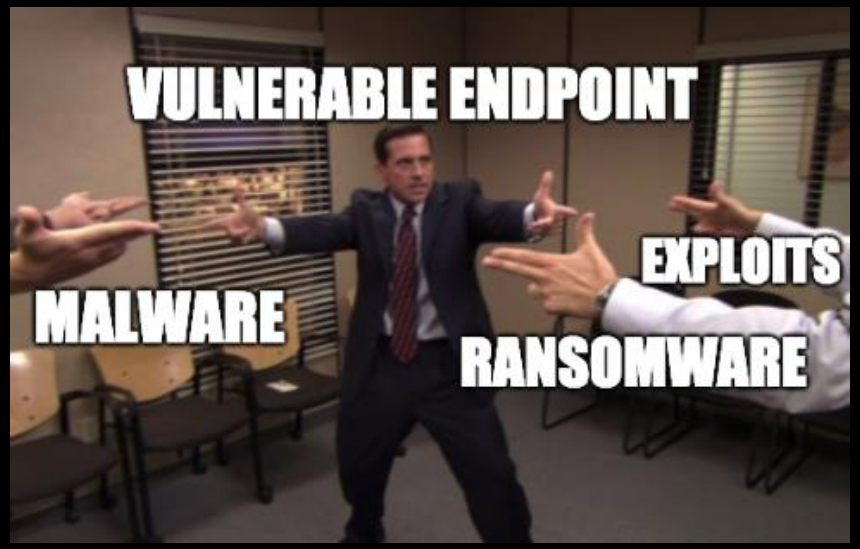
Joas Antonio (C0d3Cr4zy)

Whoami

- Joas Antonio (C0d3Cr4zy)
- 19 years – Brazil, São Paulo
- Asperger
- PenTester na Inmetrics
- Information Security Research
- Mentor de segurança cibernética
- Red Team Village, Mitre, Womcy, Hacker Culture, Hacker is NOT Crime, Texas Cyber Security Summit Contributor
- CEH Master, OSWP, eJPT e OSCP (em andamento)

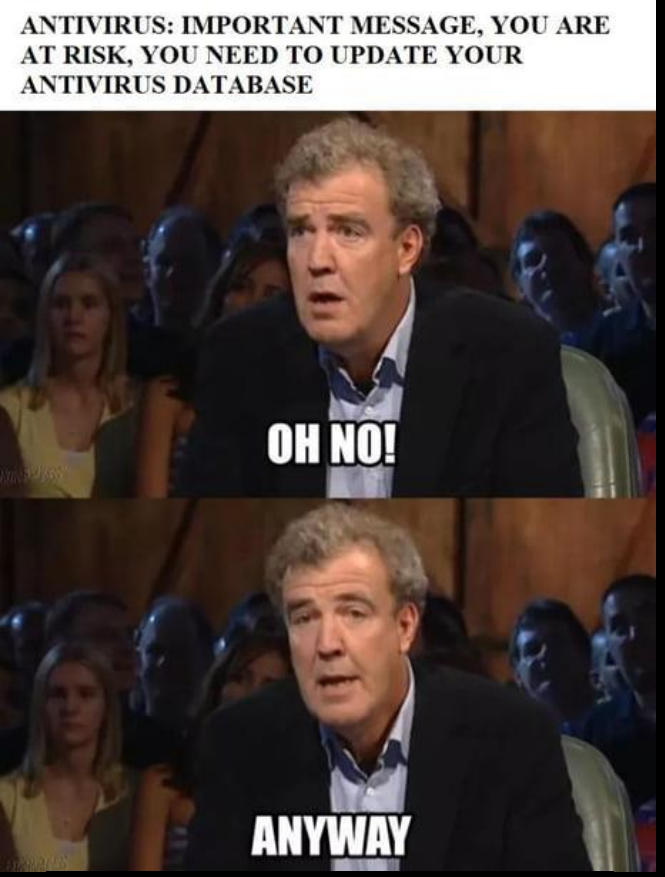
O que é EDR e AV?

Conceitos



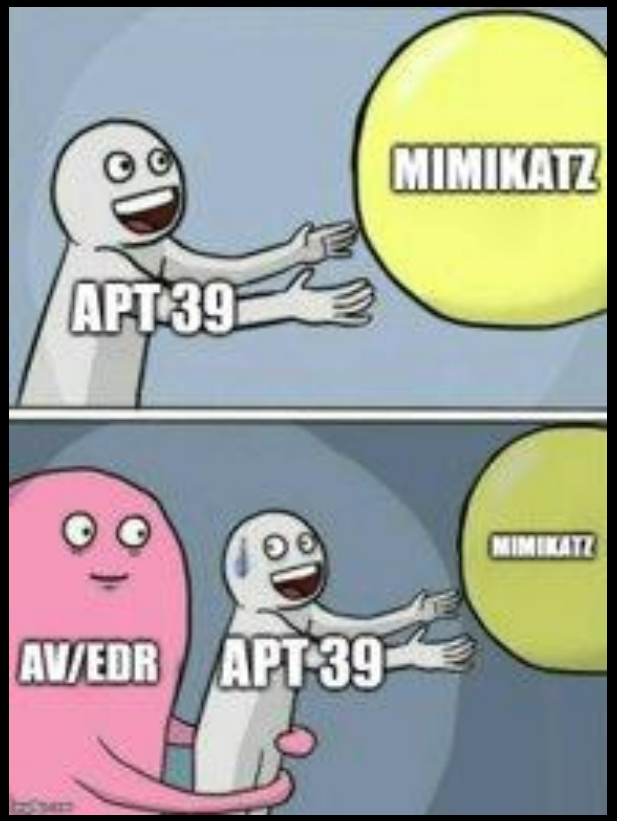
O que é EDR?

- Endpoint Detection and Response (EDR), também conhecido como Endpoint Threat Detection and Response (ETDR), é uma tecnologia cibernética que monitora e responde continuamente para mitigar ameaças cibernéticas;
- A tecnologia EDR é usada para proteger endpoints, que são dispositivos de hardware de computador, contra ameaças. Os criadores das plataformas baseadas na tecnologia EDR implantam ferramentas para coletar dados de dispositivos terminais e, em seguida, analisam os dados para revelar possíveis ameaças e problemas cibernéticos. É uma proteção contra tentativas de hacking e roubo de dados do usuário. O software é instalado no dispositivo do usuário final e é constantemente monitorado. Os dados são armazenados em um banco de dados centralizado. Em um incidente quando uma ameaça é encontrada, o usuário final é imediatamente avisado com uma lista de ações preventivas;



O que é AV?

- Definição: Software criado especificamente para ajudar a proteger, detectar, prevenir e remover malware (software malicioso);
- Antivírus é um tipo de software usado para prevenir, escanear, detectar e excluir vírus de um computador. Depois de instalado, a maioria dos softwares antivírus é executada automaticamente em segundo plano para fornecer proteção em tempo real contra ataques;
- Programas de proteção abrangente contra vírus ajudam a proteger seus arquivos e hardware contra malwares, como worms, cavalos de Tróia e spyware, e também podem oferecer proteção adicional, como firewalls personalizáveis e bloqueio de sites;



AV x EDR

- Os antivírus tradicionais são mais simplistas e limitados em comparação com os sistemas EDR modernos. O antivírus pode ser percebido como parte do sistema EDR.
- Geralmente, o antivírus é um único programa que atende a propósitos básicos como varredura, detecção e remoção de vírus e diferentes tipos de malware.
- O sistema de segurança EDR, por outro lado, desempenha um papel muito maior. O EDR não inclui apenas antivírus, mas também contém muitas ferramentas de segurança como firewall, ferramentas de lista branca, ferramentas de monitoramento, etc. para fornecer proteção abrangente contra ameaças digitais. Geralmente é executado no modelo cliente-servidor e protege os vários endpoints da rede digital de uma empresa e mantém os endpoints seguros.

Bypass AV/EDR

Conceitos e Técnicas

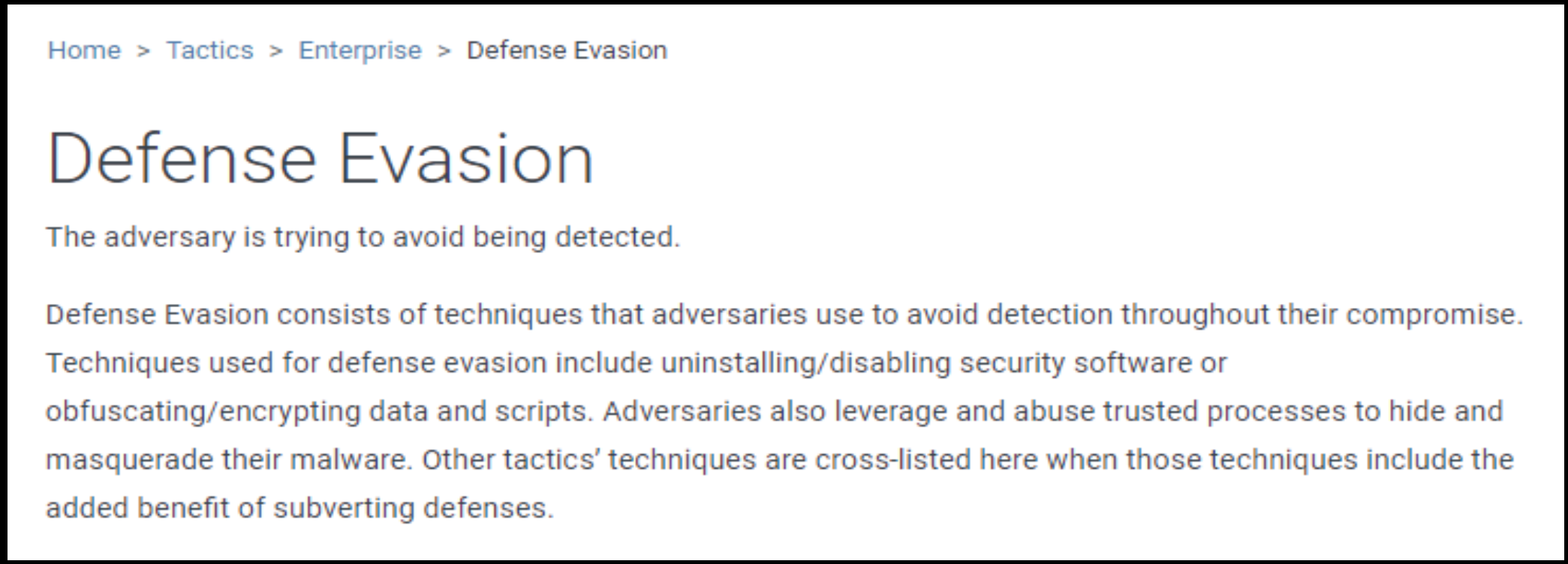
Bypass AV/EDR

Contornar a proteção de um antivírus ou EDR não é uma tarefa simples, requer um certo conhecimento.

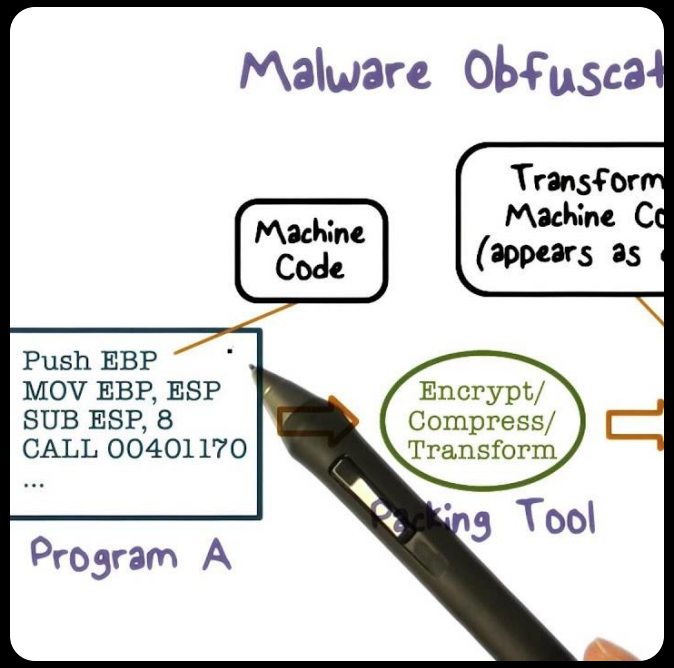
1. Saber como as soluções funcionam;
2. Saber o sistema operacional em que a solução está instalada;
3. Como o sistema operacional e a solução se comportam juntos;
4. Conhecer as técnicas de Bypass mais simples, envolvendo vetores de ataque simples, técnicas ainda mais robustas com vetores mais avançados;
5. Conhecimento de programação é essencial, seja de alto nível como (Python, Go, Ruby e C#), linguagens C e C ++ e o nível mais baixo como assembly;
6. Conceito de API e Sysinternals do Windows.

Bypass AV/EDR - Mitre Att&ck

Mitre Att&ck ajuda você a se aprofundar em técnicas para contornar os mecanismos de defesa, recomendo acessar o site e explorar: https://attack.mitre.org/tactics/TA0005/



Bypass AV - Técnicas (Ofuscação)



- Duas maneiras comuns de os hackers mitigarem a detecção de antivírus são ofuscação e criptografia.
- A ofuscação simplesmente distorce o malware enquanto mantém sua forma. Um exemplo simples seria o caso dos caracteres em um script do PowerShell. A função é a mesma, o PowerShell não se preocupa com o caso dos caracteres , mas pode enganar a digitalização baseada em assinatura simples. Na verdade, Blackhills escreveu sobre um exemplo bem conhecido de ofuscação que envolve todos os Mimikatz Mimidogz, "along strings". Este simples é surpreendentemente eficaz, pois evita com sucesso o antivírus.
- Como prova de conceito, o script powerhell ofuscado “InvokeMimidogz”, com algumas strings comuns alteradas, foi obtido e ofuscado usando a ferramenta de código aberto maravilhosamente poderosa, InvokeObfuscation, escrita por Daniel Bohannon em 2016. Esta ferramenta e o script PowerShell ofuscado já existem há vários anos, mas nossa equipe na LMG Security executa regularmente e com êxito o Invoke Mimikatz em hosts que executam soluções antivírus como Kaspersky e Windows Defender.

Bypass AV/EDR - Técnicas (C2 e Ofuscação)

Um dos métodos que costumo usar é Trevor C2 + Pyfuscation, ofuscando o agente no Powershell usando Pyfuscation eu fui capaz de contornar até EDR e AV como o Kaspersky Endpoint Security for Windows

```
root@kali:/home/joas/trevorc2/agents# ls
c  test  trevorc2_client.cs  trevorc2_client.java  trevorc2_client.ps1  trevorc2_client.py
root@kali:/home/joas/trevorc2/agents#
```

Agora vamos usar Pyfuscation para observar variáveis, strings e parâmetros

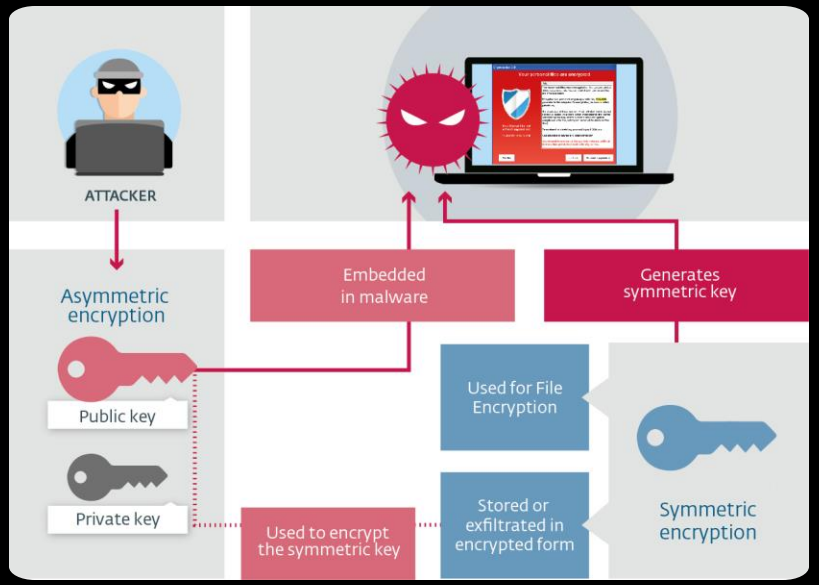
```
root@kali:/home/joas/PyFuscation# python3 PyFuscation.py -fvp --ps payload2.ps1
```

```
[+] Variables Replaced   : 24
[-] Obfuscated Variables located  : /03032021_12_45_17/03032021_12_45_17.variables
[+] Parameters Replaced  : 0
[-] Obfuscated Parameters located : /03032021_12_45_17/03032021_12_45_17.parameters
[+] Functions Replaced   : 2

Obfuscated Function Names

[*] Replaced connect-trevor With: KFC
[*] Replaced random_interval With: parquetry

[-] Obfuscated Functions located  : /03032021_12_45_17/03032021_12_45_17.functions
[-] Obfuscated script located at  : /03032021_12_45_17/03032021_12_45_17.ps1
```

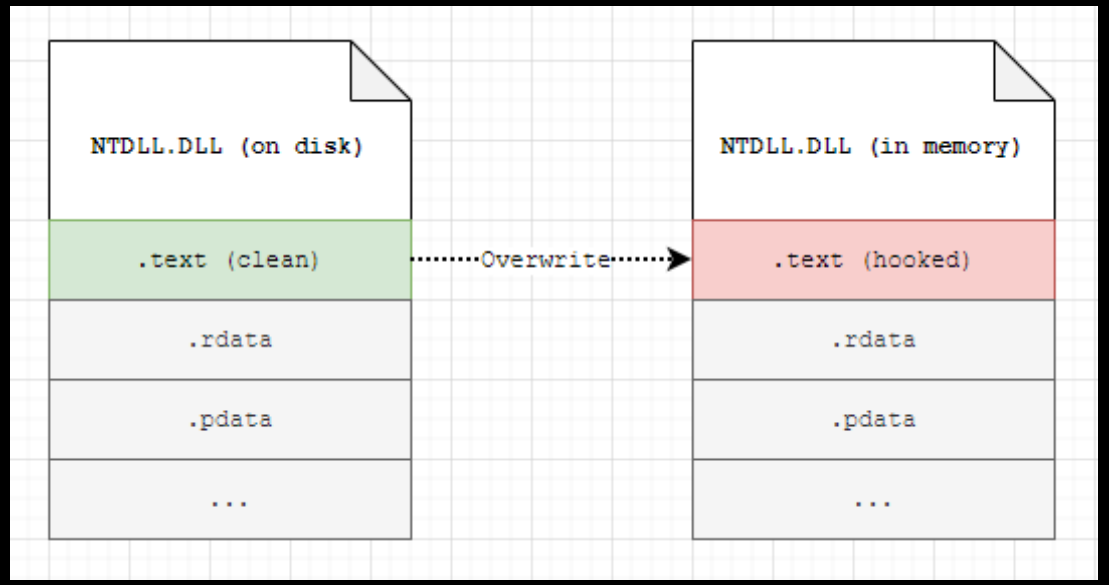


Bypass AV/EDR - Técnicas (Encriptação)

- O segundo método é a criptografia. Esse metódo elimina efetivamente a capacidade do antivírus de detectar malware apenas por meio da assinatura. Os autores de malware geralmente usam "criptografadores" para criptografar suas cargas maliciosas. Eles criptografam um arquivo e anexam um 'Stub', um programa que irá descriptografar o conteúdo e, em seguida, executá-lo.
- Existem dois tipos de criptografadores: ‘scantime’ e ‘runtime’.
- Os criptografadores Scantime são os mais ingênuos e simplesmente descriptografam o payload, colocando-o no disco e o executando.
- Os criptografadores runtime usam várias técnicas de injeção de processo para descriptografar o payload malicioso e executá-lo na memória, nunca tocando o disco.

Bypass AV/EDR - Técnicas (Desengate de DLL completo com C ++)

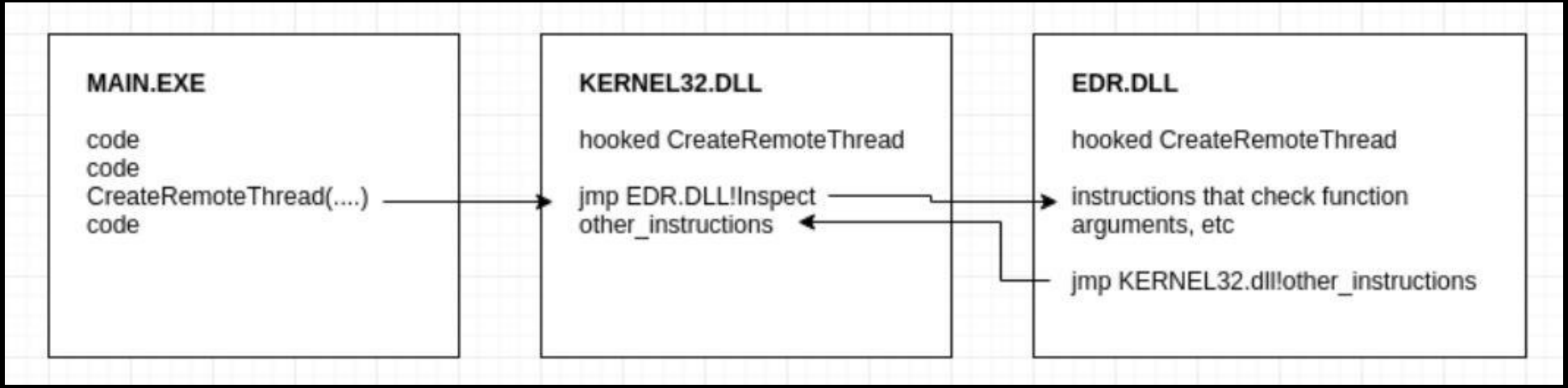
- É possível desenganchar completamente qualquer DLL carregada na memória, lendo a seção .text de ntdll.dll do disco e colocando-a no topo da seção .text de ntdll.dll que está mapeada na memória. Isso pode ajudar a evitar algumas soluções de EDR que dependem do hooking da API do usuário.
- Abaixo está um gráfico simplificado, ilustrando o conceito central da técnica, onde uma seção .text conectada de ntdll.dll é substituída por uma cópia limpa da seção .text de ntdll.dll do disco:



Bypass AV/EDR - Técnicas (Corrigindo o patch)

- Aqui estão as postagens do blog de @SpecialHoang e MDsec no início de 2019 explicando como contornar o software AV / EDR corrigindo o patch:
- https://medium.com/@fsx30/bypass-edrs-memory-protection-introduction-to-hooking-2efb21acffd6
- https://www.mdsec.co.uk/2019/03/silencing-cylance-a-case-study-in-modern-edrs/
- Se o seu implante ou ferramenta carregar algumas funções do kernel32.dll ou NTDLL.dll, uma cópia do arquivo de biblioteca será carregada na memória. Os fornecedores de AV / EDR normalmente corrigem algumas das funções da cópia na memória e colocam uma instrução JMP assembler no início do código para redirecionar a função API do Windows para algum código de inspeção do próprio software AV / EDR. Portanto, antes de chamar o código de função real da API do Windows, é feita uma análise. Se essa análise não resultar em comportamento suspeito / malicioso e retornar um resultado limpo, a função da API do Windows original é chamada posteriormente. Se algo malicioso for encontrado, a chamada da API do Windows será bloqueada ou o processo será encerrado

Bypass AV/EDR - Técnicas (Corrigindo o patch)



- Ambas as postagens do blog se concentram em contornar o software EDR CylancePROTECT e construir um código PoC para este software específico. Ao corrigir a instrução JMP adicional do NTDLL.dll manipulado na memória, o código de análise do Cylance nunca será executado.
- Uma desvantagem dessa técnica é que você pode ter que alterar o patch para cada fornecedor de AV / EDR diferente. Não é muito provável que todos eles coloquem uma instrução JMP adicional na frente das mesmas funções no mesmo ponto. Eles provavelmente irão ligar funções diferentes e talvez usar outro local para o patch.

Bypass AV/EDR - Técnicas (AV Bypass com modelos Metasploit e binários personalizados)

- Podemos recompilar os payloads que usamos para inserir nosso próprio shellcode, até mesmo modificando um modelo simples. Veja um exemplo que tirei de ired.team
- Ao gerar payloads metasploit, nosso shellcode especificado é injetado nos binários do modelo. O payload que geramos anteriormente foi injetada no modelo para o qual o código-fonte é fornecido abaixo.
- Se fizermos algumas pequenas alterações no código para tamanhos de alocação de memória:

```
root@/usr/share/metasploit-framework/data/templates/src/pe/exe# cat template.c
#include <stdio.h>

#define SCSIZE 4096
char payload[SCSIZE] = "PAYLOAD:";

char comment[512] = "";

int main(int argc, char **argv) {
        (*(void (*)()) payload)();
        return(0);
}
```

```
1   #include <stdio.h>
2
3   #define SCSIZE 4000
4   char payload[SCSIZE] = "PAYLOAD:";
5   char comment[712] = "";
6
7   int main(int argc, char **argv) {
8       (*(void (*)()) payload)();
9       return(0);
10  }
```

- Recompile e gere o payload usando o modelo recém-compilado com MSFVENOM

AV/EDR - Conclusão

- São inúmeras as técnicas para você contornar o AV / EDR, se eu fosse falar de todas elas provavelmente ficaria o dia todo e não saberia explicar nem a metade, porque são infinitas possibilidades;

- Os invasores usam essas técnicas + vetores de ataque para comprometer seus alvos; atualmente, o mais comum são os ataques de phishing para obter o primeiro acesso;

- Vou deixar alguns materiais e cursos para vocês que desejam se aprofundar no final desta apresentação;

AV/EDR - Estudos

https://s3cur3th1ssh1t.github.io/

https://www.ired.team/offensive-security/defense-evasion/

https://attack.mitre.org/tactics/TA0005/

https://www.offensive-security.com/pen300-osep/

https://www.youtube.com/watch?v=mJZCNqcO10A&t=2s&ab_channel=RedTeamVillage (Filipe Pires)

https://github.com/Techryptic/AV_Bypass

https://blog.f-secure.com/av-bypass-techniques-through-an-edr-lens/

https://www.youtube.com/watch?v=MO11gJ-WJqY&ab_channel=BlackHat (AVPASS: Leaking and Bypassing Antivirus Detection Model Automatically)

https://www.youtube.com/watch?v=2HNuzUuVyv0&ab_channel=BlackHat (Red Team Techniques for Evading, Bypassing & Disabling MS)

AV/EDR - Ferramentas

https://github.com/Ch0pin/AVIator

https://github.com/CBHue/PyFuscation

https://github.com/yeyintminthuhtut/Awesome-Red-Teaming#-defense-evasion

https://github.com/Veil-Framework/Veil-Evasion

https://www.shellterproject.com/

https://github.com/leechristensen/UnmanagedPowerShell

https://github.com/S3cur3Th1sSh1t/Amsi-Bypass-Powershell

https://github.com/danielbohannon/Invoke-Obfuscation

https://www.offensive-security.com/metasploit-unleashed/msfvenom/

https://www.ollydbg.de/

https://github.com/infosecn1nja/Red-Teaming-Toolkit (Repo Tools Red Team)

Thank you so much for the opportunity

Muito obrigado pela oportunidade

My LinkedIn Qrcode

Joas Antonio (C0d3Cr4zy)