Aula 05

Engenharia Reversa e Análise de Malware

Ronaldo Pinheiro de Lima
crimescibernéticos.com@gmail.com

Aula 05

4. Trabalhando com Executáveis

4.1. Identificação do arquivo

4.2. Unpacking Automático

4.3. Strings

4.4. Strings criptografadas

4.5. Debugging

4.6. Lab 04-01
Análise de executável malicioso com strings criptografadas

Trabalhando com executáveis

- análise costuma seguir etapas pré-estabelecidas
- técnicas de análise estática

Identificação do arquivo

- obter perfil inicial do arquivo
- utilizar mais de uma ferramenta
- Exeinfo PE: dicas de unpacking
- PEiD, RDG e file

Unpacking automático

- remover proteções
- > popularidade do packer + fácil unpacker
- seguir dica do Exeinfo PE
- buscar “unpack nome_do_packer”
- cuidado com sites undergrounds
- após unpacking - novamente os identificadores
- muitas vezes mesmo os unpackers não funcionam
- analisar o custo/benefício

Strings

- sequência de caracteres
- mensagens, URLs, conexão com db, caminhos de arquivos, chaves do registro
- terminador NULL
- ASCII = 1 byte

M	A	L	W	A	R	E	NULL
4D	41	4C	57	41	52	45	00

- UNICODE = 2 bytes

M		A		L		W		A		R		E		NULL	
4D	00	41	00	4C	00	57	00	41	00	52	00	45	00	00	00

Strings criptografadas

- comum nos trojans-bankers brasileiros
- função que descriptografa logo abaixo da string

```
UNICODE "012258464142447919694746476D5255445C5C555C1F535D5B1D554318
UNICODE "008260716A0568737B17646309080301006A770701037273067l0F017C
UNICODE "009858464142447919694746476D5255445C5C555C1F535D5B1D554318
UNICODE "005258464142447919694746476D5255445C5C555C1F535D5B1D5543"
UNICODE "005258464142OD6C193147461E214351545C43535E1F535D5B1D5543"
UNICODE "004458464142OD6C19244250542642535F17535F5C1F5240"
```

```
ASCII "P2rTeYmP65yCFhR6vcrYfO8BM4EY5Bw0"
ASCII "v+SC9xwibakY1Gvv1h37WFHCDVtgd0qGUXtUSB62ibz0psl/p+CbWg=="
ASCII "fpodg/YPZMiUzNfBXFlOXuxue9cNqYGo"
ASCII "AY7Gv4P5UC8QZXDu+I2NY0P4wg7CpSrrhtwB5saUYt0="
ASCII "nhqnII1f6g9NnF6+IJOiI1zUXee6vaiY"
ASCII "/7WLhq6efUknPP9pizgllvQ0UB1LWQEcQojTrZgzORdWedKAzoR57g=="
ASCII "V75iWN8gWEBr3h8P5PR/hrYmtJQVxxth"
ASCII "zRNthrwmr3yMB/gx1QJ567Scv9tJ3a9M1LA9Wcc/7Sf/zWT7jkDdnA=="
ASCII "rGmnrsXdkuYH16HMVV8Uzoe8ICbttz1w"
```

Debugging

- auxilia na execução de trechos de código
- permite alterar instruções e valores em tempo real
- navegar no código

Lab 04-01

Análise de executável malicioso com strings criptografadas

Material necessário:

- VM
- PEiD, Exeinfo PE
- strings.exe
- UPX
- OllyDbg
- Arquivo: Lab-04-01.scr

Obrigado!

A explicação detalhada de todos os tópicos está na apostila.

Ronaldo Pinheiro de Lima
crimescibernetico.com@gmail.com
http://www.crimescibernetico.com
@crimescibernet