Tatort Internet

Wer geht mit mir phishen?

Sebastian Neuner Michael Rodler

2010-11-25

Vorstellung

Sebastian Neuner

- Student SIB09
- Tiroler – aka Sebaschtian
- Pentester/CTF-Team h4ck!nb3rg

Michael Rodler

- Student SIB09
- aka f0rk, f0rki, f0rkmaster, Gabel, etc.
- Coding Monkey/Server-Admin

Hagenberger Kreis

WTF ist phishing?

Definition

Phishing ist eine Form von Social Engineering, die meist über digitale Medien und automatisiert durchgeführt wird.

Hagenberger Kreis

WTF ist phishing?

Was?

- Ausspionieren von Zugangsdaten

Wer?

- Kriminelle Organisationen
- Scriptkiddies
- Chinesen

Wie?

- Verbreitung per Mail, IM, Telefon, etc.
- Meist gefälschte Web Seiten

Hagenberger Kreis

Durchführung

1. Phisher sucht sich eine profitable Internet Seite
2. Phisher baut diese seite (mehr oder weniger detailliert) nach
3. Phisher versendet Phishing-Mail
4. PROFIT???

Hagenberger Kreis

Ja hoii... a email!

Aber...

Hagenberger Kreis

Aber... die meisten Phisher san deppad.

Fehler der Phisher

- Begehen Design-Fehler
- Rechtschreibfehler
- unzureichend HTTPS
- hinterlassen verdächtige Log-Entries am Opfer-Server

Hagenberger Kreis

Aber... die meisten Phisher san deppad.

```
200.x.x.x - - [26/Aug/2005:10:35:53 -0400] "GET
    /images/logo.gif HTTP/1.1" 200 3006
    "http://by14fd.bay14.hotmail.msn.com/cgi-bin/getmsg?msg=
    "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
    5.1;SV1)
```

Aber... die meisten Phisher san deppad.

```
216.x.x.x - - [26/Aug/2005:12:43:29 -0400] "GET
    /personal-banking/personal-
banking.php HTTP/1.1" 200 22867
    "http://200.213.21.5/menu/imagens/obfuscated/secure-
activ.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows
    NT 5.1; SV1)"
```

Aber... die meisten Phisher san deppad.

```
81.181.196.1XX - - [26/Aug/2005:08:08:29 -0400] "GET
    /personal-banking/personal-banking.php HTTP/1.1" 200
    22867
"http://200.213.21.5/menu/imagens/www.obfuscated.com/secure
    "Mozilla/4.0(compatible; MSIE 6.0; Windows NT 5.1;
    SV1)"
```

- weitere verdächtige log-entries von 81.181.196.1XX
- wahrscheinlich IP-Adresse des Angreifers

Hagenberger Kreis

CERTs verständigen

- Phishing Server wird down genommen
- Phisher ausforschen (über IP-Adresse)

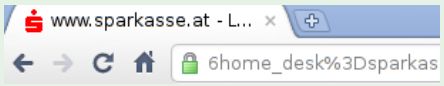
Vorsicht vor Phishern

niemals

- links aus email anklicken
- zugangsdaten leichtfertig eingeben

wichtig

- https



- valide Zertifikate
- richtiger domain name (keine typos, etc.)
- **Hausverstand einsetzen!**

Referenzen


http://www.metasploit.com/


https://secure.wikimedia.org/wikipedia/de/wiki/Phishing


http://www.nmap.org/


http://mnin.org/?page=phish

Hagenberger Kreis