



### Cybercrime

Velen van ons hebben wel eens een email uit Kenia of Nigeria ontvangen van een zogenaamde notaris die niet goed raad wist met het nalatenschap van een persoon met toevallig dezelfde achternaam als u. Mogelijk dat u familie bent en of u kunt helpen door uw bankrekeningnummer te geven.

Inmiddels heeft cybercrime een grote vlucht genomen. In bepaalde landen met een gunstig klimaat voor cybercrime vindt op grote schaal oplichting via het internet plaats.

Onder het begrip cybercrime valt meer dan alleen oplichting, diefstal en afpersing. Ook zaken als virussen, malware en dergelijke vallen onder dit begrip.

In dit artikel wil ik het hebben over de technieken phishing en pharming die steeds meer worden ingezet bij oplichting en diefstal.

#### Wat is phishing?

Phishing is het "hengelen" naar gegevens over een potentieel slachtoffer, zoals zijn bankrekeningnummer, pincode en wachtwoorden, waarmee vervolgens een bankrekening kan worden geplunderd.

Een veel gebruikte methode is het versturen van een email van de "bank". U wordt uitgenodigd om op een link te klikken naar uw bank. In plaats van naar uw eigen bank, wordt u naar een andere site geleid, die er verder hetzelfde uitziet, maar een afwijkend URL heeft. Als u vervolgens nietsvermoedend uw transacties doet, heeft de "phisher" voldoende gegevens om uw saldo bij te werken in zijn voordeel.

Een ander voorbeeld is het versturen van email naar medewerkers, schijnbaar afkomstig van bijvoorbeeld de interne IT-afdeling met een verzoek voor opgave van uw gebruikersnaam en wachtwoord via een link.

#### Wat is pharming

Vaak worden phishing en pharming in één adem genoemd. Het begrip pharming staat voor een techniek, waarbij het potentiële slachtoffer meer "voortgedreven" wordt naar een bepaald doel, een website. Door bijvoorbeeld een stukje malware in zijn browser komt het slachtoffer bij het intypen van de juiste URL voor de bank, niet bij de bank, maar bij een andere site uit.

Bij phishing is het wachten tot het slachtoffer "bijt", terwijl bij pharming de tools (malware) al actief zijn om het slachtoffer een bepaalde kant op te sturen.

Het doel van pharming is, net als bij phishing, het stelen van informatie van het slachtoffer.

### Secure Connection brengt nieuwe versie StandardGUI infrastructure uit.

In onze vorige nieuwsbrieven heeft u kunnen lezen over onze succesvolle aanpak met betrekking tot kennisobjecten en onze StandardGUI infrastructuur, waarmee u zowel stand-alone als ook in een client-server omgeving kennisobjecten kunt gebruiken en kennis kunt delen met collega's binnen uw organisatie.

Met de nieuwste client-server infrastructuur kunt u zelf bepalen via welke poort u wilt communiceren.

De payload van de communicatie tussen client en server is volledig encrypt.

StandardGUI infrastructure is in elk willekeurig TCP/IP netwerk in te zetten.

De server heeft verder een

console, waarbij u kunt zien

welke activiteiten er hebben

plaatsgevonden. Tevens

kunt u zien hoeveel users u

heeft en hoeveel er zijn aan-

gemaakt en hoeveel threads

u heeft en hoeveel er op dat

moment zijn.

| MsgName           | MsgId | Source                | Date       | Time     | Action Result | Object  |
|-------------------|-------|-----------------------|------------|----------|---------------|---|
| KeyExchangeReply  | 109   | 192.168.0.4/192.16... | 30-05-2006 | 07:32:05 |               |   |
| GetDirectory      | 10    | 192.168.0.4/192.16... | 30-05-2006 | 07:32:08 | OK            |   |
| GetObjectDir      | 30    | 192.168.0.4/192.16... | 30-05-2006 | 07:32:11 |               |   |
| GetObjct          | 30    | 192.168.0.4/192.16... | 30-05-2006 | 07:32:13 |               | SAL-Standard-v21-SC.ocb                                       |
| LoginReply        | 105   | 192.168.0.4/192.16... | 30-05-2006 | 07:34:39 | true          | janjaerma   |
| KeyExchangeReply  | 109   | 192.168.0.4/192.16... | 30-05-2006 | 07:34:39 |               |   |
| GetDirectory      | 10    | 192.168.0.4/192.16... | 30-05-2006 | 07:34:44 |               |   |
| GetObjectDir      | 30    | 192.168.0.4/192.16... | 30-05-2006 | 07:34:46 |               |   |
| GetObjct          | 20    | 192.168.0.4/192.16... | 30-05-2006 | 07:34:48 |               | SAL-Standard-v21-SC.ocb                                       |
| MsgName           | MsgId | Source                | Date       | Time     | Action Result | Object  |
| GetDirectoryReply | 11    | 192.168.0.4/192.16... | 30-05-2006 | 07:32:08 |               |   |
| GetObjectReply    | 31    | 192.168.0.4/192.16... | 30-05-2006 | 07:32:11 |               |   |
| GetObjctReply     | 21    | 192.168.0.4/192.16... | 30-05-2006 | 07:32:14 |               | C:\SecconDev\stdgui-server\data/Common\SAL-Standard-v21-SC... |
| Login             | 104   | 192.168.0.4/192.16... | 30-05-2006 | 07:34:31 |               |   |
| KeyExchange       | 105   | 192.168.0.4/192.16... | 30-05-2006 | 07:34:39 |               |   |
| GetDirectoryReply | 11    | 192.168.0.4/192.16... | 30-05-2006 | 07:34:44 |               |   |
| GetObjectDirReply | 31    | 192.168.0.4/192.16... | 30-05-2006 | 07:34:46 |               |   |
| GetObjctReply     | 21    | 192.168.0.4/192.16... | 30-05-2006 | 07:34:49 |               | C:\SecconDev\stdgui-server\data/Common\SAL-Standard-v21-SC... |

Server Status messages:

```

Connection with Client 192.168.0.4/192.168.0.4 30-05-2006 07:34:31
DataConnection bot (read loop) Client thread
Connection with 192.168.0.4/192.168.0.4 terminated by client 30-05-2006 07:45:48
User janjaerma logged off 30-05-2006 07:45:48
  
```

Max Threads: 2    Maximum Users: 5  
 Active Threads: 0    Defined Users: 2

### Actueel

#### Lek in Symantec Antivirus

Afgelopen vrijdag melde het bedrijf eEye Digital Security een lek in een tweetal producten van Symantec, te weten Symantec Antivirus 10.x en Symantic Client Security 3.x.

Het lek is inmiddels gedicht door Symantec. Het gevonden lek was een ernstig lek, omdat een hacker via deze exploit met behulp van een worm malicious code op een systeem kan uitvoeren, zonder interactie van de gebruiker.

Behalve de ernst van het lek is baart ook de exploit zelf (een stack overflow) zorgen als het gaat om de kwaliteit van de geleverde software. Dergelijke exploits zouden bij voldoende aandacht voor veilig programmeren eigenlijk niet voor mogen komen.

Dergelijke ontdekkingen doen ook vrezen dat meer lekken zijn, die vroeg of laat zullen worden ontdekt.

Bron: [www.eweek.com](http://www.eweek.com)