# ROOTKITS & CO. – DIGITALES E605

Michael Willers

http://staff.newtelligence.net/michaelw/

# IN DIESEM VORTRAG...

- Rückblende
- Stand der Dinge
- Rootkits: Digitale Tarnkappen
- Ausblick

# LIEBE, LIEBE, LIEBE

**Donnerstag, 4. Mai**
**4:12 Uhr**
Antivirus-Hersteller in Europa empfangen die ersten Meldungen von Kunden und beginnen um ca. 5:00 Uhr mit der Analyse. Es wird schnell klar: Der Wurm, geschrieben in VB Script, ist nicht sehr kompliziert, aber extrem ansteckend.

**Mittwoch, 3. Mai 2000**
Ein neuer Wurm taucht auf.
Unter den ersten „Patienten“

**Ca. 7:00 Uhr**
…urne klickt ein Mitarbeite…
…ags „Lonely Planet“ auf d…
…schickt den Wurm an …
…n in der ganzen W…

**18:40 Uhr**
Viele Antivirus-Hersteller machen Virus-Definitionsfiles zum freien Download über das Web verfügbar.

…virusmeldungen aus aller Welt
gehen zurück. Insgesamt …d jetzt
29 Varianten im Umlauf
…halbe Million PCs wurden

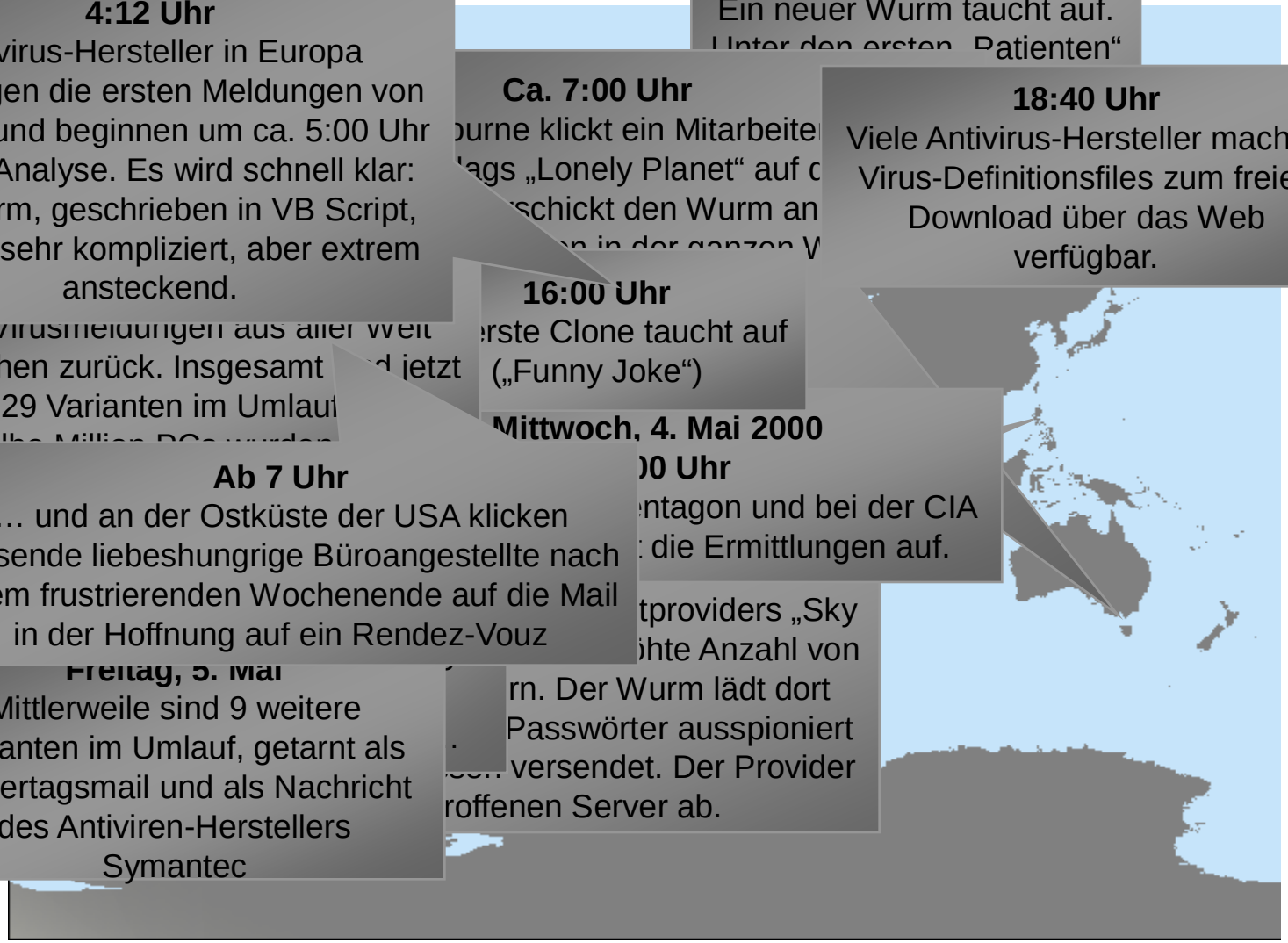
**16:00 Uhr**
…erste Clone taucht auf
(„Funny Joke“)

**Mittwoch, 4. Mai 2000**
**…00 Uhr**
…entagon und bei der CIA
… die Ermittlungen auf.

**Ab 7 Uhr**
… und an der Ostküste der USA klicken Tausende liebeshungrige Büroangestellte nach einem frustrierenden Wochenende auf die Mail in der Hoffnung auf ein Rendez-Vouz

…tproviders „Sky
…öhte Anzahl von
…rn. Der Wurm lädt dort
…Passwörter ausspioniert
…versendet. Der Provider
…roffenen Server ab.

**Freitag, 5. Mai**
Mittlerweile sind 9 weitere Varianten im Umlauf, getarnt als Muttertagsmail und als Nachricht des Antiviren-Herstellers Symantec



Quelle: PCWorld.com

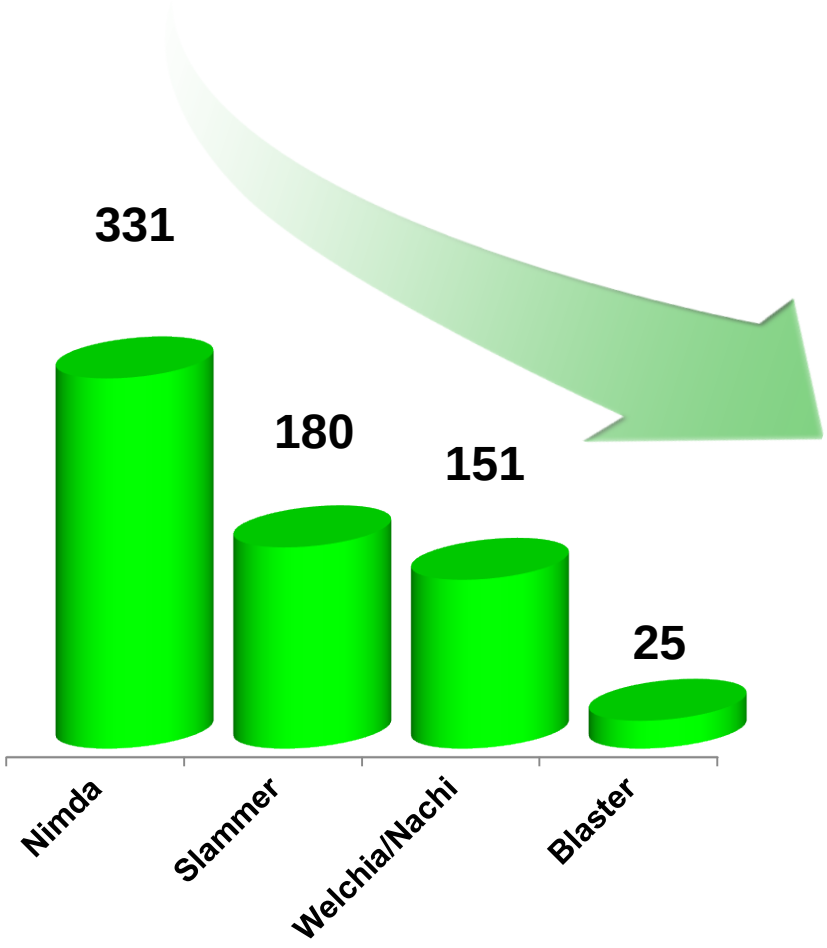
# CODE – BLASTERS ANGRIFFSZIEL

Port 135 (Z.B. aus dem Internet)

```
error_status_t _RemoteActivation(WCHAR *pwszObjectName,    ... )  {
    *phr = GetServerPath(pwszObjectName, &pwszObjectName);
    …
}
HRESULT GetServerPath(WCHAR *pwszPath, WCHAR **pwszServerPath ){
    WCHAR * pwszFinalPath = pwszPath;
    WCHAR wszMachineName[MAX_COMPUTERNAME_LENGTH_FQDN + 1];
    hr = GetMachineName(pwszPath, wszMachineName);
    *pwszServerPath = pwszFinalPath;
}
HRESULT GetMachineName(
    WCHAR * pwszPath,
    WCHAR   wszMachineName[MAX_COMPUTERNAME_LENGTH_FQDN + 1]) {
    pwszServerName = wszMachineName;
    LPWSTR pwszTemp = pwszPath + 2;
    while ( *pwszTemp != L'\\' )
        *pwszServerName++ = *pwszTemp++;
```

!!!

# PATCH MANAGEMENT - REAKTIONSZEIT




- Zeitspanne zwischen erscheinen des Patches und Auftreten eines Exploits wird immer kürzer
- Exploits werden intelligenter
- Ansatz Patch Management reicht nicht
- Neue Techniken müssen entwickelt werden

# RÜCKBLENDE

- Buffer Overruns dienen als Methode zum Einschleusen von fremdem Code
- Virenscanner reichen nicht mehr aus
- Anwendungen werden zum Angriffsziel
- In der Regel „Proof of concept“
- Administratorrechte machen dem Angreifer das Leben leicht

# UNGEZIEFER UND WIRKUNG

- Die meisten Viren werden benutzt, um Massen-Mailings auszuführen
  - Sober N schickte Benachrichtigungen über Tickets zur Fussball-WM durch die Welt
  - Sober-N missbrauchte die PCs als sogenannte Zombie-PCs, um ohne deren Wissen Neonazi-Propaganda-Mails zu versenden.
- Mytob-Familie wird oft für Phishing Attacken benutzt

# AUS DEM HEISE-TICKER...

news 14.02.2006 16:57

<< Vorige | Nächste >>

## Phishing mit gültigen SSL-Zertifikaten

Nach Angaben des Internet Storm Centers (ISC) haben die Online-Betrugsversuche in den USA eine neue Qualität erreicht, um Anwendern noch überzeugendere Phishing-Seiten zu präsentieren. So wird im Artikel "Phollow the Phlopping Phish" ein Fall geschildert, bei der die Betrüger eine Domain registrierten, um Kunden der Bank Mountain America in die Falle zu locken. Nicht nur, dass die Adresse mit www.mountain-america.com relativ unverdächtig aussah (die richtige Adresse lautet www.mtnamerica.com), zudem haben die Phisher ihren Webserver mit einem gültigen SSL-Zertifikat ausgestattet.

Besucher der Seiten konnten also selbst mit einer genauen Prüfung des Zertifikates nicht feststellen, dass sie auf einer Phishing-Seite gelandet waren. Alle im Zertifikat angegebenen Daten waren scheinbar korrekt. Selbst eine zusätzliche Überprüfung der Identität über den Dienstleister ChoicePoint, nach eigenen Angaben der führende US-Dienstleister für die Überprüfung von Identitäten, bestätigte die Echtheit der Seite. Laut ChoicePoint war die Domain auf Mountain America in Salt Lake City, dem Stammsitz der Bank, registriert.

Besonders prekär: ChoicePoints Daten stammten vom Zertifikatsaussteller Equifax, einem Reseller von GeoTrust, der auch bereits das SSL-Zertifikat herausgab. Wie es zu der Fälschung kommen konnte, ist indes nicht klar. Auf Nachfrage bekam das ISC die Antwort, dass für einen Zertifikatsantrag mehrere Dokumente erforderlich seien. Unter anderem würden amtliche Belege wie Gewerbescheine, Auszüge aus Handelsregistern und dergleichen gefordert. Dass nun auch Betrüger die Prüfungsprozedur durchstanden haben, ist gerade für GeoTrust besonders peinlich. Noch im April 2005 bemängelte der Dienstleister die laschen Prüfungsprozesse vieler anderer Zertifizierungsstellen und insbesondere deren Subunternehmer und Reseller.

# DIE NEUGIER...

- 62% der deutschen Frauen lesen die SMS Ihrer Partner
- Über 20% lesen Dokumente auf dem Rechner von Freunden, sofern sich die Gelegenheit bietet
- 27% würden Firmengeheimnisse auf dem Rechner des Chefs lesen
- Quelle: Spiegel online, 8. August 2003

# MÜLLTAUCHEN (DUMPSTER DIVING)

# KEY

- 5 S
- SÄ
- Sic
  sta
- Fü

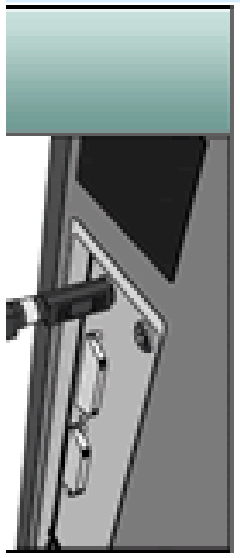
Untitled - Notepad

File Edit Format Help

```
vghostlog

Hit 'c' to slow down menu

***
KeyGhost SX Std 512KB v8.8
www.keyghost.com

Menu >

1)  Entire log download
2)  Section log download
3)  Erase log
4)  Format
5)  Options
6)  Optimize speed
7)  Password change
8)  eXit

Select > 1

- key to stop -

Keys so far 128 out of 523744 ...

<ON>This text has been recorded.  Then I access the menu
with my password

vghostlog
```

OS

en



# STAND DER DINGE

- Angriffe haben Experimentierstatium verlassen
- Buffer Overrun verliert an Bedeutung
  - Typsichere Programiersprachen
- Gezieltes Ausspionieren von personenbezogenen Daten wird zur Regel
- Phishing
  - Installieren von „Backdoors“ (MyTob)
- Social Engineering
  - „Gib mir mal Deine Email Addresse...“
  - „Ich brauch mal ganz nötig Dein Passwort...“
  - ...

# WMF-EXPLOIT (VEREINFACHT)

- WMF Dateien enthalten Code
  - „Postscript-Prinzip“
- „SetAbortProc“ des GDI-Subsystems wird als Einfallstor benutzt
- Herkömmliche Abwehrmaßnahmen sind nutzlos!!!
- Ausspionieren von persönlichen Daten auch ohne(!) Administratorrechte
- Mehr dazu unter
  - http://www.sysinternals.com/blog/2006/01/inside-wmf-backdoor.html

# ROOTKITS

- Dienen zum Verstecken von Funktionalität
  - Registryeinträge
  - OS-Prozesse
  - ...
- Tarnkappe für böswilligen Code
  - Dienen lediglich als Einfallstor
  - Heute als Gerätetreiber verpackt
  - Brauchen in der Regel Administratorrechte
- Kurz: Unterwandern des OS-Kernels!!!

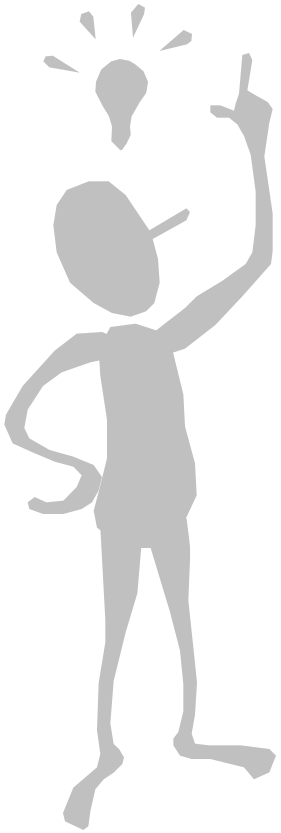
# KERNELKOMPONENTEN

- Prozessverwaltung
- Dateizugriff
- Sicherheit
- Speicherverwaltung

# VORGEHENSWEISE

- Code wird als Gerätetreiber eingeschleust
- Treiber muss geladen werden
  - Darf nicht in auslagerbarem Speicher liegen
  - Quick-and-Dirty (undokumentiert)
  - Service Control Manager
- Treiber muss Neustart „überleben“
  - Der gute alte Run-Key /Registry
  - Trojaner oder infizierte Datei / Ini-Dateien
  - Modifikation des Kernels auf der Festplatte oder des Bootloaders

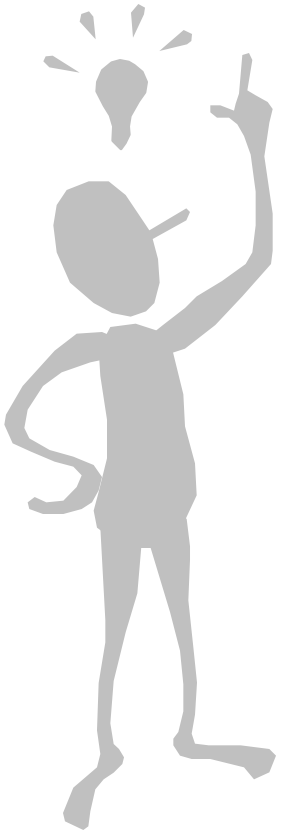
# TREIBER IM EIGENBAU...



# STRATEGIEN

- „Einklinken“ in Betriebssystemfunktionen
  - Injektion von Code in fremde Prozesse (DLL-Injection)
  - Erstellen von Hooks
- Manipulation von Kernelobjekten
  - Direct Kernel Object Manipulation (DKOM)
  - Prozesse, Threats, Treiber verbergen
  - Rechte und Privilegien ändern
  - Anfällig gehen Änderungen in neuen OS-Versionen
- Hybrider Ansatz
  - Per Treiber Code injizieren
    - Codeinjektion braucht „Platz“ im Remoteprozess (Shared Memory)
    - Kann so leicht entdeckt werden
- Direkter Hardwarezugriff

# BASTELSTUNDE...



# WIRKLICH SO EINFACH?

- Wie übersteht man das Auslagern von Speicherseiten (Paging)?
  - Code muss in einem Speicherbereich ablegt werden, der nicht ausgelagert wird
  - Ansonsten: „Blue Screen“
- Wie übersteht man einen Neustart des Systems?
  - Code im Speicher der Grafikkarte ablegen
  - Code auf vermeintlich defekten Sektoren der Festplatte ablegen und von dort laden
- Und, und, und...

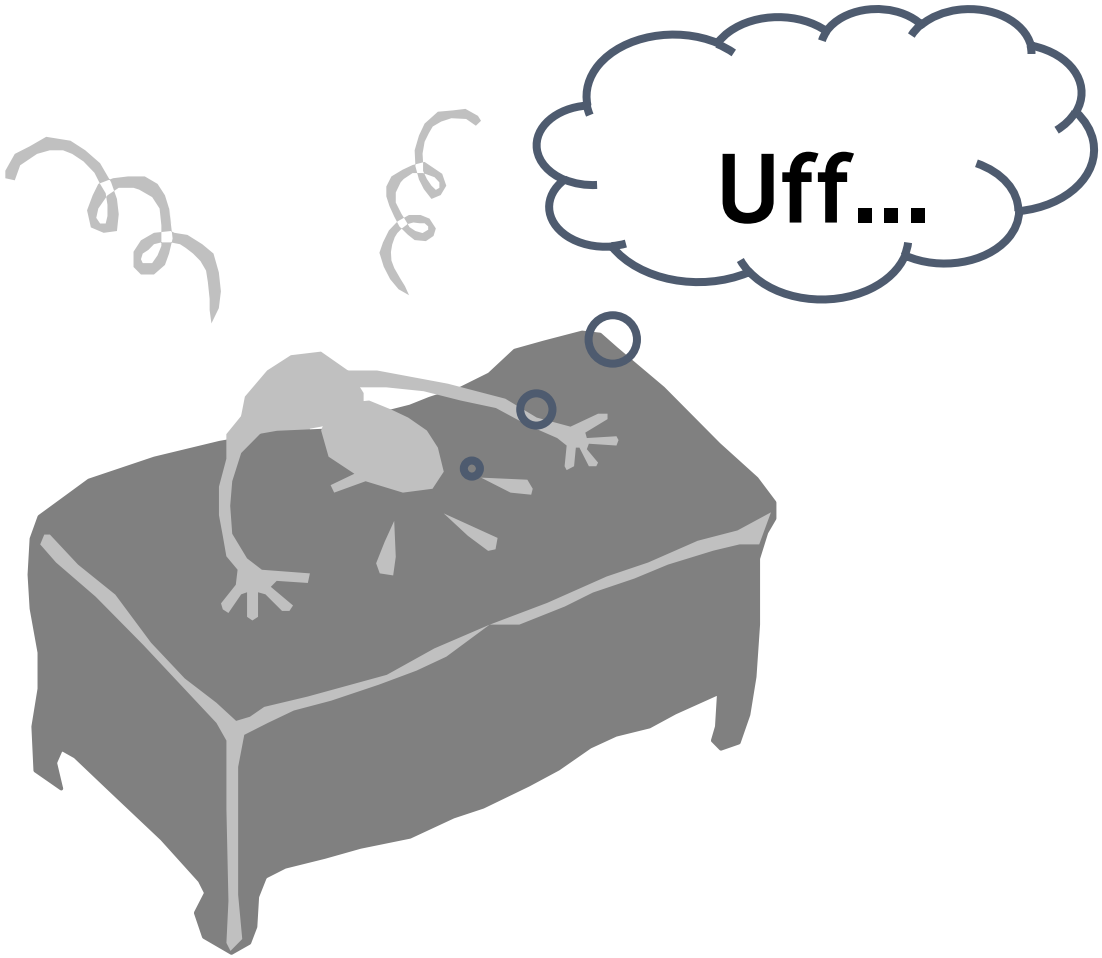
# STAND DER DINGE

- Rootkits dienen als Methode zum Einschleusen und Verstecken von fremdem Code
- Virenscanner sind nutzlos geworden
- Anwendungen sind vorrangiges Angriffsziel
- Systematisches Ausspionieren
- Administrator- oder Systemrechte (Local System) machen dem Angreifer das Leben leichter

# LERNEN WIR DAZU?

- Die Wirkung von Angriffen wird zunehmend verheerender
  - Gezieltes Ausspionieren persönlicher Daten
  - Kriminelle Energie als Hauptursache
- Die Ursache indes bleibt gleich
  - Administrator- oder Systemrechte machen dem Angreifer das Leben nach wie vor leicht

# FRAGEN!?



# DANKE FÜR IHRE AUFMERKSAMKEIT

**http://staff.newtelligence.net/michaelw**